N° 1141

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 4 juillet 2018.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA COMMISSION DE DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES

en conclusion des travaux d'une mission d'information [1]

sur la **cyberdéfense**

ET PRÉSENTÉ PAR

M. BASTIEN LACHAUD et MME ALEXANDRA VALETTA-ARDISSON,

Députés

(1) La composition de cette mission figure au verso de la présente page.

La mission d'information sur la cyberdéfense est composée de :

– M. Bastien Lachaud et Mme Alexandra Valetta-Ardisson, *rapporteurs* ;

– MM. Thibault Bazin, Florian Bachelier, Olivier Faure, Yannick Favennec Becot, Philippe Michel-Kleisbauer et Mme Patricia Mirallès, *membres.*

SOMMAIRE

—

Pages

« *Le théâtre de la guerre embrasse toutes les contrées où deux puissances peuvent s'attaquer.* »

Antoine-Henri de Jomini [(1)], *Précis de l'art de la guerre*, 1838.

INTRODUCTION

Une succession logique de 0 et de 1 au sein d'un code informatique binaire pourra-t-elle demain provoquer autant de dégâts qu'un missile de croisière naval ou qu'un obus tiré par un canon Caesar en rendant inutilisables des équipements, des matériels ou des infrastructures militaires ? Un virus aux effets systémiques, par la désorganisation massive qu'il provoquera, aboutira-t-il à la mort d'êtres humains, y compris des civils ? Comme le souligne la Revue stratégique de cyberdéfense publiée en février 2018 par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) : « *Il est probable qu'une attaque informatique de cette nature [actes de blocage ou de sabotage des systèmes informatiques] aura, un jour, des conséquences létales.* »

Ce qui pouvait relever hier encore de la science-fiction ou, du moins, de scénarios catastrophes dont on peinait à envisager le caractère réalisable à un horizon prévisible apparaît dorénavant comme une possibilité sérieuse, comme une menace tangible et comme une éventualité stratégique à prendre en considération en termes de doctrine militaire, de conduite des opérations et, plus globalement, d'organisation de la protection et de la résilience de l'ensemble de la société.

L'intérêt et la compétence de la commission de la Défense nationale et des forces armées pour le « sujet cyber » sont légitimes car les fondements de notre système de cyberdéfense ont majoritairement été posés dans le cadre des différentes lois de programmation militaire (LPM) adoptées depuis 2009. La prochaine LPM 2019-2025, votée les 27 et 28 juin successivement à l'Assemblée nationale et au Sénat, ne fait pas exception : un chapitre spécifique, le chapitre III du titre II, est consacré à la cyberdéfense.

Il était donc naturel que la commission s'empare de ce sujet à l'occasion d'un travail de plus long cours que celui effectué, sous des délais forcément contraints et sur des dispositifs ciblés, à l'occasion de l'examen du projet de loi de programmation militaire 2019-2025. Il convient toutefois d'effectuer deux remarques à titre liminaire.

(1) Militaire, baron de l'Empire, historien et théoricien de la stratégie militaire.

En premier lieu, le présent rapport ne prétend pas à l'exhaustivité, et ce pour plusieurs raisons :

– le cyber est par nature une réalité « universelle », globale, qui concerne peu ou prou tous les champs de l'activité sociale, aux niveaux local, national, européen, international. Il dépasse donc le champ de compétence d'une seule commission ;

– il s'agit d'un domaine extrêmement mouvant, en perpétuelle évolution ;

– ainsi que les rapporteurs ont pu le constater très rapidement et très directement, les analyses menées dans ce domaine se heurtent vite à l'obstacle du secret de la défense nationale ;

– la Revue stratégique de cyberdéfense précédemment évoquée a déjà dressé un panorama très complet de la question, et il était évidemment inutile de « doublonner » le travail déjà effectué dans ce cadre.

Face à un sujet inépuisable, les rapporteurs ont donc pris le parti de centrer leur analyse en insistant sur un certain nombre de points qui ont particulièrement retenu leur attention.

En second lieu, ce rapport n'a naturellement pas vocation à constituer le *vade-mecum* de référence du parfait cyber-attaquant ou du parfait cyber-défenseur. Les rapporteurs n'entreront donc pas dans des considérations excessivement techniques puisque tels ne sont ni la vocation, ni l'intérêt de leur travail.

S'agissant d'un rapport d'information élaboré au nom de la commission de la Défense, les rapporteurs s'attacheront certes plus particulièrement aux problématiques intéressant la défense, mais pas exclusivement, dès lors que le cyber irrigue tous les domaines et brouille les frontières traditionnelles entre les États, entre les acteurs, entre les secteurs.

De fait, le cyberespace est essentiellement composé d'éléments non militaires. Proportionnellement, seul un petit nombre de systèmes et d'équipements spécifiques est exclusivement de nature militaire les caractérisant comme des cibles légitimes au regard du droit des conflits armés. Dans le cyberespace, le rapport entre cibles militaires et cibles civiles s'inverse, du moins du point de vue quantitatif. Il s'agit là d'une réalité dont il faut tenir compte.

Le cyberespace n'en est pas moins devenu un champ d'affrontement supplémentaire, qui vient s'ajouter aux champs traditionnels : terre, mer, air et espace. Sa spécificité est qu'il existe en tant que tel, mais qu'il est également présent *à l'intérieur* de ces champs traditionnels, dès lors qu'une cyberattaque peut produire des effets non seulement dans le cyberespace, mais également sur les théâtres physiques.

La dimension cyber est donc dorénavant une dimension à part entière du domaine de la défense. Comme le rappelle le rapport annexé à la LPM 2019-2025 : « *En matière de lutte informatique offensive, de nouvelles capacités d'action, intégrées à la chaîne de planification et de conduite des opérations, seront systématiquement déployées en appui de la manœuvre des armées.* »

La « cyberguerre », au sens d'un conflit mené exclusivement dans le cyberespace avec l'emploi des seules armes cyber n'est sans doute pas (encore) une réalité opérationnelle. Mais il n'y aura plus, demain, de conflit sans dimension cyber. Le cyberespace est un espace qui n'est ni en guerre ni en paix, mais en état de tension permanente. Un tel constat exige de ce fait une organisation et la mise en place de politiques et d'actions à la fois spécifiques et globales de la part des pouvoirs publics. À cet égard le présent rapport a vocation à rappeler « l'état de la cyberdéfense » en France, mais également dans certains pays étrangers au regard de l'état des risques et des menaces. Par ailleurs il s'efforce, modestement compte tenu du caractère global et extrêmement mouvant de la question, de proposer des pistes de réflexion et d'évolution pour l'avenir.

I. LA CYBERDÉFENSE : DE QUOI PARLE-T-ON ?

La cyberdéfense est un sujet qui se caractérise par un degré certain de technicité et qui fait appel à des concepts dont l'appréhension et la compréhension ne sont pas toujours aisées.

Même si elle fait l'objet d'études et de débats toujours plus nombreux y compris, compte tenu de l'actualité, dans des publications généralistes à destination du grand public, la cyberdéfense demeure un sujet « de niche » relativement difficile d'accès.

C'est pourquoi il a semblé nécessaire aux rapporteurs de consacrer des développements spécifiques – sans être exhaustifs ou inutilement techniques – au cadre général de la cyberdéfense, avant de s'attacher à présenter certaines des principales spécificités du milieu cyber, notamment d'un point de vue militaire, pour enfin faire état des risques et des menaces actuellement à l'œuvre dans ce milieu ainsi que de leur évolution constatée ou prévisible.

A. CADRE CONCEPTUEL ET PRINCIPES

1. Quelques définitions préalables

« Cyberdéfense », « cybersécurité », « cyberespace »… Il peut régner une certaine confusion lexicale en matière cyber, la même expression étant parfois employée indifféremment pour qualifier deux réalités pourtant différentes [(1)]. Par ailleurs, tout a tendance à devenir « cyber ». Le terme « cyber » lui-même, associé à tout autre nom commun, est ainsi parfois utilisé par facilité afin, selon son auteur, de conférer plus de poids ou plus de hauteur à une analyse.

Les rapporteurs estiment donc nécessaire, au préalable, de rappeler certaines définitions à la lumière desquelles le présent rapport pourra être appréhendé. Pour ce faire, ils s'appuieront principalement sur les définitions fournies par l'Agence nationale de sécurité des systèmes d'information (ANSSI) et, si nécessaire, sur les définitions applicables au ministère des Armées ou utilisées par lui, notamment dans un contexte opérationnel [(2)].

● Cyberespace

L'ANSSI le définit comme un « *espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques* ».

(1) Tel est le cas notamment des termes « cyberdéfense » et « cybersécurité ».

(2) Vocabulaire de la défense : cyberdéfense (liste de termes, expressions et définitions adoptés), *JORF n° 0219 du 19 septembre 2017, et glossaire interarmées de terminologie opérationnelle.*

● Cyberdéfense

Elle comprend l'« *ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels* ».

● Cybersécurité

L'ANSSI l'entend comme l'« *état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles* ». L'ANSSI précise que la cybersécurité « *fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense* ».

● Cybercriminalité

Elle est constituée des « *actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible* ».

● Cyberattaque

D'après le glossaire interarmées de terminologie opérationnelle (GIATO), une cyberattaque est une « *action volontaire, offensive et malveillante, menée au travers du cyberespace et destiné à provoquer un dommage (en disponibilité, intégrité ou confidentialité) aux informations ou aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support* ».

● Cyberrésilience

Il s'agit de la « *capacité d'un système d'information à résister à une panne ou une cyberattaque et à revenir à son état initial après l'incident* » ou, du moins, à un état de fonctionnement et de sécurité satisfaisant.

● Lutte informatique défensive (LID)

« *Dans le cadre des opérations dans le cyberespace, action consistant à surveiller, analyser, détecter et réagir face à des attaques, intrusions ou perturbations qui pourraient compromettre, paralyser ou détruire les systèmes, réseaux et données.* »

● Lutte informatique offensive (LIO)

« *Dans le cadre des opérations dans le cyberespace, action non physique entreprise dans le cyberespace contre des systèmes d'information ou des données pour les perturber, les modifier, les dégrader ou les détruire.* »

2. Le cyberespace : un milieu artificiel, abstrait et global, nouveau lieu de confrontations au demeurant classiques dans leur nature

a. Un milieu créé, sans limites et en recomposition permanente

● Il convient tout d'abord de rappeler ce qui peut sembler une évidence mais qui est trop souvent oublié : contrairement aux autres milieux « classiques » dans lesquels s'inscrit l'activité humaine – les milieux terrestre, naval, aérien et spatial – le cyberespace est un milieu artificiel, créé, une construction humaine et non un milieu naturel.

Ce constat emporte plusieurs conséquences. Tout d'abord et à l'inverse des espaces terrestre, aérien et maritime, il s'agit d'un espace qui ne connaît ni limites ni réalités ou caractéristiques géographiques physiques, ni frontières politiques ou juridiques qui permettraient, d'une part, d'en délimiter précisément les contours et, d'autre part, de le subdiviser pour en rattacher les différentes composantes à chaque État de la planète, ou à aucun d'entre eux (cas de l'Antarctique, de l'espace aérien international ou de la haute mer).

Espace créé, il s'agit également un espace mouvant, en recréation permanente. Il n'existe pas de carte du cyberespace, de ses « continents » et de ses limites, au-delà de la cartographie des flux d'information ou des lieux d'implantation des serveurs, par exemple. Le cyberespace se recompose en permanence sans exister réellement au sens physique, au gré des actions qui y sont menées par des acteurs qui se jouent des notions de territorialité ou de souveraineté, étrangères à un espace ouvert par nature. Le cyberespace et les éventuels conflits qui s'y déroulent sont donc à repenser en permanence.

● Espace abstrait [(1)] et changeant, le cyberespace n'en constitue pas moins un *théâtre d'opération* potentiel, d'un point de vue militaire, au même titre cette fois que les espaces terrestre, aérien, maritime, voire spatial. Des acteurs, étatiques ou non-étatiques, y agissent en permanence et utilisent le cyberespace pour atteindre des buts politiques en exploitant toutes les possibilités offertes par ce nouveau milieu. C'est donc un théâtre qu'il s'agit de comprendre, de maîtriser, de sécuriser, de réguler. C'est notamment ce à quoi s'attachent les acteurs étatiques, directement ou indirectement *via* des intermédiaires (*proxies*) plus ou moins transparents [(2)]. De ce point de vue, le cyberespace ne diffère pas fondamentalement des quatre milieux traditionnels, d'autant que les actions qui y sont menées ne se distinguent pas, dans leur nature, des actions traditionnellement conduites en particulier par les États (espionnage, sabotage, déstabilisation).

Naturellement, et même si le présent rapport s'attache à titre principal à des considérations intéressant la défense au sens large, la frontière avec la sphère civile est poreuse car le cyberespace est utilisé quotidiennement, au-delà des acteurs « classiques » des relations internationales, par des organisations, des

(1) En dehors de sa couche matérielle.
(2) Certains groupes de hackers *par exemple.*

entreprises, des particuliers et pour toutes les activités humaines imaginables, y compris les activités illicites.

b. Un « milieu de milieux »

Le cyberespace est enfin un espace global qui, en s'y « superposant », en les englobant, contient les espaces traditionnels. Il n'est en effet aucun milieu qui échappe au cyber. Il serait certes présomptueux d'affirmer que l'ensemble des activités humaines, sans aucune exception, dépend du cyber, mais il faut reconnaître qu'à l'évidence, *la plupart* des activités essentielles nécessaires aux sociétés modernes reposent sur le cyberespace compte tenu du processus de numérisation croissante des sociétés contemporaines et de l'interconnexion toujours plus poussée des activités humaines.

En effet, comme l'a affirmé Marc Andreessen, créateur de Mosaic, l'un des premiers navigateurs web : « *le numérique dévore le monde* » [(1)]. Le cyberespace constitue ainsi un « méta espace » immatériel qui englobe tous les autres, ignore les frontières physiques et méconnaît les différences, juridiques et de nature, entre les différentes personnes physiques ou morales ou entre les différents secteurs d'activité.

On peut donc dire que le cyberespace est un « milieu de milieux », un « système critique de systèmes critiques ». En effet, dorénavant, toute activité humaine dépend, de près ou de loin, de l'informatique et du numérique. Qu'il s'agisse des transports, des télécommunications, des réseaux de production d'électricité, ou encore de la santé, un domaine auquel on ne songe pas spontanément, les mêmes systèmes sont nécessaires à leur fonctionnement. Cette caractéristique est d'autant plus prégnante s'agissant des réseaux informatiques qui, en réalité, reposent sur un seul et unique protocole de communication : l'*Internet Protocol* (IP).

3. Un espace structuré en trois couches distinctes

Comme le monde physique, le cyberespace n'est pas homogène mais est structuré en trois niveaux distincts, faisant l'objet d'une régulation plus ou moins poussée en fonction de leurs caractéristiques.

a. La couche physique ou matérielle

Elle comprend, en substance :

– l'ensemble des infrastructures qui permettent l'acheminement et l'échange des données au sein du cyberespace, y compris les lieux de stockage de l'information. Font ainsi partie de cette couche physique les serveurs, les centres de traitement de données (*data centers*), les câbles sous-marins [(2)], les réseaux de

(1) Marc Andreessen, « Why software is eating the world », The Wall Street Journal, *20 août 2011.*
(2) Plus de 99 % des communications intercontinentales (téléphonie et Internet) transitent par ces câbles.

fibre optique terrestre ou encore les réseaux de communication utilisant des ondes électromagnétiques (téléphonie mobile, radio, télévision, etc.) ;

– les appareils terminaux auxquels recourent les utilisateurs : ordinateurs, téléphones, tablettes numériques, objets connectés, systèmes électroniques, etc.

La couche physique du cyberespace peut être « territorialisée » juridiquement. S'agissant d'éléments physiquement situés sur des espaces géographiques donnés, ces différentes infrastructures et, par conséquent, la couche qui les regroupe, font l'objet d'une régulation et sont soumises à différents niveaux de législations et de juridictions, tant nationales qu'internationales.

La couche physique et les éléments qui la constituent peuvent donc être la cible d'actes malveillants et d'atteintes soit *via* le cyberespace, soit par des moyens conventionnels plus classiques (endommagement, altération, destruction, neutralisation, perturbation du fonctionnement, etc.).

Les câbles sous-marins ou les « pipelines du numérique »

La transmission d'informations par le biais de câbles sous-marins est loin d'être une réalité nouvelle puisque le premier câble télégraphique sous-marin fut installé en 1858 entre l'Irlande et le Canada. Vinrent ensuite les câbles téléphoniques.

Relativement peu nombreux au regard du trafic considérable qu'ils acheminent, les câbles sous-marins présentent des vulnérabilités de plusieurs ordres. Tout d'abord des vulnérabilités physiques : ils sont à la merci d'une coupure accidentelle, provoquée par un bâtiment de surface ou submersible ou un séisme, ou bien intentionnelle. Leur emplacement étant connu avec une précision de 10 à 20 mètres pour les besoins du trafic maritime, hormis celui de quelques câbles à usage militaire, ils sont l'objet de multiples opérations d'écoute, voire d'espionnage. Elles se déroulent soit dans les stations d'atterrissement des câbles, l'option la plus simple et la plus fréquente souvent utilisée par des puissances étatiques, soit en mer. Des sous-marins de grande profondeur américains et russes auraient la capacité soit de déposer un dispositif d'écoute sur le câble même, soit de s'en approcher *via* de mini-sous-marins autonomes.

L'implantation des câbles sous-marins, sans oublier celle des câbles terrestres, et leur trafic est le reflet géopolitique des équilibres mondiaux et des zones d'influence continentales et intercontinentales. En cas de conflits, la coupure d'Internet, est désormais une arme au même titre que les armes classiques dont elle peut précéder la mise en œuvre. Le sujet des câbles, maritimes ou terrestres, vecteurs de données, relève donc autant de la diplomatie, de la défense, du renseignement que de l'industrie.

En la matière, la France dispose avec Orange Marine d'une entreprise de premier ordre en matière d'ingénierie, d'installation et de maintenance de liaisons de télécommunications intercontinentales. Sa flotte câblière représente à elle seule 15 % de la flotte mondiale. En ce qui concerne la fabrication de câbles, l'annonce de la vente par Nokia de sa filiale Submarine Network Solutions (SNS), acquise avec Alcatel-Lucent, fait l'objet d'une attention particulière de l'État français qui ne souhaite pas voir tomber SNS, opérateur d'importance vitale (OIV), dans n'importe quelles mains.

Si les données sont l'or noir du XXI^e siècle, les câbles sous-marins et l'espace maritime [1] sont des interfaces stratégiques, génératrices de conflits

(1) La France possède la deuxième zone économique exclusive mondiale juste après les États-Unis.

potentiels, auxquelles la France devra à l'avenir accorder une attention croissante sauf à renoncer à une partie importante de sa souveraineté. Indispensables au fonctionnement des sociétés modernes, les différents éléments de la couche physique et les secteurs qui s'y rapportent font l'objet de mesures de protection particulières de la part de la puissance publique. Tel est le cas des douze secteurs d'importance vitale auxquels sont rattachés les différents opérateurs d'importance vitale, dont le régime sera présenté plus en détail ultérieurement.

b. La couche logique ou logicielle

Elle est constituée de l'ensemble des programmes – au sens générique du terme (1) – qui permettent d'accéder aux différents réseaux du cyberespace, de les exploiter, d'assurer le transport des données, etc.

C'est cette couche qui constitue classiquement la cible des menaces cybernétiques compte tenu, d'une part, de sa relative facilité d'accès s'agissant d'un espace totalement numérique et, d'autre part, des vulnérabilités attachées à ses éléments constitutifs. Une vulnérabilité est une erreur de conception ou une faiblesse touchant un équipement informatique, susceptible d'être exploitée par un attaquant pour conduire une action malveillante. Il peut, par exemple, s'agir d'une erreur dans le code informatique d'un équipement, qui constitue alors une faille. À titre d'exemple, on estime qu'une erreur est présente en moyenne toutes les 1 000 lignes de code. Google et l'ensemble des projets associés représenteraient deux milliards de lignes de code, Mac OS plus de 80 millions, Facebook plus de 60 millions, une frégate multimissions plusieurs millions.

Il n'en demeure pas moins que des atteintes sur la couche logicielle du cyberespace peuvent avoir – et ont déjà eu – des répercussions tout à fait concrètes sur le monde physique.

Les opérations menées sur la couche logicielle visent à agir sur les processus automatiques qui la « font vivre ». Il s'agit alors, en substance, de modifier les données en fonction desquelles les programmes déclenchent la réponse d'un appareil donné, par adjonction, altération ou suppression de ces données.

En effet, les réponses délivrées par un appareil relevant de la couche matérielle du cyberespace sont automatisées en fonction, d'une part, des données qu'il reçoit et, d'autre part, de leur traitement par son logiciel d'exploitation. La réponse d'un appareil numérique est donc conditionnée par la nature du flux entrant et par les prescriptions de son « code », qui traite ces données. Aussi, une action réalisée soit dans le champ des données, soit dans le champ logiciel, soit dans les deux champs de manière conjointe peut permettre d'assurer un contrôle sur la couche physique du cyberespace.

---

(1) Le terme « programme » regroupe ainsi les différents protocoles, langages, logiciels, etc. mis en œuvre dans le cyberespace.

Dans la couche logique, le code constitue donc à la fois la vulnérabilité et le principal levier d'action, précisément pour exploiter les vulnérabilités adverses. L'attaquant est alors à la recherche de failles de sécurité susceptibles d'être exploitées. À cet égard, les failles les plus valorisées sont les failles dites *zero-day*. Il s'agit de vulnérabilités affectant un système, inconnues de leur concepteur, qui n'ont jamais été identifiées et répertoriées, qui n'ont jamais fait l'objet d'une publication et dont la communauté de la sécurité informatique n'a donc pas connaissance. Elles confèrent dès lors à leur « découvreur » un avantage tactique certain, du moins jusqu'à ce que, une fois dévoilées, des correctifs (*patches*) leur soient apportés.

c. La couche cognitive ou informationnelle

Il s'agit de la couche du sens, du contenu, visibles sur les divers sites et pages Internet, dans les systèmes de messagerie électronique, sur les réseaux sociaux, etc. Elle est donc en réalité la raison d'être du cyberespace. Si les deux premières couches sont des couches techniques, la couche cognitive est celle de la valeur « sociale et intellectuelle », qui n'existe que grâce aux deux précédentes, mais qui constitue le cœur du cyberespace. C'est une couche par essence ouverte et globale, impossible à réguler totalement compte tenu de son étendue et de sa nature.

Sans même évoquer le *darkweb*, on estime ainsi qu'il existe plus d'1,8 milliard de sites Internet représentant plus de 4,5 milliards de pages, plus de 330 millions de noms de domaines enregistrés et que, chaque minute, 400 heures de vidéos sont téléchargées sur la plateforme YouTube, 216 millions de photos sont « aimées » sur Facebook ou encore que 350 000 tweets sont publiés sur Twitter.

L'ampleur de cette couche emporte mécaniquement un grand nombre de vulnérabilités associées, chaque élément constitutif pouvant être exploité, transformé, détourné par un acteur malveillant, ainsi que l'ont démontré les événements survenus à l'occasion de grands rendez-vous démocratiques récents : ainsi des cyberattaques subies par le *Democratic National Committee* lors de la campagne présidentielle américaine de 2016 [(1)], ou encore de celles qui ont ciblé le site Internet du mouvement En Marche ! lors de la campagne présidentielle française de 2017.

C'est sur la couche cognitive que se déploient l'information, mais également la désinformation, les activités de propagande ou encore les rumeurs et autres *fake news* dont l'actualité fournit quotidiennement des exemples, tels que l'exploitation non consentie de données dans le cadre des activités de conseil de la société Cambridge Analytica ou l'usage d'Internet et des réseaux sociaux par Daech. Il convient toutefois de rappeler que les fausses nouvelles ne sont pas nées avec Internet – on se souviendra à cet égard des fausses informations colportées

(1) Avec la divulgation de dizaines de milliers de courriels de l'équipe de campagne de la candidate démocrate Hillary Clinton.

s'agissant de l'absence de propagation du nuage de Tchernobyl au-delà de certaines frontières – mais leur diffusion par les canaux numériques en est accélérée et amplifiée.

Très schématiquement, on peut considérer que les actions menées sur la couche cognitive peuvent servir quatre buts distincts :

– la communication : il s'agit, classiquement, d'informer, de donner du sens, de convaincre ;

– la mystification : il s'agit là de tromper le public destinataire du message, de le désinformer ;

– l'aliénation : elle vise à « imposer du sens » par la pression et renvoie à toutes les activités de propagande, d'endoctrinement ou de subversion ;

– la protection : les actions menées sur la couche cognitive peuvent précisément chercher à contrer les deux buts précédents, grâce à des actions défensives de lutte contre la désinformation, de contre-propagande ou de contre-subversion.

Si les actions menées sur les couches physique et logicielle sont un phénomène relativement récent, celles menées sur la couche cognitive renvoient en définitive à des modes d'action classiques, mis en œuvre depuis des siècles tant par les États que par les entreprises ou les individus. En revanche, les caractéristiques des nouveaux réseaux de communication (étendue, facilité d'accès, vitesse de diffusion) induisent un véritable changement d'échelle qu'il convient de prendre en considération.

B. LES SPÉCIFICITÉS DU MILIEU CYBERNÉTIQUE COMME ESPACE DE CONFLITS, NOTAMMENT DU POINT DE VUE DE LA DÉFENSE NATIONALE

1. Un espace sans frontières, qui efface les distances et écrase le temps

a. Un espace global et unique

À l'exception notable de la couche physique, dont les éléments sont territorialement situés, le cyberespace est un espace qui ne connaît pas de frontières. Ainsi, il n'existe pas de cyberespace français, américain ou russe dont la violation constituerait une atteinte au même titre que la violation des frontières terrestres, de l'espace aérien national ou de la mer territoriale. Pour reprendre un terme militaire : il n'y a pas de front dans le cyberespace, ou alors il s'agit d'un front global.

Cela ne signifie pas que les actions menées dans et par le cyberespace ne peuvent pas produire d'*effets* géographiquement déterminés voire ciblés ; l'actualité en fournit des preuves presque quotidiennement. Mais l'espace cyber

pousse à l'extrême la disjonction entre, d'une part, la présence physique d'un acteur et le lieu de déclenchement de son action et, d'autre part, les effets d'une telle action.

Inversement, une attaque ciblée *a priori* peut, du fait de l'interconnexion des différents acteurs, également toucher une « victime collatérale ». Tel fut le cas pour la société française Saint-Gobain, victime indirecte mais bien réelle de la cyberattaque NotPetya qui avait ciblé l'économie ukrainienne en 2017. Le groupe français a été touché par le biais d'une filiale située dans ce pays, laquelle utilisait un logiciel de l'administration fiscale ukrainienne qui a servi de canal à la dissémination du virus. Cette attaque a produit des conséquences financières substantielles pour la société, estimées, selon les informations parues dans la presse, à hauteur de 80 millions d'euros sur son résultat d'exploitation et de près de 250 millions d'euros sur ses ventes.

Par ailleurs, le caractère transfrontière, global et abstrait du cyberespace offre une protection pour les auteurs d'actes malveillants. En effet, un attaquant physiquement situé dans un pays donné peut parfaitement déclencher son action à partir d'un équipement (serveur, par exemple) situé dans un pays tiers, voire effectuer de multiples « rebonds », afin précisément de masquer la véritable origine de l'attaque. Telle est notamment l'une des difficultés auxquelles se heurtent les autorités et services chargés d'attribuer une cyberattaque.

b. Un espace de conflit caractérisé par sa contraction et sa dilatation

Dans les milieux « classiques », les distances constituent des données dont la réalité s'impose à quiconque souhaite y agir. D'un point de vue militaire, les espaces terrestre, aérien et spatial se mesurent en centaines de kilomètres et les espaces maritimes en centaines de milles. Ceux qui planifient et mettent en œuvre les opérations conduites dans de tels espaces éprouvent concrètement la matérialité de ces distances et des conséquences qu'elles emportent sur les hommes et les matériels.

Dans le cyberespace, en revanche, se conjuguent les notions d'éloignement et de proximité. Éloignement car le cyberespace est un espace virtuel et dilaté, pour ainsi dire infini et par ailleurs en recomposition quasi permanente. Proximité car, comme cela a été rappelé, le cyberespace permet une disjonction totale entre le lieu de déclenchement d'une action et ses effets concrets. La distance physique entre adversaires perd de fait sa pertinence et ne constitue plus l'élément d'analyse qu'elle demeure dans les espaces « classiques ». Le cyberespace emporte donc une contraction du champ conflictuel.

De fait, en s'affranchissant de l'une des barrières les plus contraignantes qui soit – la distance, et donc le temps – l'attaquant dispose par hypothèse, dans le milieu cyber, d'un avantage stratégique non négligeable : l'effet de surprise. Toutes les stratégies mises en place dans le domaine cyber, qu'il s'agisse des mesures de protection et de détection ou des mesures plus « actives », visent

notamment à réduire cet avantage stratégique pour rééquilibrer la relation entre attaquant et défenseur.

c. La dimension temporelle du cyberespace : entre quasi-instantanéité et temps long

Le temps est un autre facteur classique déterminant dans le domaine stratégique s'agissant des espaces traditionnels de conflits. Là encore, le cyberespace s'en distingue puisque la dimension temporelle devient secondaire.

Au-delà des actions de préparation d'une approche, phase qui peut s'avérer particulièrement longue, une cyberattaque peut se caractériser par sa foudroyance. En une seule commande, en un « clic » de souris, un attaquant peut obtenir de manière quasi instantanée l'effet recherché : corruption d'un système par introduction d'un code ou d'un programme malveillant, défiguration (1) ou blocage d'un site, déni de service (2) (DoS), etc.

Toutefois, si la transmission des ordres informatiques se caractérise par sa rapidité extrême, l'action cybernétique peut également favoriser le temps long. Certaines formes de corruption de systèmes, notamment les bombes logiques, peuvent en réalité être présentes dans ces systèmes pendant une longue période avant d'être déclenchées ou de se déclencher, de manière automatique dès lors que certaines conditions sont réunies (mise en œuvre à une date préalablement fixée ou dès lors que le système infecté reçoit une commande spécifique, etc.).

Par ailleurs, les attaques informatiques – du moins les plus sophistiquées – nécessitent une phase de préparation parfois longue puisqu'il s'agit d'analyser de la manière la plus complète et la plus fine possible la cible. Ultérieurement, les phases d'intrusion au sein d'un système puis d'exploitation de celui-ci peuvent également nécessiter du temps, surtout si l'architecture du système visé est complexe. À titre d'exemple, la cyberattaque qui a touché TV5 Monde s'est déroulée sur près de trois mois, entre l'intrusion dans les réseaux de la chaîne et la production des effets de l'attaque (blocage des émissions).

Enfin, l'attaquant ne cherche pas systématiquement à conférer une publicité à son acte. En effet, l'efficacité de certaines atteintes repose au contraire sur le caractère indétectable de celles-ci. Tel est le cas des actions visant au vol de données : celles-ci doivent s'opérer sur une période de temps suffisamment longue pour acquérir l'ensemble des données ciblées, sans toutefois éveiller la méfiance de la victime de cette atteinte (ce qu'un « siphonnage » trop massif et trop rapide pourrait provoquer).

---

(1) Ou défacement.

(2) Attaque informatique ayant pour but et pour effet de rendre indisponible un service, d'empêcher ou de limiter fortement la capacité d'un système à fournir le service. Conduite à partir de plusieurs sources, on parle de déni de service distribué (DDoS).

2. Un certain nivellement des rapports de force permis par la relative facilité d'accès aux technologies cybernétiques et la dualité civile/militaire du milieu cyber

a. L'accès aux technologies cybernétiques est relativement ouvert

L'éventail des armes numériques est particulièrement étendu et hétérogène. Les plus complexes et celles dont le potentiel destructeur est le plus élevé ne sont naturellement pas à la portée du premier *hacker* venu. Par ailleurs, la mise en œuvre de cyberattaques d'une certaine ampleur suppose de hautes compétences matérielles et techniques nécessaires à l'évaluation préalable du système que l'attaquant envisage de cibler, voire la mobilisation de capacités que seules détiennent certaines organisations puissantes et complexes, États [(1)] ou entreprises.

Toutefois, force est de constater que s'il est relativement malaisé de se procurer les éléments traditionnels de l'exercice des conflits – les armes et matériels de guerre, compte tenu de l'existence de régimes nationaux et internationaux de régulation voire d'interdiction –, les technologies cyber restent relativement faciles d'accès y compris pour les individus, à la fois matériellement et financièrement. Par ailleurs, un programme malveillant ou des modalités d'action même « rustiques » mais répliquées des centaines de milliers de fois sur une vaste échelle au moment opportun peuvent produire des perturbations conséquentes.

De fait, la diffusion et l'utilisation de technologies et de modes d'action ni nécessairement complexes à mettre en œuvre ni nécessairement coûteux peuvent conduire à un certain nivellement et à une égalisation – qui reste relative – des rapports de force dans le cyberespace. De simples individus ou groupes d'individus, même s'ils sont par ailleurs susceptibles de bénéficier d'un soutien étatique, peuvent en effet faire peser une menace suffisamment sérieuse sur un État en perturbant la vie quotidienne de sa population. Ainsi, en mai 2017, le logiciel WannaCry, un « simple » rançongiciel [(2)] (*ransomware*) était parvenu à infecter plus de 300 000 ordinateurs, dans 150 pays. Victime de cette attaque, le service national de santé britannique (*National Health Servic* – NHS) avait été durement touché et le fonctionnement de certains services gravement affecté [(3)].

Enfin, il convient de souligner une spécificité des armes cyber par rapport aux armes « classiques ». Alors que les secondes se fondent sur des modèles produits en série, les premières sont souvent des modèles uniques, faits sur mesure en fonction des spécificités du système ciblé et des effets précis que l'attaquant

(1) Notamment les capacités de renseignement.

(2) Programme malveillant reçu par courriel ou mis à disposition sur un site Internet qui provoque le chiffrement de tous les fichiers d'un ordinateur (ainsi que des fichiers accessibles en écriture sur les dossiers partagés si l'ordinateur est connecté à un réseau informatique) et demande une rançon en échange du mot de passe de déchiffrement.

(3) Organisation du système d'ambulances et d'opérations chirurgicales, heureusement non critique.

cherche à obtenir. Ceci constitue donc une difficulté supplémentaire pour mener les actions d'analyse, de détection et de remédiation.

b. Une imbrication du civil et du militaire qui brouille la ligne de partage traditionnelle des conflits

● Le cyberespace se compose à titre principal d'éléments non militaires, qui dépendent d'individus et d'entreprises privées et publiques. Seuls quelques systèmes sont de nature exclusivement militaire ; on peut par exemple songer aux différents systèmes d'armes, aux systèmes de transmission, aux centres de commandement, etc.

De fait, dans le cyberespace, en cas de conflit, le rapport entre cibles civiles et militaires s'inverse puisque les premières représentent la « norme ». Elles sont, du reste, comparativement moins bien protégées que les secondes et constituent à cet égard des cibles de choix pour les attaquants.

Or même ciblées sur des éléments exclusivement civils, des atteintes peuvent mettre en danger le fonctionnement normal d'une société, voire la survie de la Nation, et ainsi constituer un acte d'agression inacceptable susceptible de déclencher une réponse de nature militaire, en fonction du degré de gravité de l'atteinte. Tel pourrait être le cas d'actes malveillants qui viseraient des secteurs d'importance vitale (transports, énergie, santé, par exemple). Par ailleurs, une attaque ciblant initialement des éléments civils mais non maîtrisée pourrait également affecter, par ricochet, des éléments militaires.

Le cyberespace génère donc une confusion entre les sphères civiles et militaires, à rebours de la pensée stratégique traditionnelle et des régimes juridiques applicables aux conflits, lesquels reposent sur une distinction claire – si ce n'est toujours respecté en pratique – entre ces deux champs. Si les atteintes portées à des éléments civils ne sont censées être qu'une exception dans le cadre des conflits « traditionnels », elles représentent la norme dans le cyberespace.

Le constat d'une telle imbrication entre éléments – ou cibles potentielles – civils et militaires n'est dès lors pas sans conséquence sur l'organisation et la nature de la réponse des pouvoirs publics nationaux, et sur les conditions d'application d'un certain nombre de régimes de droit international.

● Enfin, il faut souligner que le cyber constitue un champ où les technologies et les applications sont « tirées » par les usages individuels et les loisirs civils, domaines dans lesquels la sécurité est considérée comme accessoire ou, du moins, ne fait pas « nativement » l'objet de l'attention nécessaire. De fait, le champ de la sécurité/défense ne fait que profiter de ce qui est développé ailleurs, dans des champs civils, à rebours de ce que l'on avait pu constater jusqu'à un passé récent dans le domaine des technologies, avec un secteur de la défense moteur et dont les productions irriguaient par la suite les autres secteurs. Tel fut le cas pour Arpanet/Internet, initialement développé par la *Defense Advanced*

Research Projects Agency (DARPA), agence du *Department of Defense* américain.

3. L'enjeu central de l'attribution d'une cyberattaque

a. L'attribution claire d'un acte d'agression, condition préalable à la mise en œuvre d'une réponse coercitive adaptée et proportionnée

Dans le cadre d'un conflit classique opposant des acteurs étatiques ou non – mais identifiés comme prenant part à ce conflit – dans l'un ou plusieurs des quatre milieux physiques traditionnels, la mise en œuvre de moyens de coercition est clairement attribuée [(1)] et même le plus souvent officiellement revendiquée et assumée. Si elle ne l'est pas, les États disposent des capacités leur permettant d'opérer une telle attribution avec certitude, grâce à une analyse de l'action (degré de technicité de l'attaque, moyens et méthodes employés, victimes touchées, éventuelles raisons géopolitiques sous-jacentes, etc.) et à la conduite d'actions de renseignement, par exemple. En somme, dans un conflit classique, il est toujours possible d'attribuer la paternité d'un acte de coercition à un acteur déterminé et ce dans un délai raisonnable compatible avec la conduite d'une éventuelle action en réponse.

Pour faire usage de la force de manière légitime, adaptée et proportionnée à l'égard d'un agresseur, il convient d'avoir préalablement identifié cet agresseur et d'être en mesure de lui imputer de manière certaine l'acte qui justifie l'action de coercition exercée en retour.

b. Une capacité d'attribution singulièrement réduite dans le cyberespace

Or dans le cyberespace, l'attribution s'avère particulièrement difficile ce qui, par conséquent, complique singulièrement les capacités de réponse à une cyberattaque. Un tel constat s'explique par le fait que :

– les actions malveillantes menées dans le cyberespace font très rarement – voire jamais – l'objet d'une revendication par des acteurs identifiés, *a fortiori* des États. Si certains groupes de *hackers* sont bien connus [(2)], l'identité des individus qui les composent ne l'est pas et le soutien éventuel dont ils peuvent disposer de la part d'acteurs étatiques reste sujet à interprétation. Par ailleurs, l'attaquant originel, s'il peut être identifié, n'est pas nécessairement le commanditaire de l'action ;

– dans le cyberespace, rares sont les attaques directes déclenchées à partir d'un point A pour affecter immédiatement et sans détour un point B. Généralement, les auteurs d'actes malveillants dissimulent leurs actions – et donc le point de départ initial de l'action – en profitant du caractère totalement ouvert de ce milieu, de son absence de frontières et des multiples interconnexions qui en

(1) En dehors du cas des actions clandestines.
(2) Par exemple : Fancy Bear, Cozy Bear, *ou encore* Lazarus Group.

relient les différents éléments. Les cyberattaquants s'efforcent de faire « rebondir » leurs attaques de serveur en serveur et de pays en pays afin de « masquer leurs traces » et de soustraire l'origine exacte de l'attaque à tout regard extérieur ;

– au-delà des victimes expressément ciblées, une cyberattaque peut également affecter des victimes « collatérales », que l'attaquant ne cherchait pas spécifiquement à atteindre, compte tenu du degré d'interconnexion entre les différents acteurs du cyberespace ;

– le cyberespace offre à ses acteurs un degré d'anonymat sans équivalent et remonter la « chaîne d'anonymisation » représente un défi majeur. C'est d'autant plus vrai s'agissant des entités, groupes ou individus qui agissent non pas sur les réseaux ouverts, mais sur le *darkweb* (1), lequel regroupe l'ensemble des réseaux et sites entièrement cryptés, uniquement accessibles grâce à des logiciels, des configurations ou des autorisations d'accès spécifiques (2) ;

– les effets de certaines atteintes cyber peuvent se déclencher très longtemps après la pénétration effective d'un système. Tel est le cas des bombes logiques.

Sans attribution sûre à un agresseur clairement identifié, il semble compliqué d'invoquer la légitime défense ou les mécanismes de défense collective pour répondre directement à l'attaque subie. En revanche, ces mécanismes peuvent être actionnés pour obtenir la mise en commun des capacités des différents partenaires afin de parvenir à une attribution qui permettra ultérieurement la mise en œuvre d'une réponse opérationnelle adaptée et proportionnée. Mais en l'absence d'adversaire expressément identifié en tant que responsable d'une agression, nulle réponse contre celui-ci ne peut être envisagée.

Il convient toutefois de souligner qu'au-delà des aspects purement techniques, la décision d'attribuer une cyberattaque relève en dernière analyse d'une appréciation et donc d'une décision de nature politique. Plutôt que sur des certitudes absolues et des preuves irréfutables, une telle décision s'appuie sur un niveau suffisamment bas d'incertitudes, sur un faisceau d'indices à la lumière desquels l'autorité politique prend, le cas échéant, la responsabilité d'attribuer un acte. Il importe de rappeler qu'à ce stade et contrairement à d'autres pays – États–Unis, Royaume–Uni par exemple –, la France n'attribue jamais officiellement et publiquement les cyberattaques qui pourraient la cibler.

Un responsable opérationnel auditionné par les rapporteurs l'a exprimé, sous forme de boutade : le nombre de cas où une cyberattaque peut être attribuée avec une certitude absolue est quasiment nul, mais le nombre de cas où l'on ignore

---

(1) À ne pas confondre avec le deepweb*, qui désigne la partie du web accessible en ligne mais non indexée par les moteurs de recherche classiques. Y figurent des sites parfaitement légitimes et légaux (intranet, serveurs privés, bases de données de ligne, etc.).*

(2) Par exemple via *les réseaux Tor (*The Onion Router*), I2P (*Invisible Internet Project*), ou encore Freenet.*

totalement qui est à l'origine de l'attaque est quasiment nul également. Un autre l'a présenté ainsi : « *en matière cyber, il n'y a pas de* smoking gun ».

Le cyberespace empêche de « voir » distinctement son adversaire. Si l'anonymat n'y est pas absolu – aucune protection ne l'est réellement – et si toute action numérique peut techniquement finir par être tracée, les délais nécessaires pour lever cet anonymat et obtenir la parfaite traçabilité d'une action – parfois plusieurs mois ou années – peuvent s'avérer incompatibles avec la conduite d'une action de représailles, qui, par nature, doit être menée rapidement après l'acte initial d'agression.

4. L'inadaptation partielle des principaux mécanismes de défense individuelle et collective prévus par les droits international et européen

a. L'article 51 de la Charte des Nations unies : le droit à la légitime défense

À la suite des travaux menés au sein de l'Organisation des Nations unies (ONU), la France reconnaît depuis 2013 l'applicabilité du droit international existant et de la Charte des Nations unies, tant en matière de légitime défense que s'agissant du recours à des contre-mesures. Cette position, clairement exprimée dans le Livre blanc de 2013, est depuis régulièrement confirmée : par la Stratégie nationale pour la sécurité du numérique de 2015 et, encore récemment, par M. Jean-Yves Le Drian, ministre de l'Europe et des Affaires étrangères, lors de la présentation de la Stratégie internationale de la France pour le numérique le 15 décembre 2017 à Aix–en–Provence.

À cette occasion, évoquant les possibilités offertes aux États en réponse à un fait illicite commis à leur encontre, M. Le Drian a ainsi déclaré : « *Je pense également à la capacité, de chaque État, dans les cas où une attaque informatique serait constitutive d'une menace contre la paix et la sécurité internationales, de saisir le Conseil de sécurité des Nations unies, au titre des chapitres VI* (1) *ou VII* (2)*, de la Charte des Nations unies. De plus, sous réserve d'une appréciation des circonstances d'espèce, une attaque informatique majeure pourrait constituer une agression armée au sens de l'article 51 de la Charte des Nations unies et ouvrirait dès lors la possibilité d'invoquer le droit de légitime défense* (3)*, dans l'attente d'une décision du Conseil de sécurité.* »

(1) Règlement pacifique des différends.
(2) Action en cas de menace contre la paix, de rupture de la paix et d'actes d'agression.
(3) Souligné par les rapporteurs.

L'article 51 de la Charte des Nations unies

Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales. Les mesures prises par des Membres dans l'exercice de ce droit de légitime défense sont immédiatement portées à la connaissance du Conseil de sécurité et n'affectent en rien le pouvoir et le devoir qu'a le Conseil, en vertu de la présente Charte, d'agir à tout moment de la manière qu'il juge nécessaire pour maintenir ou rétablir la paix et la sécurité internationales.

b. L'article 5 du traité de l'Atlantique Nord : clause d'assistance mutuelle entre les membres de l'OTAN

L'article 5 du traité de l'Atlantique Nord est souvent considéré comme le cœur du dispositif de sécurité collective que symbolise l'OTAN. En vertu de cet article, toute attaque armée dirigée contre un ou plusieurs États parties au traité est considérée comme une attaque dirigée contre l'ensemble des parties, soit 29 États à l'heure actuelle.

Dans la même déclaration que celle précédemment évoquée, M. Le Drian affirmait que « *Si elle était dirigée contre un membre de l'OTAN, [une attaque informatique majeure] pourrait de même donner lieu à l'invocation et à la pleine application de la clause de solidarité de l'article 5 du traité de l'Atlantique-Nord.* »

L'article 5 du traité de l'Atlantique Nord

Les parties conviennent qu'une attaque armée contre l'une ou plusieurs d'entre elles survenant en Europe ou en Amérique du Nord sera considérée comme une attaque dirigée contre toutes les parties, et en conséquence elles conviennent que, si une telle attaque se produit, chacune d'elles, dans l'exercice du droit de légitime défense, individuelle ou collective, reconnu par l'article 51 de la Charte des Nations unies, assistera la partie ou les parties ainsi attaquées en prenant aussitôt, individuellement et d'accord avec les autres parties, telle action qu'elle jugera nécessaire, y compris l'emploi de la force armée, pour rétablir et assurer la sécurité dans la région de l'Atlantique Nord.

Toute attaque armée de cette nature et toute mesure prise en conséquence seront immédiatement portées à la connaissance du Conseil de Sécurité. Ces mesures prendront fin quand le Conseil de Sécurité aura pris les mesures nécessaires pour rétablir et maintenir la paix et la sécurité internationales.

c. L'article 42-7 du traité sur l'Union européenne : clause d'assistance mutuelle entre les États-membres de l'UE

L'article 42-7 du traité sur l'Union européenne prévoit qu'en cas d'agression armée subie par un État membre sur son territoire, les autres États membres lui doivent « *aide et assistance par tous les moyens en leur pouvoir* », étant entendu que ce mécanisme s'inscrit dans le respect et dans le cadre des engagements souscrits par ces États au titre de la Charte des Nations unies et du traité de l'Atlantique Nord.

À ce jour, ce mécanisme d'assistance mutuelle au niveau européen n'a été activé qu'une seule fois, à l'initiative de la France, à la suite des attentats du 13 novembre 2015.

L'article 42-7 du traité sur l'Union européenne

Article 42

[…]

7. Au cas où un État membre serait l'objet d'une agression armée sur son territoire, les autres États membres lui doivent aide et assistance par tous les moyens en leur pouvoir, conformément à l'article 51 de la charte des Nations unies. Cela n'affecte pas le caractère spécifique de la politique de sécurité et de défense de certains États membres.

Les engagements et la coopération dans ce domaine demeurent conformes aux engagements souscrits au sein de l'Organisation du traité de l'Atlantique Nord, qui reste, pour les États qui en sont membres, le fondement de leur défense collective et l'instance de sa mise en œuvre.

d. Une applicabilité qui demeure incertaine dans l'hypothèse d'atteintes cyber

Dans la pratique, les régimes de droit international et européen prévoyant des mécanismes de légitime défense ou d'assistance en cas d'agression sont d'application complexe dans le cyberespace.

● La difficulté de parvenir à un consensus international

Depuis 2004 un groupe d'experts gouvernementaux (*Group of Governmental Experts* – GGE) représentant 15, puis 20 États (après 2014), se réunit à intervalles réguliers dans le cadre de l'ONU afin de définir des recommandations visant à renforcer la sécurité internationale du cyberespace. À la suite de nombreux échecs mais après une première avancée en 2013, avec la reconnaissance générale de l'application du droit international au cyberespace, le GGE a précisé sa position en 2015 en reconnaissant que s'appliquaient au cyberespace, d'une part, les principes d'interdiction du recours à la force et de règlement pacifique des différends et, d'autre part, les principes du droit des conflits armés : *jus ad bellum* (1) et *jus in bello* (2).

Mais en 2016, la Russie, la Chine et Cuba mettent fin à ce processus, pourtant initialement soutenu par la première, et quittent le GGE. Cela ne signifie toutefois pas nécessairement que ces États souhaitent remettre en cause intégralement les travaux du GGE. Il n'en demeure pas moins qu'un tel retrait en suspend *de facto* les travaux.

Par ailleurs, en écho à ce retrait, certains États ont plaidé pour une poursuite des négociations entre « *like-minded states* », soit des États partageant la

(1) « Droit à la guerre », soit l'ensemble des critères y autorisant le recours, telle la légitime défense.

(2) « Droit dans la guerre », soit le droit international humanitaire qui réglemente la manière dont la guerre est conduite.

même philosophie en la matière. La pertinence d'une telle démarche paraît singulièrement limitée puisqu'elle aurait pour conséquence une différenciation du droit international, alors qu'il s'agit au contraire de parvenir à un corpus unanimement partagé.

● La détermination des critères susceptibles de qualifier une cyberattaque comme une « agression armée » [(1)] ou « attaque armée » [(2)]

À ce jour, il apparaît que la plupart des attaques demeurent sous le seuil autorisant « l'usage de la force », du moins au regard des régimes précédemment décrits. De fait, même la cyberattaque d'ampleur menée contre l'Estonie en 2007, qui reste probablement l'atteinte la plus massive jamais conduite à l'encontre d'un État [(3)], n'a pas entraîné la mise en œuvre de l'article 5 du traité de l'Atlantique Nord.

● La question lancinante de l'attribution

Sans revenir sur un aspect qui a déjà été présenté dans le détail, il faut souligner à nouveau la difficulté extrême qu'éprouvent les États dans l'attribution des cyberattaques.

Ainsi, les délais nécessaires à l'analyse et *in fine* à une éventuelle attribution semblent peu compatibles notamment avec la mise en œuvre d'actions reposant sur la légitime défense. Ce concept repose en effet sur trois critères : la nécessité, la proportionnalité et l'immédiateté. Si les deux premiers ne posent pas de difficulté particulière, le dernier s'avère en revanche problématique dès lors que l'attribution définitive d'une cyberattaque ne pourra survenir – si elle se produit – qu'après un laps de temps particulièrement long, plus long en tout état de cause que dans l'hypothèse de l'utilisation de moyens coercitifs traditionnels.

S'agissant du mécanisme automatique d'assistance collective prévu par l'article 5 du traité de l'Atlantique Nord, il convient de souligner que celui-ci ne pourrait être mis en œuvre que si, au préalable, les États concernés partagent la même position quant à l'attribution d'une cyberattaque. Or, si l'attribution constitue déjà un processus complexe lorsqu'il est mené par un État seul, que penser d'un éventuelle « co-attribution » qui devrait être commune à quelque 29 États ? C'est pourquoi la prudence semble de mise quant à l'application de cet article suite à une cyberattaque. Toutefois, un État victime pourrait demander l'assistance de ses alliés sur la base de l'article 5 non pour répondre directement à la cyberattaque – ce qui supposerait une attribution « partagée » en amont –, mais précisément pour l'aider à déterminer l'auteur de cette attaque.

(1) Article 51 de la Charte des Nations unies et article 42-7 du traité sur l'Union européenne.
(2) Article 5 du traité de l'Atlantique Nord.
(3) Avec les cyberattaques ayant touché l'Ukraine en 2017.

C. L'ÉTAT ET L'ÉVOLUTION DES RISQUES ET DES MENACES CYBER

1. Une vulnérabilité accrue des sociétés à la menace cyber, qui va se renforcer

a. Une élévation constante du niveau de menace

La problématique cyber n'est pas nouvelle : ainsi les premières attaques informatiques, dénommées *Titan Rain*, ont-elles été menées il y a 15 ans, en 2003, et avaient pris pour cible des systèmes d'information américains.

Toutefois, et la récente Revue stratégique de cyberdéfense publiée par le SGDSN l'a rappelé, la menace d'origine cyber se renforce à deux égards :

– quantitativement : avec, d'une part, la multiplication du nombre d'acteurs en mesure de conduire des attaques et, d'autre part, une certaine prolifération, voire une « banalisation » des capacités susceptibles d'être mises en œuvre pour perpétrer des actes malveillants dans ou *via* le cyberespace ;

– qualitativement : avec l'accroissement des capacités offensives de certains États. Au-delà des « grands États » du milieu cyber auxquels on songe spontanément, il convient de souligner qu'au cours de la décennie passée, une quarantaine d'États a cherché à développer des capacités cyber-offensives, dont des pays tels que le Bangladesh, le Soudan, ou encore le Vietnam. Toutefois, ces capacités ont des finalités parfois différentes de celles poursuivies par les acteurs majeurs du cyber (notamment, elles sont souvent « à usage interne » : ciblage de dissidents, par exemple).

Un tel constat traduit dès lors une élévation globale du niveau de dangerosité des cyber-menaces.

Ce renforcement de la menace est notamment symbolisé par la consécration de la notion d'*Advanced Persistent Threat* (APT – menace persistante avancée). Celle-ci est révélatrice de la professionnalisation et de la structuration des cyber–attaquants caractérisant les groupes dont les compétences et les ressources importantes leur permettent de mener des attaques sophistiquées. Un nombre est apposé pour identifier les différents APT, en fonction de leur date d'identification. Tel est le cas du groupe APT28, plus connu sous le nom de *Fancy Bear* [(1)], auquel des sources ouvertes attribuent les cyberattaques qui ont affecté TV5 Monde. Certains APT sont tenus pour être de simples intermédiaires d'États souhaitant masquer leurs actions dans le cyberespace. Tel est le cas, si l'on en croit certains articles de presse et sources ouvertes, du même groupe APT28, par ailleurs impliqué dans les cyberattaques ayant ciblé le *Democratic National Committee* américain en 2016 et réputé proche des services de renseignement russes, ainsi que du groupe *Cozy Bear* [(2)] (APT29).

(1) Également connu sous les dénominations suivantes : Pawn Storm, Sofacy Group, Sednit *et* STRONTIUM.
(2) Également connu sous les dénominations suivantes : Office Monkeys, The Dukes.

Il convient par ailleurs de souligner que le cyberespace agit comme un catalyseur, comme un « multiplicateur d'effet ». Ainsi, des actes de cybercriminalité « traditionnelle » peuvent, au-delà de leurs conséquences immédiates, produire des effets majeurs – directs ou indirects – en matière de défense, de sécurité nationale et de continuité des services et activités essentiels à la vie de la Nation, que ces effets soient d'ailleurs recherchés ou non par les auteurs de tels actes. La numérisation de plus en plus poussée de nos sociétés y contribue évidemment.

b. La numérisation et l'interconnexion des sociétés, sources de faiblesses cyber nouvelles et plus nombreuses

Le processus de numérisation croissant et continu des sociétés contemporaines induit une vulnérabilité de plus en plus forte aux menaces cybernétiques, cette vulnérabilité étant en outre renforcée du fait de l'interconnexion de plus en plus poussée de l'ensemble des activités sociales. En effet, il n'est sans doute pas exagéré d'affirmer que, dorénavant, aucun champ de l'activité humaine n'échappe au numérique. La fertilité de l'imagination humaine aura pour conséquence d'accroître cette emprise du numérique à l'avenir ; songeons par exemple aux villes intelligentes (*smart cities*), à l'usine 4.0, au développement des modes de transport autonomes, y compris individuels, à l'e-santé, à l'importance prise par les réseaux sociaux et les applications numériques [(1)], au recours à l'intelligence artificielle ou encore à la croissance exponentielle du nombre d'objets connectés [(2)].

Les armées ne sont évidemment pas étrangères à ce mouvement, qu'elles accompagnent, voire qu'elles suscitent, ainsi qu'en témoigne leur numérisation croissante ainsi que celle de l'environnement de combat, une dynamique porteuse de nombre d'enjeux structurants à l'avenir. D'ailleurs, la commission de la Défense a créé une autre mission d'information relative aux enjeux de la numérisation dans les armées, confiée à MM. Olivier Becht et Thomas Gassilloud, dont les analyses sont particulièrement éclairantes [(3)].

En somme, l'individu, dans toutes ses composantes (acteur social, économique, citoyenne, citoyen) et à tous les stades de sa vie dépend du numérique au quotidien. Tel est également le cas des organisations et, naturellement, des États (ministères, collectivités locales, services publics, etc.).

De fait, et sans verser dans une forme de fantasme ou de paranoïa stérile, la conjonction de ces différents facteurs conduit à considérer que les actions malveillantes menées dans et *via* le cyberespace sont potentiellement porteuses de réels risques systémiques pour nos sociétés.

---

(1) À titre d'exemple, selon les informations récemment parues dans la presse, l'application Strava, qui met en ligne les parcours géolocalisés de ses utilisateurs, aurait permis par déduction de localiser des bases militaires et des mouvements de troupes.

(2) Nombre estimé à plusieurs dizaines de milliards à l'horizon 2020.

(3) Rapport d'information n° 996 de MM. Olivier Becht et Thomas Gassilloud sur les enjeux de la numérisation des armées, Assemblée nationale, XV^e^ législature.

2. Une menace polymorphe, de nature classique mais aux effets démultipliés

Les développements qui suivent n'ont naturellement pas vocation à détailler l'ensemble des menaces susceptibles d'affecter l'ensemble des cibles potentielles d'une cyberattaque. Ils visent à fournir une typologie des principaux types de menaces en fonction de leur nature, et de leurs principaux vecteurs (du moins ceux qui sont connus). Cette typologie tend à démontrer que, si le cyberespace représente un milieu nouveau à l'intérieur et à partir duquel des actes malveillants peuvent être perpétrés, la *nature* de ces actions reste somme toute classique et que celles-ci sont entreprises depuis toujours, notamment par les acteurs étatiques.

Le cyberespace et les technologies associées leur ont toutefois ouvert de nouveaux horizons et modes d'action et permettent potentiellement d'en démultiplier les effets en leur conférant une ampleur inédite, compte tenu des caractéristiques, évoquées plus haut, du cyberespace et des sociétés contemporaines.

Pour reprendre la distinction précédemment opérée, on notera que les menaces cyber sont majoritairement menées dans la couche logique du cyberespace, les actions de déstabilisation concernant également la couche cognitive, sans oublier la couche physique que sont notamment les câbles et les cœurs de réseau, un dispositif considéré comme particulièrement vulnérable.

a. L'espionnage

L'espionnage constitue la « menace historique » et l'ensemble des États y recourent largement. Toutefois, du fait de la diffusion croissante des technologies les États ne disposent pas, loin s'en faut, du monopole de l'espionnage informatique. On peut notamment songer aux actes d'espionnage industriel réalisés par certains des acteurs économiques.

Depuis une quinzaine d'années la France et les entreprises françaises ont régulièrement été la cible d'actes d'espionnage informatique. Selon les termes de la Revue stratégique de cyberdéfense, « *les attaques informatiques conduites à des fins d'espionnage demeurent une problématique de premier plan. D'une sophistication croissante, elles constituent le plus grand nombre des offensives majeures ayant affecté notre pays ces dernières années. Elles sont aussi en France à l'origine des principales opérations de cyberdéfense conduites par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour les contrer.* »

L'espionnage informatique présente la caractéristique d'être extrêmement difficile à mesurer en termes de conséquences. Il est parfois faussement « indolore », puisque ses effets peuvent ne pas se révéler immédiatement après la commission de l'acte même d'espionnage. Il peut donc s'avérer à la fois très efficace et très difficilement attribuable.

b. Le sabotage

Le sabotage constituait une menace encore théorique il y a une dizaine d'années. Trois événements ont modifié les perceptions à ce sujet, en démontrant que les effets de cyberattaques, loin de se cantonner au seul champ numérique, pouvaient être durement ressentis dans le monde physique :

– la cyberattaque massive subie par l'Estonie en 2007 qui, en s'appuyant sur le déni de service distribué (DDoS) a partiellement paralysé le pays (sites gouvernementaux, médias, secteur bancaire, etc.) ;

– l'attaque Stuxnet, réalisée en 2010 et qui a affecté les sites nucléaires iraniens (notamment le site de Natanz) *via* leurs systèmes de contrôle et de supervision ;

– et l'attaque qui a visé la chaîne TV5 Monde en 2015, laquelle a constitué le premier acte de sabotage informatique ciblant des intérêts français. Les auteurs de l'attaque se seraient introduits dans le réseau interne de la chaîne en passant par un réseau virtuel privé (VPN) et en utilisant les identifiants et mots de passe d'un de ses sous-traitants.

Les actes de sabotage informatique ont tendance à se multiplier ce qui, du point de vue des pouvoirs publics, constitue un motif d'inquiétude face à une forme de « désinhibition » quant à l'utilisation de l'arme cyber, celle-ci produisant, du moins « facialement » des conséquences moindres que l'utilisation d'une arme cinétique « classique ». La Revue stratégique de cyberdéfense considère d'ailleurs que le sabotage informatique « *représente la menace la plus préoccupante* ».

c. La déstabilisation

La déstabilisation et la désinformation sont des menaces anciennes, qui ont toujours existé dans le domaine des relations interétatiques sous le terme classique de « propagande », dans ses différents degrés. Toutefois le cyber accélère, catalyse et démultiplie les effets des actions conduites dans ces domaines, notamment en raison du développement d'Internet et des réseaux sociaux, ces derniers constituant autant de caisses de résonance par nature impossibles à réguler totalement.

Alors qu'Internet et les réseaux sociaux jouissaient, non sans raison, d'un *a priori* positif en tant qu'espaces de liberté, de connaissance, d'échange et de communication, la perception publique et sociale a progressivement évolué ces dernières années, notamment à la faveur du retour de la menace terroriste sur la scène internationale et des soupçons de manœuvres déstabilisatrices qui ont entouré certains scrutins (élections présidentielles américaine et française et *Brexit* notamment). Le cyberespace est en effet devenu l'un des principaux outils de

propagande pour toutes les idéologies extrémistes et est largement utilisé par les groupes terroristes au premier rang desquels Daech, pour n'évoquer que celui-ci [1].

Par ailleurs, rumeurs, contre-vérités, théories du complot et autres *fake news* fleurissent dans le monde numérique, à tel point que se pose de plus en plus régulièrement la question de la responsabilité des réseaux sociaux et des hébergeurs dans la diffusion de certains contenus. Certains phénomènes ont pris une ampleur telle qu'ils sont accusés d'avoir gravement perturbé le déroulement de plusieurs scrutins importants récemment tenus au sein de pays démocratiques et d'en avoir affecté la sincérité, voire l'issue.

d. La cybercriminalité

Même si elle est moins directement liée aux enjeux de défense nationale, qui constituent l'objet principal du présent rapport, et qu'elle concerne au premier chef les forces de sécurité intérieure et non les armées, il convient néanmoins d'évoquer le cas de la cybercriminalité, comprise comme l'ensemble des actions illégales reposant sur l'utilisation des réseaux pour perpétrer crimes et délits (vols, rançonnage, usurpation d'identité, ventes en ligne de produits illégaux, diffusion de contenus illicites, voire, dans l'hypothèse d'atteinte aux personnes, prise de contrôle de dispositifs ou d'équipements médicaux).

En effet, depuis quelques années, la frontière entre la lutte contre la cybercriminalité et les objectifs poursuivis en matière de cyberdéfense a tendance à s'effacer. Tout d'abord, les groupes cybercriminels se sont renforcés et se sont professionnalisés, et les attaques qu'ils mènent peuvent être d'une telle ampleur qu'elles peuvent produire des effets systémiques au-delà de leur caractère purement délictuel ou criminel. De fait, le cyber permet d'automatiser la criminalité à grande échelle et d'en démultiplier les effets. Il permet de réaliser des gains phénoménaux au regard de la modicité des investissements consentis pour perpétrer une attaque. Par ailleurs, le degré de sophistication et, encore une fois, l'ampleur de certaines attaques laissent à penser que les actes perpétrés ne sont peut-être pas exclusivement le fait de réseaux criminels « classiques » mais aussi, possiblement, d'acteurs étatiques, les premiers pouvant agir en tant qu'intermédiaires des seconds.

La norme de référence en matière de lutte contre la cybercriminalité est la convention de Budapest sur la cybercriminalité [2], l'efficacité de cet instrument de droit international étant naturellement fonction de l'état des ratifications. D'autres

---

(1) Cf. rapport d'information de MM. Kader Arif (rapporteur) et Jean-Frédéric Poisson (président) sur les moyens de Daech (Assemblée nationale, rapport n° 3964, juillet 2016, XIVe législature) et rapport d'enquête de MM. Patrick Mennucci (rapporteur) et Éric Ciotti (président) fait au nom de la commission d'enquête sur la surveillance des filières et des individus djihadistes (Assemblée nationale, rapport n° 2828, juin 2015, XIVe législature).

(2) Convention du 23 novembre 2001, approuvée par la France par la loi n° 2005-493 du 19 mai 2005 autorisant l'approbation de la convention sur la cybercriminalité et du protocole additionnel à cette convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

mécanismes existent par ailleurs au niveau d'Europol et d'Interpol. Eurojust permet également aux différents parquets nationaux de coordonner leur action.

e. Quelques cas d'école : Stuxnet, WannaCry, NotPetya

● Le ver [(1)] Stuxnet constitue une « référence » dans le domaine des cyberattaques. Conçu à des fins de sabotage, il a exploité quatre vulnérabilités *zero-day* du système d'exploitation Windows afin de compromettre le fonctionnement de certains sites nucléaires iraniens. Certains en attribuent la paternité aux États-Unis et à Israël, dans le cadre de l'opération dite *Olympic Games*.

Stuxnet permet d'illustrer certaines des caractéristiques précédemment évoquées s'agissant des actions menées dans le cyberespace :

– la conjonction entre la quasi-instantanéité et le temps long : on estime que l'élaboration de Stuxnet a nécessité trois ans, entre 2006 et 2009, ce qui témoigne de l'importance des actions de préparation des cyberattaques dès lors qu'elles revêtent une certaine ampleur ou visent des cibles complexes. Par ailleurs, contrairement à ce que l'on observe en cas d'emploi d'armes cinétiques classiques, Stuxnet illustre la disjonction que permet le cyberespace entre l'action et l'effet (du moins la prise de conscience de l'effet). Ainsi, alors que l'action de déclencher une frappe *via* un missile produit des effets immédiatement observables, Stuxnet a été détecté un an après avoir effectivement infecté sa cible ;

– l'interconnexion des acteurs qui conduit à une imparfaite maîtrise des effets : si des infrastructures iraniennes étaient spécifiquement visées, Stuxnet a également touché l'Inde et l'Indonésie ;

– le relatif anonymat, compliquant la capacité d'attribution d'une cyberattaque : si certains États sont suspectés d'avoir conçu et exploité Stuxnet, l'attaque n'a jamais été officiellement reconnue ni revendiquée et n'a jamais été officiellement attribuée ;

– la disproportion entre la « taille » de l'arme et ses effets : on estime que Stuxnet « pèse » entre 500 Ko et 1 Mo selon les versions, soit l'équivalent d'une simple photographie numérique de qualité raisonnable.

● Lancée en mai 2017, la cyberattaque utilisant le *ransomware* WannaCry a conduit à l'infection de plus de 300 000 ordinateurs dans 150 pays. De grandes administrations et de grandes entreprises ont été touchées, à l'image du *National Heatlh Service* britannique, du constructeur automobile français Renault, de la compagnie américaine de transport international FedEx ou encore de l'entreprise de télécommunications espagnole Telefónica.

(1) Code malveillant auto-répliquant se propageant de manière autonome (sans intervention humaine) ou quasi-autonome via *les réseaux.*

● Ayant massivement affecté l'économie ukrainienne mais aussi la centrale de Tchernobyl, le logiciel NotPetya a également touché, par ricochet, des entreprises disposant de filiales dans ce pays ou y entretenant des liens commerciaux. Ainsi du groupe danois de transport maritime Maersk, du groupe industriel français Saint-Gobain ou encore du groupe de communication et de publicité britannique WPP. NotPetya a infecté ses victimes *via* une mise à jour piégée du logiciel de comptabilité MEDoc qui équipait de nombreuses entreprises ukrainiennes.

● Le schéma de déroulement d'une cyberattaque

Les rappels qui suivent s'inspirent très largement de la présentation figurant dans la Revue stratégique de cyberdéfense. Schématiquement, une cyberattaque se structure en quatre phases :

– la reconnaissance de la cible : cette phase est celle du travail préparatoire au lancement de la cyberattaque. Il s'agit d'analyser les systèmes de la cible, leur organisation et les technologies utilisées afin d'en avoir la connaissance la plus fine possible dans le but de pénétrer la cible de la manière la plus efficace ;

– la pénétration du système informatique de la cible : elle s'opère en exploitant les vulnérabilités du système.

– l'installation d'implants et l'extension de la prise de contrôle : les implants sont des codes malveillants utilisés par le cyber-attaquant pour, d'une part, se maintenir et évoluer dans le système qu'il a pénétré et, d'autre part, produire par la suite les effets recherchés (exfiltration de données, par exemple). L'attaquant peut également chercher à étendre son contrôle sur le système en se propageant au sein du réseau (processus dit de latéralisation) ;

– l'exploitation du système infecté : l'attaquant déclenche les implants préalablement installés pour atteindre ses objectifs (vol de données, sabotage, etc.).

II. L'ORGANISATION DE LA CYBERDÉFENSE : DES CONCEPTIONS VARIÉES

A. LE MODÈLE FRANÇAIS : ACTEURS, MOYENS, MISSIONS

Puisque le cyber est partout et irrigue tous les champs de l'activité humaine, chacun – individus, entreprises, collectivités, État – « fait » de la cybersécurité et participe, même indirectement, à la cyberdéfense. Les développements qui suivent n'ont donc pas vocation à présenter l'ensemble des acteurs, publics ou privés, responsables à un niveau ou à un autre, mais l'architecture générale du système français et ses principaux intervenants, spécifiquement au travers du prisme de la défense nationale.

Il convient toutefois de souligner les limites d'un tel exercice. Quiconque s'intéresse aux enjeux de cyberdéfense se heurte rapidement aux contraintes de confidentialité, nombre d'éléments étant couverts par le secret de la défense nationale. Tel sera le cas notamment le cas s'agissant des développements relatifs aux services relevant de la communauté du renseignement : direction générale de la sécurité extérieure (DGSE), direction générale de la sécurité intérieure (DGSI) et direction du renseignement et de la sécurité de la Défense (DRSD).

1. Un système dual de séparation entre le défensif et l'offensif

● Globalement, s'agissant de l'organisation et de la gouvernance de la cyberdéfense, la France a fait le choix d'un système dual, séparant strictement les capacités et missions défensives et les capacités et missions offensives. L'Allemagne a opéré un choix similaire.

Le modèle français repose sur quatre acteurs principaux qui forment en quelque sorte le « premier cercle » de la cyberdéfense :

– l'ANSSI est responsable de la cyber-protection et de la lutte informatique défensive (LID) de l'État, des OIV et des opérateurs de services essentiels ;

– par délégation, le commandement cyber (COMCYBER) est chargé de la LID au sein du ministère des Armées, compte tenu de ses spécificités et de celles de ses réseaux. Il peut mener des actions, y compris actives, afin de les protéger. En outre, le COMCYBER peut également conduire des opérations dans l'espace numérique, dont des actions de lutte informatique offensive (LIO), mais uniquement dans le champ et dans le cadre d'opérations militaires. De fait, par exception à la philosophie générale du système français, le COMCYBER cumule bien capacités défensives et offensives, mais dans un domaine très spécifique et très restreint, et ce de manière parfaitement logique et légitime ;

– les services spécialisés, la DGSE et la DGSI, mènent quant à eux, chacun dans leur champ de compétence, des actions de renseignement et participent à la

prévention, voire à l'attribution des cyberattaques (la DGSE pouvant par ailleurs mener des actions clandestines, dans le domaine cyber comme dans les autres).

Il convient également d'évoquer un autre maillon de cette « chaîne cyber » : le maillon judiciaire, qui comprend l'action de la police, de la gendarmerie et de la justice et qui est chargé des investigations dans ce domaine.

Selon la nomenclature proposée par la Revue stratégique de cyberdéfense, les six missions de la cyberdéfense française sont les suivantes : prévention, anticipation, protection, détection, attribution, réaction (actions de remédiation technique, répression des infractions, actions militaires).

● L'autre modèle en vigueur est le modèle anglo-saxon, avec un système totalement intégré où l'ensemble des actions, défensives comme offensives, sont mises en œuvre par la communauté du renseignement. Ainsi, au Royaume-Uni, ces actions relèvent du *Government Communications Headquarters* (GCHQ) et, aux États-Unis, de la *National Security Agency* (NSA).

De manière très classique, chaque modèle présente des avantages et des inconvénients, du moins des limites qu'il s'agit de corriger. En extrayant les capacités défensives de la communauté du renseignement, le modèle dual rend les interventions des pouvoirs publics plus acceptables par la société et facilite sans doute l'établissement de relations de confiance entre les autorités publiques et l'ensemble des acteurs privés concernés par ces enjeux (partie des OIV, opérateurs de télécommunications, par exemple). De fait, un tel système paraît davantage garantir les libertés individuelles et la protection de la vie privée.

Toutefois, une telle dualité nécessite d'assurer une coordination très forte entre des « pôles » défensif et offensif qui ne partagent pas la même structure et ne sont pas soumis à la même autorité directe. Or le cyberespace nécessite souvent d'agir ou de réagir rapidement, et de manière coordonnée.

En négatif, le modèle intégré présente les avantages et limites inverses : grandes coordination et fluidité d'un côté ; acceptabilité et relations avec les acteurs privés moins évidentes de l'autre, du fait notamment de soupçons quant au respect des droits et libertés individuels s'agissant d'actions menées par des services de la communauté du renseignement.

2. L'ANSSI : autorité civile tête de réseau de la cyberdéfense pour les autorités publiques, les OIV et les opérateurs de services essentiels

a. Les missions de l'ANSSI

● L'Autorité nationale de la sécurité des systèmes d'information est une entité relativement récente, créée il y a moins de dix ans sous la forme d'un

service à compétence nationale [1]. Elle est rattachée au SGDSN, lui-même directement rattaché au Premier ministre qu'il assiste dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

En application de l'article L. 2321-1 du code de la défense [2], la définition et la coordination de l'action gouvernementale en matière de sécurité et de défense des systèmes d'information relèvent de la compétence du Premier ministre, celui-ci disposant 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 et des opérateurs de services essentiels, auprès desquels elle exerce par ailleurs une mission de conseil et de soutien. Elle a ainsi notamment vocation à intervenir au niveau technique en cas d'attaque affectant ces acteurs, en participant à la restauration des systèmes compromis et en mettant en œuvre des mesures de remédiation qui visent à bloquer l'attaquant et à « durcir » la sécurité des systèmes pour prévenir toute nouvelle intrusion. Elle peut également être amenée à intervenir ponctuellement auprès d'autres acteurs en cas de crise cyber, comme ce fut le cas auprès de TV5 Monde en 2015, ou de Saint-Gobain en 2017.

L'ANSSI a également vocation à conseiller les autorités publiques en amont d'une possible crise. C'est ainsi que l'ANSSI avait recommandé au Gouvernement de renoncer au vote électronique pour les Françaises et les Français de l'étranger lors des élections législatives de 2017, compte tenu d'un niveau de menace élevé et d'insuffisances constatées qui n'avaient pas permis d'homologuer la plateforme de vote.

En substance, il est possible de regrouper les missions de l'ANSSI au sein de trois domaines :

– la prévention, le conseil, la formation et la réglementation ;

– la détection des attaques, laquelle passe notamment par le développement, la mise en œuvre et le déploiement de sondes par l'ANSSI ;

– l'assistance apportée aux victimes d'attaques.

Ces différentes missions sont plus précisément développées par l'article 3 du décret n° 2009-834 du 7 juillet 2009, reproduit ci-après.

On soulignera par ailleurs que son article 4 prévoit que l'ANSSI est chargée de la qualification, de la certification, de l'agrément des services, produits

---

(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 ».

(2) Créé par l'article 21 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

et dispositifs de protection des systèmes d'information proposés par les prestataires privés.

Les missions de l'ANSSI aux termes de l'article 3 du décret n° 2009-834

« L'Agence nationale de la sécurité des systèmes d'information est l'autorité nationale en matière de sécurité des systèmes d'information.

À ce titre :

– 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 conçoit, fait réaliser et met en œuvre les moyens interministériels sécurisés de communications électroniques nécessaires au Président de la République et au Gouvernement ;

– 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 un système de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de l'État et coordonne la réaction à ces événements. Elle recueille les informations techniques relatives aux incidents affectant les systèmes d'information de l'État et d'opérateurs publics ou privés. 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 ;

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

● Au quotidien, la cyberdéfense est assurée par le centre opérationnel de la sécurité des systèmes d'information (COSSI). Cette structure est opérationnelle en permanence, 24 heures sur 24 et sept jours sur sept. Le centre de cyberdéfense assure :

– la veille sur les menaces cyber et l'alerte des autorités gouvernementales et des victimes ;

– le pilotage des opérations de cyberdéfense conduites par l'ANSSI.

● D'après le rapport d'activité de l'ANSSI au titre de l'année 2017, ont été enregistrés 2 435 signalements dont 1 621 ont fait l'objet d'un traitement. Le rapport

fait état de 794 incidents hors OIV, de 20 incidents considérés comme majeurs et de trois crises.

Le dispositif national d'assistance aux victimes d'actes de cyber malveillance

Mis en place en 2017, le dispositif ACYMA (actions contre la cyber malveillance) a pour vocation de porter assistance aux particuliers, entreprises et collectivités territoriales concernés par de tels actes.

Il s'appuie sur une plateforme numérique en ligne dédiée (www.cybermalveillance.gouv.fr) qui a vocation à :

– aider les victimes par l'établissement d'un diagnostic de leur situation ;

– les mettre en relation avec des prestataires de proximité susceptibles de leur porter assistance ;

– mettre à disposition outils et publications délivrant des conseils pratiques.

ACYMA s'appuie sur les prestataires techniques dits « de proximité », sur les réseaux territoriaux de l'État (gendarmerie, police, référents de l'ANSSI) ainsi que sur les acteurs locaux, qu'il s'agisse des collectivités territoriales, des chambres consulaires, ou encore des fédérations professionnelles.

Depuis le lancement de la plateforme, plus de 12 000 « parcours victimes » ont été réalisés, qui ont permis d'identifier des menaces dont certaines étaient jusqu'alors sous-estimées (arnaques au faux support technique, par exemple).

b. Les moyens de l'ANSSI : un renforcement constant corrélé à l'évolution de la menace

L'ANSSI employait 546 agents à la fin juin 2018, contre 80 en 2009, lors de sa création. Il s'agit d'une croissance substantielle, dans un contexte de maîtrise de la dépense publique. 77 % de ses personnels sont des contractuels, et l'âge moyen des agents est de 35 ans. Ce personnel est très majoritairement masculin bien que l'effectif féminin progresse lentement, passant de 15 % en 2016 à 20,1 % au 30 juin 2018. Sur ces 20,1 %, 70 % des femmes occupent des postes techniques informatiques, 30 % étant employées dans les métiers des ressources humaines, du soutien juridique, de la communication ou du secrétariat.

Plusieurs interlocuteurs des rapporteurs ont souligné et déploré la faible féminisation des métiers de l'informatique. Les raisons invoquées pour cette maigre appétence sont soit un blocage culturel, soit l'ignorance de ces métiers, soit le fait que le système éducatif qui n'intègre pas cette discipline à la formation des élèves. Les rapporteurs reviendront plus avant sur ce sujet.

Ses ressources budgétaires [(1)] ont suivi une évolution analogue, passant d'environ 30,6 millions d'euros en 2016 à 37 millions d'euros en 2017 et 49,6 millions d'euros en 2018, soit une augmentation de 62 % en trois ans.

(1) Crédits de paiement.

c. Quelques rappels sur les OIV

Il n'est sans doute pas inutile d'apporter quelques précisions sur la notion d'OIV, afin de justifier les mesures de protection particulières dont ils font l'objet et qui seront présentées plus en détail ultérieurement (1).

À la suite des attentats du 11 septembre 2001, la France a engagé une réflexion sur la notion d'infrastructure critique afin de moderniser la protection des points et des réseaux sensibles. Dans ce cadre, douze secteurs d'activité d'importance vitale ont été identifiés (2) et qui relèvent chacun d'un ministre coordonnateur : activités civiles de l'État ; activité judiciaire ; activités militaires de l'État ; alimentation ; communications électroniques, audiovisuel et information ; énergie ; espace et recherche ; finances ; gestion de l'eau ; industrie ; santé ; transports.

Au sein de chaque secteur sont identifiés un certain nombre d'OIV, lesquels sont définis par l'article L. 1332-1 du code de la défense comme « *des opérateurs privés ou publics exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation* ». Les gestionnaires de certains établissements relèvent également de la catégorie des OIV (3).

Il existe moins de 350 OIV, la liste précise étant classifiée pour des motifs de sécurité nationale.

3. Le COMCYBER : autorité de référence pour la cyberdéfense au sein du ministère des Armées

a. L'existence d'une chaîne cyberdéfense spécifique au ministère des Armées

Compte tenu de l'importance de la cyberdéfense pour le ministère des Armées et des spécificités de celui-ci, les missions exercées par principe par l'ANSSI s'agissant de la prévention et de la détection des cyberattaques ont été confiées, par délégation de celle-ci, à une structure interne aux armées, laquelle exerce par ailleurs d'autres attributions opérationnelles dans le cyberespace.

Ainsi, dans le domaine de la cyberdéfense, le chef d'état-major des armées (CEMA) exerce trois responsabilités :

– la protection des réseaux des armées et des principaux réseaux transverses du ministère des Armées ;

---

(1) Partie III du présent rapport.

(2) Arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs.

(3) Articles L. 1332-2 et R. 1332-1 du code la défense.

– la conduite de la défense des réseaux de l'ensemble du ministère à l'exception de ceux relevant des services de renseignement précisés par arrêté du ministre des Armées (en l'espèce la DGSE et la DRSD) [1]. Au-delà des actions défensives, des mesures actives peuvent être menées pour assurer la défense de ces réseaux ;

– la conduite des opérations dans l'espace numérique, au même titre que celles conduites dans les autres espaces [2]. Cette mission regroupe l'ensemble des actions, y compris offensives, menées dans le champ strictement militaire.

Le CEMA a confié l'exercice de ces trois missions à une structure spécifique : le COMCYBER. Les attributions du COMCYBER sont précisées par un arrêté du 4 mai 2017 modifiant l'organisation de l'état-major des armées [3] et aux termes duquel le COMCYBER :

– exerce les responsabilités précitées pour le compte du CEMA : protection des systèmes d'information placés sous la responsabilité du CEMA ; conduite de la défense des réseaux de l'ensemble du ministère des Armées, hors DGSE et DRSD ; conception, planification et conduite des opérations militaires de cyberdéfense, sous l'autorité du sous-chef d'état-major chargé des opérations ;

– contribue à l'élaboration de la politique des ressources humaines de cyberdéfense ;

– coordonne : d'une part, la contribution des armées et organismes interarmées à la politique nationale et internationale de cyberdéfense, notamment pour l'élaboration et la mise en œuvre des plans de coopération ; d'autre part, la définition des besoins techniques spécifiques de cyberdéfense ;

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

– développe et anime la réserve de la cyberdéfense.

Enfin, le COMCYBER assiste et conseille le ministre des Armées pour les sujets relevant de son domaine de compétence.

En substance, la création du COMCYBER résulte donc d'une double volonté : d'une part, placer la problématique cyberdéfense sous l'autorité directe du CEMA et ancrer définitivement le cyber dans les opérations ; d'autre part, conférer une cohérence ministérielle sur l'ensemble de la chaîne cyberdéfense.

---

(1) Article R 3121-2 du code de la défense.*

(2) L'ensemble des opérations cyber, qu'elles soient de nature défensive ou offensive, menées en appui des armées sur les théâtres d'opérations sont planifiées et conduites par un centre d'opérations cyber (COCYBER) placé sous les ordres du COMCYBER et intégré au centre de planification et de conduite des opérations (CPCO).

(3) Article 6 de l'arrêté.

b. Les moyens à disposition du COMCYBER : des ressources spécifiques et interarmées pour une montée en puissance progressive

Le COMCYBER commande l'état-major de la cyberdéfense (EM-CYBER), basé à Balard et disposant d'une antenne à Rennes, et dont les effectifs devraient progressivement atteindre 70 personnes en 2019. Pour l'exercice de ses missions, le COMCYBER dispose par ailleurs d'une autorité fonctionnelle sur les unités spécialisées en cyberdéfense relevant des différentes armées et des organismes interarmées [(1)], représentant plus de 3 000 « combattants numériques » à l'horizon 2019 et 4 000 à l'horizon 2025.

La répartition des cyber-combattants est la suivante :

– un tiers au sein des unités spécialisées placées sous l'autorité fonctionnelle du COMCYBER ;

– la moitié au sein d'autres organismes transverses mutualisés, qui contribuent directement à la fonction cyber du ministère des Armées dans ses dimensions capacitaires (équipement, opérateurs, etc.) ou renseignement ;

– le reste est intégré au sein des différentes armées, directions et services [(2)], qui assurent sur le territoire national comme en opérations extérieures la protection et la défense des systèmes d'information de l'état-major des armées.

À ces quelque 3 000 cyber-combattants doivent s'ajouter les réservistes des deux réserves de cyberdéfense susceptibles d'être mobilisés.

Les réserves de cyberdéfense

Le COMCYBER est chargé du développement et de l'animation de la réserve de cyberdéfense. À l'heure actuelle, celle-ci se compose de deux entités, lesquelles ont vocation à fusionner à l'avenir.

● Une composante « intéressée par le domaine cyber » issue de la réserve citoyenne des armées et de la gendarmerie. Mise en place en 2012, cette réserve est copilotée par l'ANSSI, la gendarmerie et le COMCYBER. Elle assure, d'une part, des missions de sensibilisation à la cyberdéfense et, d'autre part, des actions de rayonnement et de communication s'agissant du COMCYBER et des besoins du ministère des Armées.

● Une réserve spécialisée en cyberdéfense, dont la vocation est directement opérationnelle. Mise en place à partir de mai 2016, son modèle est aujourd'hui en cours d'actualisation et s'articulera autour des besoins en renfort opérationnel sur l'ensemble des missions de lutte informatique défensive du COMCYBER. Elle peut être mobilisée au profit du ministère des Armées, mais également au bénéfice d'autres organismes publics ou privés, sur demande du Premier ministre.

Les réservistes opérationnels spécialisés sont des étudiants ou des professionnels du secteur de la cyberdéfense, encadrés par du personnel d'active du ministère des Armées et du personnel de réserve opérationnelle.

(1) Soit une vingtaine d'unités dont, par exemple, la 807e compagnie de transmissions de l'armée de terre.

(2) Armée de terre, armée de l'air, marine nationale, commandement des opérations spéciales, service du commissariat des armées, service de santé des armées.

Sur le plan budgétaire, la cyberdéfense représente un investissement annuel d'environ 250 millions d'euros pour le financement de la R&D, des technologies défensives et offensives, et des infrastructures.

c. La conduite de la lutte informatique défensive : l'action du CALID

S'agissant de l'ampleur de la menace sur le périmètre placé sous la responsabilité du COMCYBER, quelque 700 événements ont été détectés en 2017. Un « événement » correspond à un incident ou une attaque ayant donné lieu à une action conservatoire de la part du COMCYBER. Parmi ces 700 événements, une dizaine ont été considérés comme critiques et ont nécessité une mobilisation d'ampleur afin d'y apporter une réponse adaptée.

La lutte informatique défensive est confiée au centre d'analyse de lutte informatique défensive (CALID), chargé de la recherche et du traitement des attaques contre les systèmes du ministère des Armées, et sur leurs relais dans l'ensemble des entités du ministère. Centre névralgique de la LID, comprenant 80 agents, le CALID est colocalisé avec le centre opérationnel de l'ANSSI, ce qui permet des échanges rapides et efficaces et le partage tant de l'expertise que de certains moyens techniques. Ainsi, les sondes utilisées par le COMCYBER et opérées par le CALID ont-elles été développées par l'ANSSI. Si les deux structures ne sont pas intégrées, le degré de coopération est très élevé, ce qui constitue non seulement un avantage, mais une condition indispensable à la gestion des événements dans le cyberespace nécessitant réactivité et vision globale.

L'exercice DEFNET

La cinquième édition de l'exercice interarmées de cyberdéfense DEFNET, conduit sous l'autorité du COMCYBER s'est déroulée du 12 au 23 mars 2018. Plus de 300 spécialistes militaires des armées, directions et services, 250 étudiants issus d'établissements d'enseignement supérieur et 50 réservistes y ont participé ainsi que, pour la première fois, sept pays étrangers partenaires.

Les exercices DEFNET visent à entraîner la chaîne de cyberdéfense et à améliorer la coordination et l'expertise des acteurs cyber des armées. Au cours de l'édition 2018, les militaires, les réservistes de la réserve de cyberdéfense et les étudiants de plusieurs grandes écoles ont dû, en liaison avec le CPCO, planifier, coordonner et mettre en œuvre les mesures de défense pour faire face à des menaces et des attaques cyber simulées.

L'exercice DEFNET 2018 a consisté à simuler une attaque informatique de grande ampleur visant plusieurs systèmes d'information et se déroulant de manière simultanée dans toute la France (Paris, Rennes, Coëtquidan, Mont-de-Marsan, Toulon, Rennes, Rochefort et Brest).

d. La conduite d'actions offensives dans l'espace numérique en appui des opérations militaires

Il convient de rappeler à titre liminaire le principe de l'applicabilité, dans le cyberespace, du droit international humanitaire, c'est-à-dire le droit de la guerre, dont les grands principes sont la nécessité, la proportionnalité, la distinction et l'humanité. Ainsi, dans le domaine cyber comme dans les domaines traditionnels, les armées françaises se conforment au droit international

humanitaire dès lors que l'opération militaire de cyberdéfense produit des effets sur le territoire concerné.

Cela a été rappelé, le COMCYBER exerce, pour le compte du CEMA la conduite des opérations menées dans l'espace numérique, qu'il s'agisse d'opérations défensives ou offensives. Dans tous les cas, il s'agit d'opérations exclusivement menées dans un cadre militaire.

S'il n'est pas possible de détailler les mesures de lutte informatique active potentiellement conduites, il convient de souligner que la mise en œuvre de telles actions est officiellement reconnue et assumée en tant que capacité complémentaire à laquelle les armées peuvent recourir dans le cadre d'opérations militaires.

Le rapport annexé à la LPM 2019-2025 reconnaît ainsi pleinement la dimension cyber des opérations de demain et consacre le caractère incontournable des actions de lutte informatique active puisqu'il précise qu'« *En matière de lutte informatique offensive, de nouvelles capacités d'action, intégrées à la chaîne de planification et de conduite des opérations, seront systématiquement déployées en appui de la manœuvre des armées.* » (1)

e. La nécessité de conserver un équilibre entre innovation et rusticité afin que les armées puissent continuer à opérer, même en « mode dégradé »

Il importe que les armées restent en mesure d'agir « en mode dégradé », c'est-à-dire même privées de technologies et de capacités numériques. Une telle « corde de rappel » est essentielle. Ainsi que l'ont rappelé toutes les personnes auditionnées par la mission d'information, aucun système n'est absolument impénétrable, aucune défense n'est parfaitement infaillible.

Le constat est encore plus prégnant dans le domaine cyber où les technologies évoluent constamment et sont à la portée d'un nombre important d'acteurs, potentiellement malveillants. Il est donc nécessaire que les armées « conservent de la rusticité » et puissent continuer à mener leurs missions en se passant de certaines fonctions numériques si celles-ci venaient à se trouver indisponibles. D'où l'importance d'assurer non seulement la résilience des systèmes, mais également leur redondance, y compris en recourant à des alternatives plus « rustiques » (2).

4. La DGSE : la conduite d'actions dans le cadre de ses missions de contre-espionnage, de contre-ingérence et de renseignement

Aux termes de l'article D. 3126-2 du code de la défense, la DGSE a pour mission « *de rechercher et d'exploiter les renseignements intéressant la sécurité de la France, ainsi que de détecter et d'entraver, hors du territoire national, les*

(1) Souligné par les rapporteurs.
(2) Sur ce sujet, voir également le rapport d'information sur les enjeux de la numérisation des armées, op. cit.

activités d'espionnage dirigées contre les intérêts français afin d'en prévenir les conséquences. »

À l'instar des autres services spécialisés du renseignement [1], la DGSE dispose d'une habilitation générale à mettre en œuvre l'ensemble des techniques de surveillance pour l'exercice de ses missions et pour l'ensemble des finalités limitativement prévues par la loi [2] concourant à la défense et à la promotion des intérêts fondamentaux de la Nation, à savoir :

– l'indépendance nationale, l'intégrité du territoire et la défense nationale ;

– les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;

– les intérêts économiques, industriels et scientifiques majeurs de la France ;

– la prévention du terrorisme ;

– la prévention : des atteintes à la forme républicaine des institutions ; des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 du code de la sécurité intérieure ; des violences collectives de nature à porter gravement atteinte à la paix publique ;

– la prévention de la criminalité et de la délinquance organisées ;

– la prévention de la prolifération des armes de destruction massive.

Dans l'hypothèse d'une cyberattaque qui menacerait les intérêts fondamentaux de la Nation, la DGSE serait alors fondée à mettre en œuvre une ou plusieurs techniques de renseignement, dans les conditions prévues par la loi [3]. À cet égard, il convient de rappeler que la loi de novembre 2015 sur le renseignement a déterminé le cadre juridique applicable à la mise en œuvre de mesures de surveillance des communications électroniques internationales [4].

Le renseignement recueilli dans ce cadre peut s'avérer particulièrement précieux, non seulement aux fins d'anticipation et de caractérisation d'une cyber-menace, mais également afin d'appuyer le travail d'analyse permettant *in fine* l'attribution d'une cyberattaque. Au-delà de la prévention et de la détection

---

(1) Désignés par décret en Conseil d'État, ces six services sont : la direction générale de la sécurité extérieure ; la direction du renseignement et de la sécurité de la défense ; la direction du renseignement militaire ; la direction générale de la sécurité intérieure ; la direction nationale du renseignement et des enquêtes douanières ; le service dénommé « traitement du renseignement et action contre les circuits financiers clandestins ».

(2) Article L. 811-3 du code de la sécurité intérieure.

(3) Livre VIII du code de la sécurité intérieure.

(4) Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales (dispositions codifiées aux articles L. 854-1 à L. 854-9 du code de la sécurité intérieure).

d'attaques, la DGSE mène également des actions d'investigation numérique (*computer forensics*) permettant l'analyse *ex post* des atteintes.

5. La DGSI : la conduite d'actions cyber dans le cadre du renseignement intérieur

Comme la DGSE, la DGSI peut mettre en œuvre des capacités cyber pour conduire les missions dont elle a la charge, sa mission générale et fondamentale étant la recherche, la centralisation et l'exploitation, sur l'ensemble du territoire national, du renseignement intéressant la sécurité nationale ou les intérêts fondamentaux de la Nation [(1)].

Schématiquement, ses missions s'articulent autour de cinq domaines :

– le contre-espionnage : il s'agit de prévenir et neutraliser, sur le territoire national, toute menace résultant des activités menées par les services de renseignement de pays étrangers, d'organisation ou d'individus se livrant à l'espionnage, au sabotage ou à la subversion ;

– la contre-ingérence économique ;

– la lutte contre la prolifération ;

– la lutte contre le terrorisme et les extrémismes violents ;

– la lutte contre la cybercriminalité.

La DGSI a vocation à agir en amont, à titre préventif, en conseillant notamment les entreprises au titre de la contre-ingérence économique ; mais également en aval, à titre répressif, dans le cadre de la conduite d'enquêtes judiciaires relatives aux cyberattaques dont pourraient être victimes l'État, les OIV et certaines entreprises.

6. La DRSD : la protection des industries de défense et du potentiel technique et scientifique de la Nation

Au-delà des quatre acteurs du « premier cercle », les rapporteurs ont jugé important de consacrer des développements spécifiques à un autre acteur souvent méconnu : la direction du renseignement et de la sécurité de la défense.

Créée en 2016 en remplacement de la direction de la protection et de la sécurité de la défense (DPSD), la DRSD est le service de renseignement du ministère des Armées dont l'action est dédiée à la contre-ingérence. Sa mission principale est de déceler et d'entraver les menaces visant les armées et les entreprises en lien avec la défense. Comme le précise l'article D. 3126-5 du code de la défense, le ministre des Armées en dispose « *pour assumer ses*

(1) Article premier du décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure.

responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles. ». La DRSD fait partie des services spécialisés du renseignement (le « premier cercle » de la communauté du renseignement).

Ses missions (1) sont les suivantes :

– la participation à l'élaboration et au contrôle de l'application des mesures à prendre en matière de protection et de sécurité ;

– la prévention et la recherche des atteintes à la défense nationale. À ce titre, la DRSD peut notamment mettre en œuvre des mesures de contre-ingérence pour contrer toute menace pouvant prendre la forme d'activités de terrorisme, d'espionnage, de subversion, de sabotage ou de crime organisé ;

– la contribution à la protection des personnes susceptibles d'avoir accès à des informations protégées ou à des zones, des matériels ou des installations sensibles. La DRSD met notamment en œuvre la procédure d'habilitation prévue pour les différents niveaux de classification (2) (confidentiel-défense, secret-défense, très secret-défense) ;

– la participation aux études de sécurité et à l'élaboration des textes réglementaires en rapport avec le traitement de l'information, notamment en matière de traitement automatisé, et le contrôle de l'application des mesures de sécurité édictées ;

– la participation à l'application de la plupart des dispositions du code de la défense relatives aux matériels de guerre, armes et munitions (3).

Au-delà du périmètre strict du ministère des Armées, la DRSD exerce sa mission de protection auprès des entreprises titulaires de marchés intéressant la défense ou sous-traités à son profit et nécessitant la prise de précautions particulières, notamment lorsque le titulaire du marché est susceptible de détenir des informations classifiées. À cet égard, elle participe à l'élaboration des mesures nécessaires à la protection du personnel, des informations, des matériels et des installations sensibles intéressant la défense et en contrôle l'application au sein de ces sociétés.

L'action de la DRSD en direction de l'industrie de défense se traduit prioritairement par l'accompagnement des entreprises habilitées à détenir ou avoir accès à des informations classifiées. Son contrôle s'exerce en amont et en aval, ses officiers de contre-ingérence cyber travaillant en étroite collaboration avec les responsables de la sécurité de ces sociétés. À cet égard, si les risques cyber sont bien pris en considération par les grands groupes, tel n'est pas forcément le cas au niveau des PME et ETI, dès lors qu'elles ne disposent pas nécessairement des ressources tant humaines que financières pour le faire.

(1) Article D. 3126-6 du code de la défense.
(2) Lesquels ont d'ailleurs vocation à évoluer, sous l'égide du SGDSN.
(3) Articles L. 2331-1 à L. 2339-13 du code de la défense.

Les entreprises concernées sont habilitées par la DGA, après avis de la DRSD, qui audite leurs systèmes d'information et de communication. En 2017, environ 300 avis ont ainsi été rendus. Une succession de concertations avec l'entreprise doit conduire, dans un délai d'un an maximum, à l'homologation du système considéré. À l'issue de processus et si le système ne garantit pas une protection du secret suffisante, l'entreprise ne peut se voir remettre aucune information classifiée.

De fait, la DRSD entretient des contacts réguliers avec les responsables de la sécurité informatique de chaque groupe industriel ou société suivi. Toute attaque sur un réseau classifié de défense est portée à sa connaissance. Les plus notables, c'est-à-dire celles qui induisent un préjudice à la protection du secret, font naturellement l'objet d'une enquête.

Grâce aux informations recueillies, la DRSD sera en mesure de dresser une cartographie des attaques, susceptible d'être utilisée à des fins de prévention. Cette cartographie sera le fruit de l'analyse des évolutions de la situation cyber et permettra d'identifier les secteurs ciblés, les marqueurs qui caractérisent l'action, voire les objectifs recherchés.

Afin d'améliorer la surveillance des industries de défense, la DRSD travaille actuellement au développement d'une plateforme automatisée, qui fera remonter les informations nécessaires pour analyser la situation cyber et émettre des alertes vers les industriels, et dont la mise en œuvre est prévue au second semestre 2018.

Naturellement, la DRSD travaille étroitement avec l'ANSSI, avec qui elle échange sur les différents types et modalités d'attaques cyber.

● La DRSD participe en outre à la protection du potentiel scientifique et technique de la Nation (PPST). Le dispositif de protection du patrimoine scientifique et technique français a fait l'objet d'une révision en 2011 [(1)], afin de l'adapter face à la multiplication des atteintes qui avait été constatée à l'époque. Ce potentiel scientifique et technique est en effet l'un des éléments constitutifs des intérêts fondamentaux de la Nation mentionnés par l'article 410-1 du code pénal.

En substance, ce dispositif vise à protéger les éléments essentiels du potentiel scientifique et technique de la Nation, soit les savoirs, savoir-faire et technologies les plus sensibles des établissements, publics comme privés :

– dont la captation serait de nature à affaiblir les moyens de défense de la Nation, à compromettre sa sécurité, ou à porter préjudice à ses autres intérêts fondamentaux ;

(1) Voir notamment le décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation et l'arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la Nation.

– ou dont le détournement pourrait contribuer à la prolifération d'armes de destruction massive et de leurs vecteurs, au renforcement d'arsenaux militaires étrangers, ou à la commission d'actes terroristes, sur le territoire national comme à l'étranger.

Au total donc, la DRSD accompagne plusieurs milliers de sociétés en lien contractuel avec le ministère des Armées ou présentant un intérêt particulier en raison de leur secteur d'activité et plusieurs milliers d'acteurs sur lesquels le service veille au titre de la protection du patrimoine scientifique et technique de la Nation.

7. Les actions « traditionnelles » menées par les armées, notamment sur la couche physique du cyberespace

Au-delà des acteurs et services spécialisés, il convient de rappeler que l'ensemble des armées ont vocation à participer à la cyberdéfense dans le cadre des missions et opérations qu'elles conduisent, notamment s'agissant des éléments constitutifs de la couche physique du cyberespace.

Pour n'évoquer qu'un seul exemple, la marine nationale est susceptible, au cours des déploiements de ses bâtiments de surface, de ses sous-marins et de ses avions de patrouille, de mener des actions de surveillance s'agissant des câbles sous-marins. Principaux vecteurs des communications intercontinentales, leur nombre est relativement réduit puisqu'on en compte environ 400 ; à titre d'exemple, moins d'une vingtaine relient l'Europe et les États-Unis [(1)]. De fait, toute action de dégradation, de sabotage ou de prise de contrôle d'un de ces éléments pourrait engendrer d'importantes conséquences sur la fluidité des flux de communication, sans parler de la captation des données qui y transitent.

De telles vulnérabilités avaient bien été identifiées par le SGDSN à l'occasion de la publication de son étude intitulée *Chocs futurs*. Celle-ci soulignait expressément que « *Les câbles sous-marins assurant les communications numériques deviennent par exemple de potentielles cibles dans le jeu des puissances.* » [(2)]

8. La DGA : le responsable de la sécurité numérique des systèmes d'armes et des systèmes d'information dont disposent les armées

La direction générale de l'armement (DGA) est avec le COMCYBER un acteur essentiel de la cyberdéfense au sein des armées. En effet, agir dans le cyberespace ou mener un combat en opérations avec des systèmes d'armes numérisés requiert d'une part, des produits spécifiques, et, d'autre part,

---

(1) Commission de la défense nationale et des forces armées de l'Assemblée nationale, audition de l'amiral Christophe Prazuck, chef d'état-major de la marine, mercredi 26 juillet 2017, compte rendu n° 9.

(2) Secrétariat général de la défense et de la sécurité nationale, Chocs futurs – Étude prospective à l'horizon 2030 : impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité*, 2017.*

l'assurance d'une résistance maximale aux attaques cyber des matériels mis en œuvre, dont il est admis qu'elle ne peut être totale. La DGA est garante de cette expertise et de cette confiance. Elle remplit pour cela différentes missions.

a. Une action en amont

Qu'il s'agisse de besoins exprimés en matière de systèmes d'armes, de systèmes d'information ou de produits de cybersécurité, une réflexion est systématiquement menée, sur la base d'une analyse des risques, quant à l'opportunité d'une conception interne ou d'un achat sur étagère, en France ou à l'étranger. La protection cyber est dans tous les cas prise en compte aux tout premiers stades de la conception avec un ciblage des composants de cybersécurité nécessaires.

Le développement d'un système d'armes peut ainsi intégrer différentes « briques » acquises ou conçues en propre. La conception intégrale d'un système permet d'en minorer les vulnérabilités numériques et d'identifier les vulnérabilités résiduelles. En revanche, la connaissance d'un système existant, qui aura été soumis à de multiples tests et analyses, demeurera toujours incomplète.

Dans un souci de rationalisation et afin de réduire le temps de conception, la DGA a entrepris une stratégie de mutualisation des produits de cybersécurité ou de « briques » disponibles pour l'ensemble des programmes, évitant ainsi de dupliquer les développements. Il peut, par exemple, s'agir de sondes ou de chiffreurs élaborés en coopération avec l'ANSSI, qui en évalue la performance et délivre un agrément.

b. Une action en aval

Les systèmes utilisés en opérations font par la suite l'objet de tests intrusifs pour en évaluer la résistance et en déterminer les vulnérabilités qui feront, le cas échéant, l'objet d'une correction. Des menaces sont conçues puis simulées, sur la couche logicielle pour tenter de prendre le contrôle d'un système, sur la couche physique (l'intégrité des câbles sous-marins, par exemple) ou encore sur les modalités de guerre électronique.

En ce qui concerne les équipements anciens, la DGA effectue, en fonction du besoin, une mise à niveau numérique lors de leur rénovation à mi vie, étant entendu que la numérisation et l'interconnexion de certains sont si faibles que le risque cyber est quasiment nul.

La DGA organise par ailleurs des formations, des entraînements, assure le soutien opérationnel et exploite le retour d'expérience tout en incitant les forces opérationnelles à réfléchir aux attaques potentielles et à leurs conséquences sur les systèmes qu'elles utilisent.

c. Une action permanente de conseil, d'expertise, de collaboration et de soutien

La cyberdéfense est, on l'a vu, un milieu paradoxal au sein duquel prédomine la confidentialité mais où les échanges entre les différents protagonistes jouent un rôle déterminant. La DGA collabore étroitement avec le COMCYBER, l'ANSSI, la DRSD, la communauté scientifique et l'industrie.

En sa qualité d'expert technique cyber du ministère des Armées, la DGA met son expertise à disposition en interne mais aussi en externe, auprès de l'ANSSI, et plus largement de l'État, par exemple, pour l'analyse d'attaques complexes et de menaces dangereuses.

La DGA soutient la recherche et l'innovation en consacrant un budget de R&T important au secteur cyber et en finançant une dizaine de thèses chaque année. Elle anime une filière d'excellence cyber, qu'il s'agisse de la formation, de la recherche ou du soutien aux entreprises. Les PME peuvent bénéficier du dispositif RAPID [(1)] au titre duquel la DGA consacre annuellement entre deux et trois millions d'euros au cyber. Le tissu industriel est particulièrement dynamique et compte de grandes entreprises, fleurons du numérique, ainsi que de très nombreuses start-up et PME. En revanche, il est souvent déploré le trop faible nombre d'ETI, pourtant nécessaires à la vitalité et à la consolidation de ce secteur économique.

d. Un centre technique de premier plan

Pour l'ensemble de ces missions, la DGA dispose d'un centre technique à Bruz, en Ille-et-Vilaine, non loin de Rennes, voué à la maîtrise de l'information, dénommé DGA-MI.

C'est là que sont mis au point, en collaboration avec des industriels de confiance, les composants numériques des systèmes d'armes et des systèmes d'information des armées. Une autre activité importante est le test des « briques » et composants achetés sur étagère ainsi que celui des SCADA [(2)].

L'ensemble des activités du centre DGA-MI est le suivant :

- aide à la spécification d'architecture de systèmes de systèmes et ingénierie des systèmes ;
- expertise et évaluation de l'utilisation du spectre des fréquences ;
- expertise des réseaux de télécommunication et des systèmes de transmission ;
- spécification, évaluation et validation de l'interopérabilité des systèmes de commandement et de communication ;
- spécification et évaluation des systèmes de renseignement (capteurs spatiaux, drones, etc.) ;

(1) Régime d'appui à l'innovation duale.

(2) Supervisory contral and data acquisition *(système d'acquisition et de contrôle de données).*

• évaluation de la sécurité des systèmes d'information, conception et évaluation de produits de sécurité ;

• évaluation des performances de systèmes d'armes, de guerre électronique et de guerre optronique ;

• expertise et évaluation des systèmes de missiles tactiques et stratégiques ;

• expertise de composants électroniques spécifiques pour la défense.

Source : ministère des Armées.

Ce centre, désormais indispensable pour ce qui concerne le cyber militaire mais également dual, emploie environ 400 personnes, principalement des ingénieurs, dans le seul domaine cyber.

9. Vers la définition d'une doctrine d'action fondée sur le degré de gravité des atteintes cyber

● Face à chaque grand type de menace, dans chaque milieu, l'État doit pouvoir se reposer sur une doctrine d'action élaborée *a priori*, afin d'assurer la mise en œuvre de la réponse la plus rapide, la plus adaptée et la plus efficace possible face à ladite menace. Tel est le cas dans les milieux traditionnels, tel doit également être le cas dans le domaine cyber.

C'est ainsi que la Revue stratégique de cyberdéfense a fort justement préconisé l'établissement d'une doctrine d'action, l'élaboration d'une échelle des réponses possibles face aux cyberattaques. Les États-Unis disposent d'une telle grille de lecture, que la Revue rappelle et qui est reproduite ci-après.

SCHÉMA NATIONAL DE CLASSEMENT DES ATTAQUES INFORMATIQUE (ÉTATS-UNIS)

Echelle de gravité	Equivalence avec l'échelle CISS USA	Caractérisation de l'impact	Caractérisation comme agression armée au sens de l'article 51 de la Charte des Nations-Unies
Niveau 5 - Situation d'urgence extrême	Level 5 Emergency (Black)	Impact extrême	Probablement possible : à examiner au cas par cas.
Niveau 4 - Crise majeure	Level 4 Severe (Red)	Impact majeur	Probablement impossible : les actions correspondant à ces niveaux pourraient néanmoins constituer d'autres faits internationaux illicites (intervention, violation de la souveraineté, usage de la force, etc.).
Niveau 3 - Crise	Level 3 High (Orange)	Impact fort et étendu	
Niveau 2 - Incident grave	Level 2 Medium (Yellow)	Impact fort et circonscrit	
Niveau 1B - Incident	Level 1 Low (Green)	Impact significatif et circonscrit	
Niveau 1A - Evénement significatif		Impact faible	
Niveau 0 - Evénement	Level 0 Baseline (White)	Impact négligeable	

Source : Revue stratégique de cyberdéfense – SGDSN.

D'après la Revue stratégique de cyberdéfense, au moins six critères devraient être pris en considération pour caractériser de la manière la plus précise possible le degré de gravité d'une cyberattaque :

– les effets induits (avec, en substance, une « échelle » des conséquences allant de l'impact négligeable à l'impact extrême, si l'on reprend la classification américaine) ;

– l'intentionnalité (le but poursuivi par l'attaquant) ;

– la dangerosité (la nature des cibles notamment) ;

– l'attribution (la nature de l'attaquant) ;

– la massivité/la volumétrie (la relation de la cyberattaque avec d'autres incidents) ;

– la récurrence (la répétition de la cyberattaque).

Par ailleurs, la Revue souligne que la gravité d'une cyberattaque doit être évaluée à l'aune de l'atteinte portée à quatre champs spécifiques :

– les intérêts fondamentaux de la Nation, sa souveraineté et sa démocratie ;

– la sécurité intérieure et civile ;

– la population et l'environnement ;

– l'économie.

● S'agissant de la réaction possible de l'État face à une cyberattaque, il convient de rappeler cette réalité : la nature de l'attaque qu'il subit ne contraint pas la nature de la réponse qu'il y apporte, dans le respect des règles applicables aux conflits naturellement. Ainsi, une attaque par voie navale n'oblige pas automatiquement l'État victime à conduire en représailles une opération dans le même milieu avec le même type de capacités.

De la même manière, la réponse à une cyberattaque n'est pas forcément elle-même de nature cyber. L'État dispose d'un large éventail de réponses possibles, militaires ou non. La réponse apportée dépend en réalité de l'objectif que l'on cherche à atteindre, et des effets que l'on cherche à produire sur celui-ci. De fait, elle peut être politique, diplomatique, économique, ou reposer sur la mise en œuvre de moyens militaires « traditionnels » mais, également, cyber. Les modes d'actions peuvent rester exclusivement nationaux ou être menés conjointement avec des partenaires, dans le cadre des mécanismes internationaux de défense collective existants.

B. LES AUTRES MODÈLES : QUELQUES ÉLÉMENTS DE COMPARAISON INTERNATIONALE

1. Allemagne

● Les pouvoirs publics allemands ont récemment été la cible d'actes malveillants qui ont donné une résonance particulière au sujet cyber. Ainsi le réseau du *Bundestag* a-t-il fait l'objet d'une intrusion en mai 2015, rappelant la vulnérabilité des systèmes, y compris ceux des plus hautes institutions de l'État, aux menaces cyber et la nécessité de conduire une politique globale pour les contrer.

De fait, en novembre 2016, le gouvernement fédéral a adopté une « stratégie de cybersécurité » articulée autour de quatre objectifs principaux :

– l'adaptation de l'environnement normatif national et des pratiques de l'ensemble des acteurs concernés, y compris le grand public ;

– le renforcement de la coordination entre les autorités publiques et le monde économique ;

– le renforcement de l'architecture de cybersécurité, à tous les niveaux (État, *Länder*, entreprises) ;

– le développement de la coopération européenne et internationale.

En Allemagne, c'est le ministère fédéral de l'Intérieur (BMI [1]) qui est chargé de coordonner la mise en œuvre de la stratégie de cybersécurité. Il réunit sous son autorité le conseil national de cybersécurité, qui rassemble des acteurs publics mais également des acteurs économiques. Ce conseil a vocation à renforcer la cybersécurité au niveau national, en proposant des évolutions normatives et en travaillant avec les partenaires internationaux de l'Allemagne. Participent à ce conseil la Chancellerie fédérale, les principaux ministères concernés [2], les *Länder*, ainsi que des fédérations d'entreprises.

● La cyberdéfense allemande est organisée autour des acteurs suivants.

o L'Agence fédérale pour la sécurité des technologies de l'information (BSI [3]) constitue l'organe central en charge de la sécurité des systèmes d'information au niveau national et, de ce fait, est comparable à l'ANSSI française. Le BSI a également un rôle de prescripteur et de régulateur puisqu'il développe des normes de sécurité informatique, attribue des certificats de sécurité et assure la gestion de la sécurité et du cryptage pour toutes les institutions fédérales.

Il constitue également l'institution de référence quant à la surveillance des infrastructures critiques. À cet égard, le BSI met en place des équipes mobiles de réponse aux incidents [4] chargées du rétablissement des systèmes informatiques suite à une cyberattaque. Il est par ailleurs susceptible d'apporter son soutien aux services de police et de renseignement allemands dans le domaine de la cybersécurité ou de la défense contre les cyberattaques. Le cas échéant, l'Office fédéral d'aide en cas de catastrophe et de la protection de la population (BBK [5]) pourrait également intervenir en apportant son assistance aux infrastructures critiques.

Le BSI compte environ 850 agents et dispose d'un budget d'environ 110 millions d'euros par an.

Il convient de préciser qu'un centre national de cyberdéfense [6] a été créé en 2011 au sein du BSI, qui a vocation à assurer la coopération de toutes les institutions fédérales impliquées dans le domaine cyber (BSI, *Bundeswehr*, services de police et de renseignement, BBK).

---

(1) Bundesministerium des Innern.
(2) Affaires étrangères, Défense, Économie, Justice et protection des consommateurs, Recherche, Finances.
(3) Bundesamt für Sicherheit in der Informationstechnik.
(4) Mobile Incident Response Teams *(MIRTs)*.
(5) Bundesamt für Katastrophenhilfe und Bevölkerungsschutz.
(6) Nationaler Cyber-Abwehrzentrum.

o Dans le domaine de la police et de la justice et s'agissant de la lutte contre la cybercriminalité, ce sont les services de police et de justice de chaque *Land* qui sont compétents. De fait, les directions générales de la police judiciaire des *Länder* disposent de services spécialisés de défense contre les menaces cyber et la lutte contre la cybercriminalité. Naturellement, des mécanismes de coordination existent entre les différents *Länder*, sachant que le niveau fédéral est également compétent en la matière, *via* l'Office criminel fédéral (BKA [(1)]) et la police fédérale (BPOL [(2)]), notamment en cas de menace majeure.

o Dans le champ du renseignement, plusieurs services sont impliqués. L'Office fédéral pour la protection de la Constitution (BfV [(3)]), qui pourrait être considéré comme l'équivalent de la DGSI, est responsable du contre-espionnage. L'une de ses missions consiste à identifier et analyser les cyberattaques à des fins de renseignement, ainsi que de mettre en œuvre des mesures de sensibilisation des victimes potentielles. Au-delà des moyens « traditionnels » à sa disposition, le BfV a constitué des « équipes cyber mobiles » susceptibles d'intervenir en cas de cyberattaques menées à des fins de renseignement, ou en lien avec les sphères extrémistes et terroristes.

Le Service fédéral de renseignement (BND [(4)]), équivalent de la DGSE, est chargé de la reconnaissance des menaces depuis l'étranger. Enfin, le Service de renseignement militaire (MAD [(5)]), dont les missions recoupent notamment celles de la DRSD française, est chargé de la protection de l'armée allemande, la *Bundeswehr*.

o Au niveau militaire, le ministère fédéral de la Défense et la *Bundeswehr* ont adapté leur organisation et leurs capacités en matière cyber. Une direction générale « cyber et technologies de l'information » a ainsi été créée au sein du ministère, tandis que la mise en place d'un nouveau commandement organisationnel CIR [(6)], équivalent du COMCYBER français, doit permettre de mieux prendre en compte l'espace cyber en tant que domaine opérationnel et, potentiellement, à dimension militaire. Un nouvel état-major CIR [(7)] a également été constitué, qui rassemble les missions cyber, informatiques et de renseignement militaire, y compris la guerre électronique, la géo-information et la communication opérationnelle et assure une centralisation du commandement dans ces domaines.

2. Chine

● Depuis son accession au pouvoir en 2013, le président Xi Jinping a fait de la sécurité des systèmes d'information et de communication un enjeu politique

(1) Bundeskriminalamt.
(2) Bundespolizei.
(3) Bundesamt für Verfassungsschutz.
(4) Bundesnachrichtendienst.
(5) Militärischer Abschirmdienst.
(6) Cyber- und Informationsraum.
(7) Kommando CIR.

majeur, en soulignant la nécessité de déployer des efforts afin de contrôler Internet en matière de technologie, de contenu, de sécurité et de criminalité. De fait, le président Xi s'inscrit dans la continuité des politiques menées depuis la fin des années 1990, lorsque les dirigeants chinois ont réalisé l'importance de l'informatisation et ont, en conséquence, mis en œuvre plusieurs plans nationaux (1) de transformation des modes de gouvernement, de l'économie et de l'armée. Un *Small Leading Group* compétent en matière de cybersécurité et de technologies de l'information a été constitué pour devenir la plus haute instance dirigeante en matière de cyber. Présidé par Xi Jinping lui-même, il est composé d'une douzaine de hauts dignitaires de rang ministériel, civils et militaires, et témoigne de l'importance accordée à ce domaine par les autorités chinoises.

Pour la Chine, le cyber constitue d'abord un enjeu de souveraineté nationale. Il s'agit pour elle de garantir la sécurité des systèmes d'information, le bon fonctionnement des institutions et des infrastructures vitales pour l'activité socio-économique du pays, ainsi que la protection des entreprises et des citoyennes et des citoyens, notamment vis-à-vis de la menace que représente Internet, perçu comme une construction occidentale. Il s'agit également pour les autorités chinoises d'affirmer le contrôle de l'État au plan domestique, notamment en régulant la circulation des informations à l'échelle nationale. Telle est la vocation du projet de « Grande Muraille électronique », mis en place en 2003 et qui permet de contrôler les flux d'information en les obligeant à transiter par des points d'entrée spécifiques.

Dans le domaine économique, la lutte contre la cybercriminalité constitue un autre enjeu qui suppose la protection tant des entreprises que des particuliers.

Enfin, la « Stratégie militaire de la Chine » de 2015 estime que le pays est l'une des plus grandes victimes de cyberattaques, qu'il fait face à des menaces sévères dans la sécurité des cyber-infrastructures et que l'influence du cyberespace sur la sécurité militaire s'accroît progressivement.

● Administration de niveau ministériel notamment en charge de la sécurité du cyberespace, la *Cyberspace Administration of China* (CAC) a été créée en 2014. Elle est placée sous l'autorité du *Central Leading Group for Internet Security and Informatisation*, dirigé par le président Xi.

La CAC contribue à l'élaboration de la réglementation, contrôle les appels d'offres pour les services et équipements de réseaux et vérifie notamment le niveau de sécurité des équipements fournis. Elle est par ailleurs responsable de la « régulation » du contenu d'Internet et délivre les licences d'exercice pour les médias en ligne. Enfin, elle assure la coordination avec les autres acteurs intéressés :

– la commission centrale pour les secrets d'État, chargée de la lutte contre la cybercriminalité et la sécurité des infrastructures ;

(1) À titre d'exemple, les plans « Internet Plus *» et «* Made in China 2025 *».*

– le Groupe central en charge du cryptage des données ;

– l'Armée populaire de libération chinoise (APL), responsable de la surveillance des réseaux, de l'expertise technique et de l'aide d'urgence en cas de crise ;

– le ministère de la Sécurité publique, chargé de l'ensemble des réseaux gouvernementaux ;

– le ministère pour l'Industrialisation et l'informatisation, chargé de la coopération avec le secteur économique pour la mise en œuvre des lois et règlements et le développement des nouvelles normes.

Au-delà des institutions publiques, il existe par ailleurs des groupes de *hackers* civils dont d'aucuns soupçonnent que leurs activités sont tolérées par l'État central, voire que celui-ci exerce un contrôle sur eux. Le groupe China 1937CN Team peut être cité, qui a récemment conduit des opérations au Vietnam et en Corée du Sud [(1)].

● Publiée en 2016, la « stratégie nationale de sécurité dans le cyberespace » identifie et analyse les risques et les menaces cyber qui pèsent sur la Chine et qui sont susceptibles de compromettre sa sécurité politique, économique et, de manière plus originale, sa sécurité culturelle, en particulier les « valeurs fondamentales du socialisme » [(2)]. Sont également soulignés les risques engendrés par le cyberterrorisme et la cybercriminalité.

Les grands principes qui forment la base de cette stratégique sont :

– le respect et la protection de la souveraineté dans le cyberespace, aucun pays ne devant s'engager dans un processus de « cyber-hégémonie » ;

– l'utilisation pacifique du cyberespace, en accord avec les principes de la Charte des Nations unies s'agissant de l'emploi ou de la menace d'emploi de la force ;

– la gouvernance du cyberespace en accord avec la loi ;

– le pilotage global de la cybersécurité et du développement.

Dans ce document, la Chine souligne la nécessité de renforcer la coopération internationale dans le cyberespace, affirmant son soutien à l'action de l'ONU afin de promouvoir l'émergence de normes internationales universellement reconnues. Toutefois la « stratégie nationale de sécurité dans le cyberespace »

---

*(1) Attaque contre le groupe coréen Lotte en mars 2017, suite au déploiement du système de missiles antibalistiques américain THAAD (*Terminal High Altitude Area Defense*) en Corée du Sud, sur des terrains loués par ce groupe industriel.*

(2) « Online rumors and degenerate culture as well as obscenity, violence, superstition and other such harmful information violating the Socialist core value view are corroding the physical and mental health of minors, undermining the social atmosphere, misleading value orientations and endangering cultural security. »

tempère cette position de principe favorable au droit international en précisant : « *Aucune atteinte à la souveraineté dans le cyberespace ne sera tolérée, les droits de tous les pays à choisir de manière indépendante leur modèle de développement, leur mode de gestion des réseaux et leur politique publique vis-à-vis d'Internet, ainsi qu'à participer de manière équitable à la gouvernance internationale du cyberespace devront être respectés.* »

Sur le plan militaire, si le rôle de l'APL est officiellement reconnu en matière de cyberdéfense – sauvegarde de la « sécurité commune » – son organisation et sa doctrine dans ce domaine ne sont pas publiques.

3. États-Unis

● Publiée en décembre 2017, la stratégie de sécurité nationale des États-Unis (*National Security Strategy* – NSS) fait de la protection contre les cyber-menaces l'une des priorités en termes de politique publique. Elle participe ainsi à la protection du « peuple américain, du territoire national et du mode de vie américain » au même titre que la protection des frontières, la défense antimissile et la protection du territoire contre la menace djihadiste, ce qui témoigne de l'importance que lui accordent les autorités américaines. De fait, la NSS y consacre un chapitre spécifique, intitulé « *Keep America Safe in the Cyber Era* ».

Quatre domaines requérant une attention particulière au regard de leur importance et de leur dépendance aux réseaux numériques sont identifiés : les centres de commandement et de contrôle militaire, le système bancaire et financier, le réseau électrique et les moyens de communication [(1)].

La NSS énumère par ailleurs cinq « actions prioritaires » devant guider l'action publique afin de renforcer la cybersécurité et la résilience du pays :

– identifier et hiérarchiser le risque : ceci passe par l'évaluation du risque dans six domaines clé, au sein desquels des cyberattaques pourraient produire des conséquences « catastrophiques ou en cascade » (la sécurité nationale, le secteur de l'énergie, le secteur bancaire et financier, le secteur de la santé et de la sécurité, les communications, les transports) ;

– mettre en place des réseaux gouvernementaux pouvant effectivement être défendus : il s'agit notamment d'assurer la continuité et la sécurité des communications et des services en toutes circonstances ;

– dissuader et entraver les cyber-acteurs malveillants : à cet égard la NSS précise notamment que face à des activités cyber malveillantes d'une ampleur significative, les États-Unis imposeraient des mesures immédiates et coûteuses à leurs auteurs (gouvernements étrangers, criminels ou autres acteurs) ;

(1) « The vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication. »

– améliorer le partage de l'information et la détection : la NSS souligne en particulier la nécessité pour les États-Unis de renforcer leurs moyens pour améliorer leur capacité d'attribution des cyberattaques ;

– déployer des défenses « en couches » (*layered defenses*) : la NSS précise que le gouvernement américain collaborera avec les acteurs privés afin de contrer les activités malveillantes en amont, au niveau des réseaux, ce qui contribuera par ailleurs à renforcer la sécurité des utilisateurs de ces réseaux [(1)].

● L'organisation de la cyberdéfense américaine présente un degré de complexité qui reflète la réalité institutionnelle du pays, qui est un État fédéral. De fait, des acteurs sont présents au niveau des administrations locales et de chacun des États fédérés. Les développements qui suivent s'intéresseront à l'organisation actuelle des seules administrations de niveau fédéral, chargées à titre principal de la protection des réseaux fédéraux.

o La protection opérationnelle des réseaux fédéraux non classifiés relève du Département de la Sécurité Intérieure (DHS [(2)]). Le DHS peut notamment élaborer des directives opérationnelles à destination des différentes agences fédérales et leur apporter un appui opérationnel et technique, en temps normal comme en cas d'incident.

Il existe au sein du DHS une division spécialisée, qui apporte son expertise technique et notamment ses capacités de réponse en cas de cyberattaque : le *National Cybersecurity and Integration Center* (NCCIC). Le NCCIC dispose à cet effet de deux structures :

– la *United States Computer Emergency Readiness Team* (US-CERT), spécialisée dans la réponse aux incidents majeurs et l'analyse des menaces. Elle apporte son expertise en matière de protection, de détection et de prévention des intrusions, et élabore des recommandations de sécurité des systèmes d'information à destination des agences fédérales, des administrations de chaque État et des collectivités locales ;

– la *Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT) est chargée de mettre en œuvre une politique de sécurisation des systèmes de contrôle industriel, à destination notamment des infrastructures nationales critiques. Elle apporte son assistance aux opérateurs vitaux, identifie les vulnérabilités en matière de cybersécurité et développe des stratégies de prévention et de réduction des risques.

De fait, la réponse technique à un incident relève du DHS et de ses entités, en liens avec l'agence touchée par l'acte malveillant.

---

(1) On peut rapprocher une telle volonté de la philosophie du dispositif de détection des cyberattaques prévu par l'article 19 de la loi de programmation militaire 2019-2025.

(2) Department of Homeland Security.

o La sécurité des réseaux d'information et de communication classifiés relève quant à elle du Département de la Défense (*Department of Defense* – DoD). C'est la *National Security Agency* (NSA), service de renseignement technique bien connu, qui assume cette mission auprès des agences fédérales utilisant de tels réseaux. Pour sa part, le commandement de la cyberdéfense, le *U.S. Cyber Command*, créé en 2010, est chargé de la défense des réseaux militaires et, plus généralement, de la protection de la Nation dans le cyberespace. Il convient de souligner que le directeur de la NSA est également commandant du *U.S. Cyber Command*, qui recourt dès lors largement aux moyens et capacités de la NSA pour assumer sa mission.

Plus précisément, le *U.S. Cyber Command* a pour mission de planifier, coordonner, intégrer, synchroniser et conduire les activités permettant de :

– diriger les opérations et la défense des réseaux internes du DoD ;

– préparer et, le cas échéant, conduire les opérations militaires dans le cyberespace.

Alors qu'il n'était jusqu'alors un simple sous-commandement placé sous l'autorité du *Strategic Command* (STRATCOM), le *U.S. Cyber Command* a récemment [(1)] été élevé au rang de *Combattant Command* de plein exercice, témoignant ainsi de l'importance accordée au domaine cyber. Une telle évolution, qui était recommandée par le Congrès, va se traduire pour le *U.S. Cyber Command* par une plus grande autonomie budgétaire, un accès facilité aux autorités politiques, une latitude opérationnelle plus importante et une capacité renforcée à former des coopérations internationales.

Par ailleurs, la séparation organique entre le *U.S. Cyber Command* et la NSA doit prochainement s'opérer, afin de mieux distinguer les opérations cyber relevant du domaine militaire et la mission de renseignement technique, « cœur de métier » de la NSA.

S'agissant des capacités, les forces cyber relevant du *U.S. Cyber Command* doivent comprendre 133 équipes à la fin de l'année 2018, réparties entre :

– les forces de mission nationales (*National Mission Teams*), chargées de la défense du territoire national et de ses infrastructures critiques face à des attaques extérieures (13 équipes) ;

– les forces de cyber protection (*Cyber Protection Teams*) chargées de la défense des réseaux internes du DoD et des systèmes militaires (68 équipes) ;

– les forces de mission de combat (*Combat Mission Teams*) mises à disposition des commandements opérationnels et susceptibles de conduire des

(1) Le 4 mai 2018.

attaques cyber ou d'autres opérations offensives en appui des opérations planifiées (27 équipes) ;

– les forces de soutien cyber (*Cyber Support Teams*) qui apportent des analyses techniques et participent à la planification des opérations (25 équipes).

Ces forces sont fournies par les différentes armées et la garde nationale (réserve opérationnelle), à savoir : l'*Army Forces Cyber Command* pour l'armée de terre, la *Fleet Cyber Command* (1) pour la marine, l'*Air Forces Cyber* (2) pour l'armée de l'air, et le *Marine Corps Cyberspace Command* pour le corps des Marines.

En termes de doctrine, l'armée américaine a publié en octobre 2014 une version déclassifiée de sa doctrine interarmées pour les opérations dans le cyberespace, la *Joint Publication 3-12 (R) Cyberspace Operations*.

Le cyberespace y est considéré comme un milieu de confrontation en tant que tel et comme un moyen d'atteindre l'adversaire : toutes les forces armées sont dès lors susceptibles d'y conduire des opérations et peuvent également l'utiliser pour obtenir des effets dans les milieux physiques « traditionnels », mais également dans le champ des perceptions.

Du point de vue militaire, les cyberattaques peuvent être utilisées pour dégrader, perturber ou détruire l'accès, la disponibilité ou l'intégrité d'une cible à un niveau défini et pour une durée définie. Elles peuvent être utilisées pour contrôler ou modifier les informations d'une manière qui soutiennent les objectifs du commandement.

La posture défensive (*Defensive Cyber Operations* – DCO) s'applique aux réseaux internes du DoD et relève de la responsabilité du *U.S. Cyber Command*.

Les actions offensives (*Offensive Cyber Operations* – OCO) sont, à l'instar des opérations dans les domaines physiques, autorisées par un ordre d'exécution (EXORD). Il est intéressant de noter que, dès lors que les OCO peuvent potentiellement compromettre les activités de collecte de renseignement, une évaluation systématique d'un tel impact, sous la forme d'un « bilan coûts/avantages » (3) est réalisée avant l'exécution d'une OCO. Les OCO doivent être conduites après un examen attentif des effets produits et une prise en compte appropriée de facteurs non militaires impliqués. Il convient de souligner que les attaques directes ne doivent être dirigées que contre des cibles militaires.

Enfin, le dispositif de gestion des crises cyber a été réaménagé par une directive présidentielle publiée le 26 juillet 2016 (4) afin d'être en mesure de faire face à des « incidents significatifs ». Ceci concerne les incidents susceptibles de

---

*(1) 10e flotte de l'*U.S. Navy.
(2) 24e Air Force.
(3) Intelligence Gain or Loss *(IGL).*
(4) PPD-41, Presidential Policy Directive for Cyber Incident Coordination.

causer un dommage concret aux intérêts de sécurité nationale, de politique étrangère ou économique des États-Unis, ou capables de porter atteinte à la confiance, aux libertés publiques, à la santé ou à la sûreté du peuple américain.

o Le Département de la Justice (*Department of Justice* - DoJ) est logiquement responsable de la « chaîne judiciaire » (collecte d'éléments de preuve, conduite d'une enquête, opportunité de poursuites judiciaires) et de la détermination de l'origine d'un incident. Le DoJ agit en ces matières par l'intermédiaire du *Federal Bureau of Investigation* (FBI) et d'une structure d'investigation inter-agences spécifique hébergée par celui-ci, la *National Cyber Investigative Joint Task force* (NCIJTF).

o Enfin, les activités d'assistance dans le domaine du renseignement sont confiées au Directeur du Renseignement National (*Director of National Intelligence* – DNI) par le biais du *Cyber Threat Intelligence Integration Center* (CTIIC). Le CTIIC regroupe les informations issues de la communauté du renseignement et est chargé de produire une analyse consolidée sur les menaces et les incidents cyber. Le DNI, qui est placé sous l'autorité et le contrôle direct du Président des États-Unis, est également en charge de l'attribution de l'attaque.

o S'agissant des moyens consacrés par les États-Unis à la cyberdéfense, plusieurs sources permettent d'en évaluer l'ampleur, même si le montant exact reste naturellement inconnu, ne serait-ce que parce que les moyens de certaines agences demeurent confidentiels.

D'après le *Congressional Research Service*, les dépenses des agences fédérales de cybersécurité pour l'année 2015 s'élevaient à 13,1 milliards de dollars. Pour 2017, ce budget avait atteint 19 milliards de dollars.

L'ONG *Taxpayers for Common Sense* évoque des chiffres nettement plus élevés. Selon l'organisation, les dépenses de cybersécurité pour l'année fiscale 2016 atteindraient 28 milliards de dollars, le DoD représentant à lui seul 18,5 milliards de dollars.

S'agissant des moyens du seul *U.S. Cyber Command*, la requête budgétaire pour 2018 est de 647 millions de dollars, en augmentation de 16 % par rapport à 2017.

4. Israël

Pour Israël, les cyberattaques constituent une menace de premier ordre. En premier lieu, le pays subit régulièrement des attaques, attribuées tant à des États (Iran, Corée du Nord), qu'à des groupes de *hackers* tel le groupe Anonymous. Par ailleurs, la structure de son économie rend Israël très sensible à la menace cyber. En effet, les secteurs des hautes technologies et du numérique représentent une

part importante du PIB national et fondent en grande partie le dynamisme économique d'un pays régulièrement présenté comme la *start-up Nation* [1].

● L'institution centrale en matière de cyberdéfense est *l'Israel National Cyber Directorate* (INCD). Il s'agit d'une structure récente puisqu'elle a été formellement mise en place en décembre 2017. Elle regroupe deux structures, plus anciennes :

– l'*Israel National Cyber Bureau* (INCB). Créé en 2011, il est placé sous l'autorité du Premier ministre et a pour mission de conseiller le gouvernement sur les sujets cyber, de veiller au développement des capacités cyber du pays et d'améliorer la protection cyber des infrastructures jugées vitales pour le pays en édictant des consignes dans ce domaine ;

– l'*Israel National Cyber Security Authority* (INCSA), créée en 2015, est en charge de la protection contre les cyberattaques, en partenariat avec les agences de renseignement militaire. L'INCSA a autorité sur le *Computer Emergency Response Team* (CERT) pour la gestion de crises cyber. Son rôle est strictement défensif ; les actions offensives ne sont susceptibles d'être conduites que par l'armée. À l'instar de la France, Israël a donc fait le choix d'une séparation entre ces deux fonctions. L'INCSA est également chargée d'élaborer la doctrine cyber au niveau national et dispose de compétences en matière de régulation.

L'INCD, que l'on pourrait comparer à l'ANSSI française, n'est toutefois pas la seule institution compétente en matière cyber.

● Au niveau militaire, deux services en sont principalement chargés :

– le Corps C4I, dont la mission est la construction et la protection des infrastructures de communication et des réseaux de l'armée, si nécessaire par la mise en œuvre de contre-attaques. Le renforcement de cette capacité défensive est envisagé, afin de lutter contre les actions attribuées à l'Iran et au Hezbollah ;

– l'unité 8200, service de renseignement de *Tsahal*, chargée de collecter le renseignement et, le cas échéant, de conduire des actions offensives.

Le projet de création d'un commandement centralisé cyber, qui aurait regroupé les capacités cyber de chaque armée et du renseignement militaire, a récemment été abandonné, en raison notamment de l'opposition des unités qui auraient été concernées par une telle réorganisation.

● Considérée comme un enjeu majeur pour la défense du pays, la cyberdéfense bénéficie de moyens importants et d'une expertise de haut niveau. À titre d'exemple, on peut notamment citer le projet de *Cyber Dome* [2], financé par le ministère de la Défense et ayant vocation à renforcer les capacités défensives.

---

(1) D'après le titre de l'ouvrage de Dan Senor et Saul Singer Start-up Nation: The Story of Israel's Economic Miracle*, paru en 2009.*

(2) Ou Digital Iron Dome.

Il convient de souligner l'importance de la coopération qui existe entre Israël et les États-Unis en matière de cyberdéfense. Plusieurs programmes de coopération ont ainsi été mis en place à compter de 2006 entre la NSA américaine et les services israéliens en charge du cyber.

En termes de doctrine, si Israël n'exclut pas le recours à des actions offensives, la conduite des actions de cyberdéfense a une visée principalement défensive. De fait, Israël est réputé ne conduire que peu de cyberattaques, notamment par crainte de représailles de même nature qui, si elles se concrétisaient, pourraient potentiellement avoir d'importances conséquences pour un pays aussi connecté et dépendant du numérique. Les principaux éléments relatifs à la doctrine cyber israélienne figurent dans un document intitulé « *IDF in cyber space : Intelligence gathering and clandestine operations* » (1). De manière assez classique, ce document fait état de trois axes principaux en matière de cyberdéfense : les aspects défensifs, les aspects offensifs et le renseignement.

Il est nécessaire de rappeler la réalité de la situation géopolitique et sécuritaire en Israël, qui a des effets induits s'agissant de ses capacités de cyberdéfense. Ainsi, l'existence d'un service militaire particulièrement long (2) se traduit par la mobilisation de tous les jeunes ingénieurs (ou futurs ingénieurs) du pays et par leur affectation, pour cette durée, au sein notamment des services chargés de la cyberdéfense et ce pour leur plus grand bénéfice. Les étudiants concernés sont par ailleurs incités à prolonger cet engagement puisqu'ils peuvent percevoir une aide au financement de leurs études supérieures – très onéreuses – proportionnelle à la durée de service effectuée dans l'armée. Le fait qu'Israël soit en guerre constitue par ailleurs un catalyseur d'efforts, dans le domaine cyber comme dans les autres champs de la recherche militaire.

● Il convient enfin de préciser qu'au-delà de la sphère strictement militaire, le service de renseignement intérieur israélien, le *Shin Bet*, dispose également de sa cellule de recherche et de lutte cyber.

5. Royaume-Uni

● En novembre 2016, le Royaume-Uni a publié sa deuxième *National Cyber Security Strategy*, qui couvre la période 2016-2021. Celle-ci présente le pays comme l'économie du G20 la plus exposée au risque cyber, compte tenu de l'importance des services dans l'économie et la croissance britanniques. Cette stratégie repose sur trois piliers :

– *Defend* (défendre) : ce pilier vise à renforcer la protection de l'espace cyber britannique en mettant en œuvre le principe de l'*Active Cyber Defence* (ACD). Trois leviers d'action sont identifiés à cet égard : mettre en place un partenariat approfondi avec les opérateurs de télécommunication ; renforcer les

(1) « L'Armée de Défense d'Israël dans le cyber-espace : recueil de renseignement et opérations clandestines ».

(2) Soit deux ans et huit mois pour les hommes et deux ans pour les femmes.

capacités des acteurs gouvernementaux compétents en la matière pour faire échec aux attaques ; améliorer la protection des infrastructures nationales critiques ;

– *Develop* (développer) : ce pilier vise à planifier une stratégie devant permettre au pays de disposer des capacités nécessaires à moyen et long termes. Il s'agit de : répondre à la carence de main-d'œuvre qualifiée ; stimuler l'innovation ; faire du Royaume-Uni un pôle en matière de science et technologie ;

– *Deter* (dissuader) : c'est le pilier le plus novateur, qui applique les principes de la dissuasion au cyberespace [(1)]. Vis-à-vis des États en particulier, il envisage notamment l'attribution officielle et publique d'une cyberattaque à un acteur étatique, dès lors qu'une telle attribution est jugée conforme à l'intérêt national. Ainsi les autorités britanniques ont-elles publiquement attribué l'attaque WannaCry à un groupe de *hackers* lié à la Corée du Nord.

Depuis 2010, la menace cyber constitue l'une des priorités majeures en matière de sécurité nationale, considérant la probabilité de son occurrence et ses conséquences. La *National Security Strategy* de 2010 la place ainsi en deuxième position, après le terrorisme et avant les accidents majeurs, catastrophes naturelles et crise militaire internationale [(2)].

Particulièrement attaché à la liberté d'Internet, le Royaume-Uni s'oppose aux volontés de régulation de l'espace numérique, notamment soutenues par la Chine et la Russie. Du point de vue britannique, les initiatives diplomatiques dans ce domaine sont perçues, d'une part, comme des leviers pour justifier des politiques de restriction interne et, d'autre part, comme des instruments visant à contrer la position largement dominante des entreprises américaines sur le secteur.

Par ailleurs, la proximité du Royaume-Uni avec les États-Unis et son attachement à l'Alliance atlantique le rendent peu réceptif à la volonté, notamment française, de favoriser une « autonomie stratégique » [(3)] européenne.

● Au-delà des actions relevant de la cybercriminalité et s'agissant des menaces d'origine étatique, le Royaume-Uni considère que quatre États sont en mesure d'attenter à sa sécurité : la Russie, la Chine, l'Iran et la Corée du Nord. Parmi ces États, la Russie est jugée la plus menaçante pour les intérêts stratégiques et politiques britanniques, la Chine étant quant à elle supposée mener des actions à visée essentiellement économique.

● S'agissant de l'organisation de sa cyberdéfense, il est intéressant de noter que le Royaume-Uni a récemment fait évoluer sa doctrine. Alors que la précédente revue stratégique cyber de 2011 s'inscrivait dans une logique clairement libérale de recours au marché et aux initiatives privées pour remédier

(1) « The principles of deterrence are as applicable in cyberspace as they are in the physical sphere. », National Cyber Security Strategy 2016-2021, *novembre 2016.*

(2) A Strong Britain in an Age of Uncertainty: The National Security Strategy, *octobre 2010.*

(3) Selon l'expression employée par Mme Florence Parly, ministre des Armées, lors de la Conférence sur la sécurité de Münich en février 2018.

aux défaillances de sécurité dans l'espace numérique, la stratégie de 2016, constatant les insuffisances du primat précédemment accordé au marché, assume quant à elle le principe d'une intervention publique forte dans ce domaine [1].

Par ailleurs, la *National Cyber Security Strategy* a prévu une réorganisation des différentes institutions compétentes en matière de cyberdéfense afin de rationaliser le partage des responsabilités entre celles-ci.

o L'*Office of Cyber Security and Information Assurance* (OCSIA), rattaché au *Cabinet Office*, est chargé de la stratégie nationale menée en matière cyber et de la coordination interministérielle dans ce domaine.

Une partie de ses précédentes prérogatives ont été confiées au *National Cyber Security Center* (NCSC), autorité technique de référence et, à ce titre, comparable à l'ANSSI française. Il en diffère toutefois fondamentalement puisque, contrairement à l'ANSSI, le NCSC devrait disposer d'une capacité offensive dans le domaine cyber. Par ailleurs, le NCSC est placé sous la tutelle du *Government Communications Headquarters* (GCHQ), service de renseignement en charge des interceptions et de la cybersécurité. Il compte environ 700 personnes. À l'instar de l'ANSSI, le NCSC doit développer une approche collaborative tant au sein de la sphère publique que vis-à-vis du secteur privé.

o S'agissant des acteurs militaires et suite à la publication de la stratégie de 2016, le ministère de la Défense britannique (MoD) a renforcé ses capacités en matière cyber. Cette volonté s'est d'abord traduite par la création du *Joint Forces Cyber Group* (JFCyG), dont la mission est d'assurer la cohérence des fonctions cyber assumées par les trois armées et de coordonner les capacités défensives. Par ailleurs, un *Cyber Security Operations Center* doit être créé pour renforcer la protection des services du MoD et assurer la coordination avec le NCSC. Le MoD entend également promouvoir l'innovation dans le domaine des technologies militaires émergentes et disruptives, notamment dans le cadre de l'*Innovation Initiative*, dotée de 800 millions de livres sterling sur dix ans. Enfin, en mars 2018, a été inaugurée officiellement la *Defence Cyber School* (DCS). Celle-ci a vocation à regrouper sur un site unique l'ensemble des capacités militaires de formation et d'entraînement à la cyberdéfense à destination des personnels du MoD concernés et, au-delà, du gouvernement.

En termes de doctrine, l'usage offensif du cyber est assumé par les pouvoirs publics et par le MoD, qui est susceptible d'y recourir en appui des opérations militaires [2].

Au Royaume-Uni, la partie *policy* de la cyberdéfense, à savoir la détermination des grandes orientations et objectifs politiques et stratégiques du

---

(1) « A market based approach to the promotion of cyber hygiene has not produced the required pace and scale of change. […] Only Government can draw on the intelligence and other assets required to defend the country from the most sophisticated threats. »

(2) Michael Fallon, alors Secrétaire d'État à la Défense, avait ainsi évoqué l'emploi de capacités cyber offensives dans le cadre des opérations menées contre Daech.

MoD en la matière est du ressort du ministère lui-même. En revanche, la partie opérationnelle relève du commandant du *Joint Forces Command*, responsable interarmées de la planification et de la conduite des opérations militaires dans le cyberespace. Toutefois, en pratique, il est intéressant de noter que celui-ci délègue cette responsabilité au *Chief of Defence Intelligence* (équivalent de la DRM française) en tant que *Defence Authority for Cyber*.

● Le Royaume-Uni a consenti un effort substantiel quant aux moyens consacrés à la cyberdéfense. Le *National Cyber Security Program* qui faisait suite à la revue de 2011 était doté d'un budget de 860 millions de livres sterling sur la période 2011-2016. La *Strategic Defense and Security Review* [(1)] de 2015 prévoit que ces ressources soient plus que doublées, avec 1,9 milliard de livres sterling consacrés à la cyberdéfense sur la période 2016-2021 [(2)].

6. Russie

● D'un point de vue sémantique, il est tout d'abord intéressant de souligner que, selon la doctrine russe, le cyberespace est conçu comme un « espace d'information ». En conséquence, le concept de « sécurité informationnelle » est largement utilisé, au même titre que les concepts de « cybersécurité » ou de « cyberdéfense ».

La doctrine russe de 2016 relative à la sécurité informationnelle [(3)] identifie six menaces majeures qui pèsent sur la sphère informationnelle russe :

– d'une part, l'augmentation des capacités étrangères susceptibles d'influencer « l'infrastructure informationnelle » russe dans le cadre de la poursuite d'objectifs militaires et, d'autre part, l'augmentation des activités étrangères de renseignement technique ciblant les organes du pouvoir, les sphères scientifiques, ainsi que les entreprises du secteur militaro-industriel ;

– l'utilisation des systèmes d'information par les services de renseignement de certains États pour déstabiliser la situation sociale et politique interne de plusieurs régions, pour saper la souveraineté et violer l'intégrité territoriale d'autres États. La Russie relève à cet égard la tendance des médias étrangers à publier de plus en plus d'informations biaisées relatives à la politique menée par la Fédération de Russie, la discrimination dont les médias russes font l'objet à l'étranger, ainsi que la « pression informationnelle » qui pèse sur la population russe – et notamment sa jeunesse – aux fins d'éroder les valeurs spirituelles et morales russes traditionnelles ;

– l'utilisation des « outils de l'information » par des groupes terroristes et extrémistes ;

(1) Équivalent du Livre blanc sur la défense et la sécurité nationale français.
(2) Avec quatre domaines prioritaires : la surveillance, la détection, l'analyse et les capacités offensives.
(3) Approuvée par le décret présidentiel n° 646 du 5 décembre 2016.

– l'augmentation de la cybercriminalité ;

– la dépendance de la Russie, d'une part, aux politiques étrangères d'exportation de matériel informatique et, d'autre part, vis-à-vis de certaines entreprises internationales concernant la fourniture de matériels spécifiques (super-ordinateurs, composants électroniques) ;

– le désir de certains États de profiter de leur domination technologique dans la sphère informationnelle pour atteindre des buts géopolitiques et économiques.

Au regard de cette analyse, trois axes d'effort prioritaires ont été dégagés. Il s'agit tout d'abord de développer les capacités informatiques nécessaires pour faire face à la guerre informationnelle. Par ailleurs, il convient d'assurer le contrôle de l'information à des fins de protection de la population. Les pouvoirs publics estiment en effet qu'une exposition de celle-ci – et notamment des jeunes générations – à certaines idéologies pourrait remettre en cause la stabilité politique et sociale du pays. Enfin, il s'agit de mettre en place des entraînements réguliers à l'attention de l'ensemble des acteurs de la sphère informationnelle afin d'assurer une réponse efficace, le cas échéant.

À cet égard, il est intéressant d'évoquer le projet RuNet [(1)] 2020. Initialement, le RuNet s'est développé librement sans intervention particulièrement poussée de l'État russe. Il a permis de reconstituer, sur une base nationale [(2)], l'ensemble de l'écosystème d'Internet largement dominé par les acteurs américains (moteurs de recherche, réseaux sociaux, messageries, sites de e-commerce, etc.).

Face au succès rencontré par le RuNet, les autorités russes ont progressivement manifesté leur intérêt à son endroit en renforçant les possibilités d'intervention publique [(3)], et en ont fait l'un des aspects de la doctrine russe de sécurité informationnelle. En substance, il s'agit pour la Russie d'acquérir une pleine souveraineté numérique en plaçant le RuNet sous le contrôle de l'État. L'objectif est qu'à l'horizon 2020, 99 % du trafic Internet russe soit effectivement situé sur le territoire de l'État russe et que 99 % des infrastructures de sauvegarde du RuNet s'y trouvent également.

Dès lors, le projet RuNet 2020 donnerait corps à la souveraineté numérique telle qu'envisagée par les autorités russes et selon laquelle un État détient le droit et la capacité de déterminer souverainement ses intérêts

(1) Contraction de « Russian Internet ».

(2) Mais il rencontre également un grand succès, au-delà de la seule Russie, dans les anciennes républiques de l'URSS.

(3) Ainsi le Roskomnadzo *(service fédéral de supervision des communications, des technologies de l'information et des médias de masse) peut-il prendre des mesures administratives pour censurer les sites web ou contenus en ligne considérés comme portant atteinte à l'ordre public. Par ailleurs, le gouvernement peut contrôler les activités des blogueurs et des médias citoyens dépassant un certain seuil d'audience (les blogs et médias dépassant le seuil de 3 000 personnes en audience quotidienne sont tenus de s'enregistrer auprès du gouvernement fédéral).*

géopolitiques dans le cyberespace. De manière pratique, il s'agit de permettre à un État de se doter de son propre cyberespace national, indépendant de l'Internet global et sous son contrôle.

● En termes d'organisation institutionnelle, la cyberdéfense russe relève principalement des structures suivantes.

Au sein du FSB [(1)], la direction opérationnelle du Centre de sécurité informationnelle (TSiB) serait chargée tant des actions de lutte informatique défensive que des actions de lutte informatique offensive. En 2013, le FSB s'est vu confier la mise en place d'un système national de détection, d'alerte, d'analyse et de mitigation des attaques informatiques, le SOPKA. Reposant sur des équipes d'intervention au niveau gouvernemental [(2)], le SOPKA a vocation à assurer la protection des systèmes d'information gouvernementaux et des opérateurs d'infrastructures critiques.

Le ministère de la Défense ne disposerait à l'heure actuelle que de capacités défensives [(3)]. S'agissant de la protection de ses réseaux, le ministère a mis en place, à compter de 2016, un réseau spécifique dénommé « segment fermé de transmission de données » (SFTD) entièrement déconnecté d'Internet. En 2013, une force d'opérations d'information a été créée, dont la mission est de protéger les intérêts de défense russe et de mener des actions dans le domaine de la sphère informationnelle. À la fin de cette même année, le général Sergueï Choïgou, ministre russe de la Défense, avait confié à l'état-major des forces armées la mission de créer un cyber-commandement ayant vocation à regrouper les activités de luttes contre les attaques cyber, mais également les unités d'opérations d'information. Cette structure serait opérationnelle depuis 2014.

S'agissant du ministère de l'Intérieur, la direction K du Bureau des événements techniques spéciaux (BSTM) est notamment compétente en matière de lutte contre la cybercriminalité.

Pour le secteur bancaire et financier, c'est la banque centrale *via* le centre FinCERT qui est chargée de la supervision des cyber-menaces.

C. LA CYBERDÉFENSE DANS LE CADRE EXTRANATIONAL

Les développements qui suivent n'ont pas vocation à dresser un historique complet de la problématique cyber au sein de l'Union européenne et de l'OTAN, mais de présenter les évolutions les plus récentes en la matière.

---

*(1) Service fédéral de sécurité de la fédération de Russie, les services secrets russes (*Federalnaïa sloujba bezopasnosti Rossiyskoï Federatsii – ФСБ*).*

(2) Computer Emergency Response Team *(Gov-CERT).*

(3) Même si le GRU, le service de renseignement militaire, est réputé développer des programmes offensifs.

1. L'importance d'une coopération internationale lucide

La coopération dans le domaine de la cyberdéfense militaire doit aboutir à un état de sécurité devant permettre aux armées françaises et aux armées partenaires de conduire leurs opérations dans les conditions de sûreté requises. Le partage des informations sur l'état de ses réseaux, les incidents et les attaques subies suppose, d'une part, l'établissement de relations de long terme, dans la durée, et, d'autre part, l'existence d'un haut niveau de confiance et de maturité dans le domaine de la lutte informatique défensive. D'un point de vue matériel, le partage d'éléments techniques nécessite naturellement l'établissement des liaisons sécurisées en bilatéral.

Les échanges entre partenaires peuvent concerner les modalités d'organisation générale des services compétents en matière cyber, les perceptions sur les potentielles attributions d'attaques malveillantes, etc. En revanche, d'après les informations communiquées aux rapporteurs, les solutions techniques mises en œuvre et les « banques » de marqueurs demeurent souveraines.

Si de tels échanges peuvent s'avérer fructueux, et parfois même indispensables, il convient toutefois de faire preuve de lucidité. Tous les États étant concurrents, notamment dans le domaine économique, il convient de faire preuve de prudence. Les États étrangers avec lesquels la France coopère – y compris ses alliés – peuvent par ailleurs chercher à identifier ses propres failles voire à l'instrumentaliser. La coopération doit donc être conduite sans naïveté, son champ doit être clairement défini au préalable et le service partenaire bien identifié au sein du pays avec lequel la France choisit de travailler. En effet, en matière cyber comme dans le domaine des relations internationales en général, les États n'ont pas d'amis ; au mieux, ils ont uniquement des alliés.

2. Au sein de l'Union européenne

● Les questions numériques et cyber de portée européenne ont connu une forte actualité ces derniers mois avec notamment :

– l'application, au 25 mai 2018, du règlement général sur la protection des données (RGPD) [(1)] qui, de manière très schématique, renforce et unifie la protection des données pour les individus au sein de l'Union européenne. Il s'applique aux traitements de données à caractère personnel gérés par des entités présentes sur le territoire de l'UE, que le traitement ait lieu ou non au sein de l'UE. De manière plus originale, et sous certains critères, il est également opposable aux traitements de données à caractère personnel gérés par des entités non présentes sur le territoire de l'UE, quel que soit leur pays d'origine, dès lors

(1) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

que ces traitements concernent des données à caractère personnel relatives à des personnes se trouvant elles-mêmes sur le territoire de l'UE [1] ;

– la transposition récente en droit interne [2] de la directive sur la sécurité des réseaux et des systèmes d'information, dite « directive NIS » [3], laquelle prévoit notamment la mise en place d'un cadre réglementaire permettant de renforcer la cybersécurité des « opérateurs de services essentiels » au fonctionnement de l'économie et de la société (OSE) et des fournisseurs de services numériques (FSN) [4].

L'ENISA

Créée en 2004, la *European Union Agency for Network and Information Security* (ENISA) est une agence de l'UE qui constitue un centre d'expertise pour la cybersécurité en Europe et a vocation à assister les pouvoirs publics dans l'identification des enjeux de cybersécurité et à proposer des solutions techniques pour lutter contre les menaces cyber.

En substance, ses missions sont les suivantes :

– conseiller les institutions de l'UE et les États membres en matière de cybersécurité ;

– favoriser l'échange de bonnes pratiques en la matière, en mettant notamment en place des partenariats entre le secteur public et le secteur privé, en particulier les entreprises spécialisées dans ce domaine.

L'ENISA organise par ailleurs depuis 2010 un exercice bisannuel dénommé *Cyber Europe*, qui permet aux États membres de tester leur collaboration en cas de crise.

● S'agissant de la cyberdéfense au sens strict, des initiatives ont été prises dans le cadre de la politique de sécurité et de défense commune (PSDC), les efforts portant actuellement sur la formation et l'entraînement, la France assurant dans ce cadre le pilotage d'un groupe chargé d'identifier les besoins et l'offre de formation. L'Agence européenne de défense anime quant à elle une *Cyber Defence Project Team* permettant aux États membres participant de progresser sur les sujets de la formation et de l'entraînement, ainsi que les questions de développement capacitaire.

(1) Article 3 – Champ d'application territorial.

(2) Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

*(3) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite NIS (*Network and Information Security*).*

(4) Pour une présentation précise des dispositions de la directive, on se reportera au rapport de M. Christophe Euzet, fait au nom de la commission des Lois constitutionnelles, de la législation et de l'administration générale de la République, sur le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (Assemblée nationale, rapport n° 554, janvier 2018, XV^e^ législature).

Par ailleurs, parmi les 17 projets identifiés dans le cadre de la coopération structurée permanente [1] (CSP – PESCO) initiée en 2017, deux sont spécifiquement dédiés au cyber. Ils concernent :

– la plateforme de partage d'informations en matière de réaction aux menaces et incidents informatiques [2] : piloté par la Grèce, ce projet doit permettre de renforcer les capacités de cyberdéfense des États participants en favorisant le partage du renseignement sur les menaces cyber grâce à une plate-forme en réseau rassemblant ces mêmes États ;

– les équipes d'intervention rapide en cas d'incident informatique et l'assistance mutuelle dans le domaine de la cybersécurité [3] : piloté par la Lituanie, ce projet a pour but d'intégrer l'expertise des États membres dans le domaine de la cyberdéfense. Des équipes d'intervention rapide (CRRTs [4]) seront constituées qui permettront aux États membres de s'entraider pour garantir un niveau plus élevé de cyber-résilience et pour répondre collectivement aux incidents cyber. Les CRRTs pourront porter assistance tant aux États membres, qu'aux institutions européennes ou encore à des pays partenaires.

Si ces deux projets sont ambitieux dans leurs objectifs, leur portée réelle reste à ce stade sujette à interrogations. Le déploiement des CRRTs notamment se heurtera probablement, de manière concrète, à la réticence de certains États à voir des équipes pour partie composées de non-nationaux intervenir sur leurs réseaux.

Par ailleurs, la liste des États membres participant à chacun des deux projets n'est pas révélatrice d'un élan particulier, alors même qu'il s'agit de sujets par nature globaux et transnationaux. Ainsi, seuls sept États participent à chaque projet [5].

Enfin, s'agissant des modalités pratiques de mise en œuvre des projets, il convient de rappeler que les décisions et recommandations du Conseil prises dans le cadre de la CSP le sont à l'unanimité des 25 États membres participants [6], ce qui pourrait singulièrement compliquer la mise en œuvre de celle-ci.

---

(1) La CSP est une stipulation du traité sur l'Union européenne qui permet aux États membres qui le souhaitent de développer leur coopération dans le domaine de la défense. Elle est prévue par l'article 42-6 qui stipule que : « Les États membres qui remplissent des critères plus élevés de capacités militaires et qui ont souscrit des engagements plus contraignants en la matière en vue des missions les plus exigeantes, établissent une coopération structurée permanente dans le cadre de l'Union. » *La CSP est régie par l'article 46 du même traité.*

(2) Cyber Threats and Incident Response Information Sharing Platform.

(3) Cyber Rapid Response Teams and Mutual Assistance in Cyber Security.

(4) Cyber Rapid Response Teams.

(5) Grèce, Espagne, Italie, Chypre, Hongrie, Autriche et Portugal pour le premier ; Lituanie, Espagne, France, Croatie, Pays-Bas, Roumanie, et Finlande pour le second (données au 6 mars 2018 – décision (PESC) 2018/340 du Conseil du 6 mars 2018 établissant la liste des projets à mettre sur pied dans le cadre de la CSP).

(6) Article 46-6 du traité sur l'Union européenne. Ces 25 États sont : l'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, la Croatie, l'Espagne, l'Estonie, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, les Pays-Bas, la Pologne, le Portugal, la République tchèque, la Roumanie, la Slovaquie, la Slovénie et la Suède.

Un instrument spécifique de la lutte contre la cybercriminalité : la convention de Budapest

Élaborée dans le cadre du Conseil de l'Europe, la convention sur la cybercriminalité faite à Budapest le 23 novembre 2001 vise à harmoniser les législations nationales en matière d'incrimination et de sanctions pénales pour une liste de comportements soumis à répression (par exemple, l'accès illégal à un système informatique ou la diffusion de matériel pédophile par le biais d'un système informatique).

Elle vise également à modifier les procédures pénales en vigueur dans les États parties afin de leur donner les pouvoirs nécessaires à l'instruction et à la poursuite des infractions relevant de la cybercriminalité, ainsi que d'autres infractions commises au moyen d'un système informatique ou pour lesquelles les preuves existent sous forme électronique.

Enfin, elle vise à mettre en place un régime rapide et efficace de coopération internationale dans ce domaine.

3. Au sein de l'OTAN

● L'OTAN a pris en compte la nouvelle réalité stratégique issue de l'apparition de la problématique cyber puisque dès 2002, au sommet de Prague, les chefs d'États et de gouvernements des membres de l'Alliance ont approuvé le principe de la mise en œuvre de mesures de renforcement des capacités de défense contre les cyberattaques.

Une étape importante a été franchie plus de dix ans plus tard, en 2014, au sommet de Newport (Pays de Galles). Les membres de l'OTAN y ont ainsi affirmé que le droit international s'appliquait au cyberespace, que la cyberdéfense « *relève de la tâche fondamentale de l'OTAN qu'est la défense collective* », et que l'article 5 du traité de l'Atlantique pourrait le cas échéant être invoqué à la suite d'une cyberattaque [(1)].

Il a toutefois été confirmé que l'attribution d'une cyberattaque resterait une prérogative exclusivement nationale. À cet égard, deux philosophies existent au sein de l'Alliance avec, d'une part, les partisans d'une capacité d'attribution collective (États-Unis et Royaume-Uni, notamment) et, d'autre part, les partisans du maintien d'un mécanisme d'attribution individuel, souverain, dès lors que l'attribution constitue, en dernière analyse, une décision fondamentalement politique (France, par exemple). Un tel débat reste encore d'actualité au sein de l'OTAN.

Un plan d'action a par ailleurs été entériné au cours de ce même sommet, qui a fait l'objet d'une actualisation en février 2017.

Une autre étape a été franchie en 2016, au sommet de Varsovie. Le cyberespace a alors été reconnu comme un nouveau domaine au sein duquel l'OTAN a vocation à se défendre, au même titre que dans les domaines traditionnels (terre, air, mer). Cette reconnaissance s'est accompagnée d'une

(1) Point 72 de la Déclaration du sommet du Pays de Galles.

initiative, soutenue par la France, dénommée « Engagement en faveur de la cyberdéfense » ou *Cyber Defense Pledge*. Celle-ci souligne notamment le rôle de l'OTAN afin de faciliter les coopérations en la matière [1] (mise en place de projets multinationaux, de formations, d'entraînements et d'exercices, échange d'informations) et consacre l'engagement de chacun des alliés à améliorer ses moyens et ses capacités en matière de cyberdéfense [2].

En 2017, les ministres de la Défense des pays de l'OTAN ont approuvé la création d'un Centre des cyberopérations (CyOC) afin de renforcer les moyens de défense cyber et d'intégrer les capacités cyber dans les plans et les opérations de l'OTAN. L'Alliance dispose par ailleurs d'une capacité de réaction aux incidents informatiques (NCIRC [3]) située au Commandement suprême des forces alliées en Europe (*Supreme Headquarters Allied Powers Europe* – SHAPE). Le NCIRC protège les réseaux appartenant à l'OTAN en assurant, 24 heures sur 24, leur soutien en matière de cyberdéfense.

Les membres de l'OTAN ont réaffirmé à plusieurs reprises que la responsabilité de l'Alliance est purement défensive en matière cyber, comme elle l'est dans les autres domaines. L'OTAN est chargée de la protection de ses propres systèmes et dispose d'une agence spécialisée, la *NATO Communication and Information Agency* (NCIA).

● L'aide apportée par l'OTAN à ses membres dans le cadre du renforcement de leurs propres moyens de cyberdéfense prend différentes formes :

– le partage d'informations en temps réel sur les menaces (au moyen d'une plateforme d'échange d'informations sur les logiciels malveillants) et le partage des meilleures pratiques en matière de traitement des cybermenaces ;

– l'existence d'équipes de réaction rapide « cyberdéfense », pouvant être mises à la disposition des membres en tant que de besoin ;

– l'élaboration d'objectifs à atteindre par les Alliés, afin de faciliter une approche commune de leurs capacités de cyberdéfense ;

– l'investissement dans la formation, l'entraînement, et les exercices [4].

L'OTAN dispose par ailleurs d'une entité spécifique, le Centre d'excellence pour la cyberdéfense en coopération (CCD-CoE [5]). Situé à Tallin, il s'agit d'un centre de recherche et d'entraînement accrédité par l'OTAN, compétent en matière de formation, de recherche et de développement dans le domaine de la cyberdéfense. Ce centre a notamment publié un « manuel de Tallin » relatif à l'application du droit international au cyberespace.

---

(1) Point 4 de l'Engagement en faveur de la cyberdéfense.
(2) Ibid. point 5.
(3) NATO Computer Incident Response Capability.
(4) Exercice Cyber Coalition *notamment.*
(5) NATO Cooperative Cyber Defence Centre of Excellence.

L'organisation d'exercices et d'entraînements individuels et collectifs constitue un aspect important dans la « montée en gamme » des capacités des membres de l'OTAN et dans la construction de l'interopérabilité. Des entraînements collectifs ont ainsi été organisés en Estonie dans le cadre du centre virtuel. Celui-ci permet de dupliquer les réseaux de manière réaliste, sans pour autant rendre vulnérables les vrais réseaux.

L'OTAN est particulièrement attachée au concept de « cyber fédéré ». En application de ce principe, les moyens de l'OTAN sont constitués par les éléments que ses membres acceptent de partager. Il convient de préciser qu'en tout état de cause, ces moyens ne passent pas sous commandement de l'OTAN ; les nations conservent leur pleine souveraineté, et leurs capacités peuvent par ailleurs continuer à être mobilisées au profit d'autres.

● L'OTAN ne développe pas de capacités offensives dans le domaine cyber. Le cas échéant, l'Alliance pourrait faire appel aux nations volontaires afin de produire des effets dans le seul cadre des opérations et missions qui seraient conduites. La procédure pour y parvenir – le « mécanisme » – constitue l'un des objectifs du plan d'action d'intégration du domaine cyber. Ce mécanisme est en cours d'élaboration.

Pour l'État membre qui réaliserait une action offensive dans un tel cadre, il serait naturellement nécessaire de garantir la confidentialité des moyens mis en œuvre pour ne pas dévoiler ses capacités, dans leur étendue comme dans leurs limites. D'après les informations communiquées aux rapporteurs, la structure de commandement de l'OTAN recourrait alors à une structure unique de coordination qui servirait également de « chambre de blanchiment » pour que même la nation participante à l'action ne puisse être clairement identifiée.

Le prochain sommet de l'OTAN, organisé à Bruxelles en juillet 2018 abordera sans doute à nouveau les sujets cyber.

III. CE QUI A DÉJÀ ÉTÉ FAIT : UN RENFORCEMENT DES MOYENS ET DES CAPACITÉS JURIDIQUES ET TECHNIQUES

Identifiée comme un domaine critique devant faire l'objet d'une attention particulière dans le Livre blanc de 2008, la cyberdéfense n'a depuis lors cessé de faire l'objet de dispositions spécifiques tendant à renforcer les capacités de notre pays en la matière, notamment à l'occasion des lois de programmation militaire successives.

A. SOUS LA PRÉCÉDENTE LÉGISLATURE : LA LOI DE PROGRAMMATION MILITAIRE 2014-2019 ET LA LOI DE JUILLET 2015 SUR LE RENSEIGNEMENT

1. La LPM 2014-2019 : l'augmentation des capacités et la création d'un cadre juridique inédit applicable aux OIV

a. Le renforcement des capacités techniques et des moyens

● L'article 21 de la loi de programmation militaire 2014-2019 [(1)] a en premier lieu consacré juridiquement l'importance de la cyberdéfense en précisant que la définition et la coordination de l'action gouvernementale en matière de sécurité et de défense des systèmes d'information relevaient de la compétence du Premier ministre, et que celui-ci disposait à cette fin de l'ANSSI, autorité nationale de défense des systèmes d'information [(2)].

● Le même article autorisait par ailleurs les services de l'État à accéder à des systèmes automatisés de données à l'origine d'une attaque informatique et à détenir les équipements nécessaires pour interagir afin de repousser l'attaque, ces dispositions ayant vocation à répondre aux attaques informatiques les plus malveillantes, à savoir celles visant « *les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* » [(3)].

● Pour les seuls besoins de la sécurité des systèmes d'information de l'État et des OIV, l'article 24 de cette LPM permet quant à lui à l'ANSSI d'obtenir des opérateurs de communications électroniques un certain nombre d'informations afin d'alerter les utilisateurs ou détenteurs de systèmes d'information vulnérables, menacés ou attaqués, de la compromission ou de la vulnérabilité desdits systèmes [(4)].

---

(1) Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
(2) Dispositions codifiées à l'article L. 2321-1 du code de la défense.
(3) Article L. 2321-2 du code de la défense.
(4) Article L. 2321-3 du code de la défense.

● La LPM 2014-2019 prévoyait enfin d'augmenter les effectifs de l'ANSSI de 357 à 500 personnes en 2015, les moyens consacrés par le ministère de la Défense à la cyberdéfense devant également poursuivre leur montée en puissance avec le recrutement « *d'au moins* » 350 personnels supplémentaires sur la période 2014-2019. Les effectifs du pôle « sécurité des systèmes d'information » de la DGA, qui avaient déjà fait l'objet d'une augmentation substantielle depuis fin 2010, devaient être doublés en passant d'environ 200 à plus de 400 experts de haut niveau en 2017.

Au total, la LPM consacrait un milliard d'euros au profit de la cyberdéfense, dont 550 millions d'euros d'investissement.

Le ministère de la Défense avait par ailleurs décidé la mise en place d'un plan d'action spécifique, cohérent avec la LPM, dénommé Pacte Défense Cyber et qui comportait six axes [(1)] et cinquante mesures.

Dans sa version actualisée [(2)], la LPM 2014-2019 avait opéré un nouveau renforcement significatif des services chargés de la cyberdéfense au sein du ministère de la Défense, avec une accélération des recrutements devant passer d'au moins 350 à d'au moins 1 000 civils et militaires d'active supplémentaires.

b. La création d'un cadre juridique inédit contraignant pour les OIV

La France a été précurseur dans le domaine de la protection des principaux opérateurs face aux menaces cyber. Comme l'a rappelé M. Guillaume Poupard, directeur général de l'ANSSI devant la commission à l'occasion de l'examen du projet de LPM 2019-2025, « *La France a été le premier pays au monde à développer une telle approche réglementaire et nous pouvons en être fiers […]* » [(3)].

À cet égard, l'article 22 de la LPM 2014-2019 a permis de renforcer les obligations pesant sur les OIV s'agissant de la sécurité et de la défense de leurs systèmes d'information.

---

(1) Axe 1 : durcir le niveau de sécurité des systèmes d'information et les moyens de défense et d'intervention du ministère et de ses grands partenaires de confiance.

Axe 2 : préparer l'avenir en intensifiant l'effort de recherche tant technique et académique qu'opérationnel, tout en soutenant la base industrielle.

Axe 3 : renforcer les ressources humaines dédiées à la cyberdéfense et construire les parcours professionnels associés.

Axe 4 : développer le Pôle d'excellence en cyberdéfense en Bretagne au profit du ministère de la défense et de la communauté nationale de cyberdéfense.

Axe 5 : cultiver un réseau de partenaires étrangers, tant en Europe qu'au sein de l'Alliance Atlantique et dans les zones d'intérêt stratégique.

Axe 6 : favoriser l'émergence d'une communauté nationale défense de cyberdéfense en s'appuyant sur un cercle de partenaires et les réseaux de la réserve.

(2) Loi n° 2015-917 du 28 juillet 2015 actualisant la programmation militaire pour les années 2015 à 2019 et portant diverses dispositions concernant la défense.

(3) Rapport n° 765, tome 2, de M. Jean-Jacques Bridey fait au nom de la commission de la Défense nationale et des forces armées sur le projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense (Assemblée nationale, mars 2018).

De manière schématique, les nouvelles dispositions prévues par le texte se sont traduites pour les OIV par les obligations suivantes :

– des obligations en matière de sécurité de leurs systèmes informatiques, notamment l'installation de dispositifs de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information ;

– l'obligation de déclarer, au Premier ministre, tout incident majeur qui affecterait le fonctionnement ou la sécurité de ces systèmes ;

– l'obligation de soumettre leurs systèmes d'information à un processus de contrôle et d'audit, à la demande du Premier ministre. Les contrôles sont réalisés par l'ANSSI, un service de l'État désigné par le Premier ministre ou un prestataire de services labellisé.

Par ailleurs, en cas de crise majeure menaçant ou affectant la sécurité de leurs systèmes d'information, le Premier ministre peut imposer aux OIV la mise en œuvre des mesures d'urgence susceptibles de répondre à ladite crise.

2. La loi relative au renseignement de juillet 2015 : le dispositif d'« excuse pénale » au bénéfice des « cyber-espions » en cas d'atteinte à des systèmes d'information situés à l'étranger

L'article 18 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement a institué un régime d'irresponsabilité pénale pour les agents des services spécialisés de renseignement amenés à réaliser des opérations de cyberdéfense portant atteinte à des systèmes d'information situés à l'étranger [(1)] afin d'assurer, hors du territoire national, la protection des intérêts fondamentaux de la Nation [(2)].

Il s'agissait ainsi légitimement de protéger les « cyber-espions » qui conduisent, notamment depuis le territoire national et donc passibles de la loi pénale française, des actions intrusives sur les systèmes d'information d'entités menaçant les intérêts fondamentaux français et localisés à l'étranger.

B. LA LOI DE PROGRAMMATION MILITAIRE 2019-2025

Alors que la loi de programmation militaire pour les années 2019-2025 vient d'être votée par le Parlement, il convient de rappeler succinctement les principales évolutions et dispositions prévues par ce texte, tel qu'issu des travaux de l'Assemblée nationale. Celui-ci a fait l'objet d'une analyse détaillée dans le rapport présenté par M. Jean-Jacques Bridey, président de la commission de la Défense de l'Assemblée nationale et rapporteur du projet de loi [(3)].

(1) Dispositions codifiées à l'article 323-8 du code pénal.

(2) Mentionnés à l'article L. 811-3 du code de la sécurité intérieure.

(3) Rapport n° 765, tome 1, de M. Jean-Jacques Bridey fait au nom de la commission de la Défense nationale et des forces armées sur le projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense (Assemblée nationale, mars 2018).

1. Le cyber : l'un des axes prioritaires tant en termes de ressources humaines que de moyens financiers

a. Les moyens

S'agissant des ressources humaines, la LPM 2019-2025 prévoit la création de 1 500 postes dans le domaine de la cyberdéfense et de l'action dans l'espace numérique sur la période couverte par la programmation. Parmi eux, on comptera 1 000 « cyber-combattants » supplémentaires, afin de porter leur nombre total à 4 000 personnels environ.

Environ 500 postes seront placés sous l'autorité du COMCYBER, accompagnant ainsi la montée en puissance de ce nouveau commandement.

En termes financiers, 1,6 milliard d'euros seront investis dans la cyberdéfense et la lutte dans l'espace numérique sur la période 2019-2025.

b. La mise en place d'une « posture permanente cyber »

La prochaine LPM prévoit par ailleurs la création d'une « posture permanente cyber » (PPC), traduisant ainsi l'importance stratégique accordée au cyberespace au même titre que les autres espaces qui disposent de leurs propres postures permanentes [(1)]. Placées sous le contrôle opérationnel du COMCYBER, trois missions principales y sont rattachées :

– surveiller l'espace numérique et détecter les atteintes affectant le ministère des Armées ;

– permettre aux forces de se déployer en sécurité au regard des menaces provenant du cyberespace, et d'accomplir leur mission ;

– contrer les agressions informatiques ou informationnelles, y compris en prenant les mesures visant à faire cesser les effets de l'attaque.

2. L'adaptation du cadre juridique pour une résilience étendue et plus active

L'article 19 vise à renforcer la résilience nationale face aux cyberattaques. Il permettra la mise en œuvre de dispositifs de détection des événements susceptibles de constituer une menace pour certains systèmes d'information nationaux. Deux types d'acteurs pourront recourir à de tels dispositifs :

– les opérateurs de communications électroniques, sur leurs propres réseaux, aux fins de détecter les événements pouvant affecter la sécurité des systèmes d'information qu'ils mettent à la disposition de leurs abonnées ;

(1) Postures permanentes de sécurité aérienne et maritime.

– l'ANSSI, sur certains réseaux et systèmes d'information [(1)], dès lors qu'elle serait informée d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques, des OIV ou des opérateurs de services essentiels.

De manière pratique, les dispositifs permettant de détecter les événements susceptibles de constituer une menace fonctionneront à partir de marqueurs techniques capables de repérer la « signature » d'une cyberattaque. Il peut, par exemple, s'agir de l'adresse IP d'un serveur malveillant, ou du nom d'un site Internet piégé. Les événements repérés correspondront donc aux tentatives d'attaque informatique associées aux marqueurs contenus dans les systèmes de détection mis en place.

L'article 19 impose par ailleurs trois types d'obligations aux opérateurs de communications électroniques :

– ils seront tenus d'informer l'ANSSI sans délai dès lors qu'un événement susceptible d'affecter la sécurité des systèmes d'information serait détecté ;

– sur demande de l'ANSSI, ils devront informer leurs abonnés de la vulnérabilité de leurs systèmes d'information ou de l'atteinte qui y serait portée ;

– dans l'hypothèse où un événement affecterait la sécurité des systèmes d'information d'une autorité publique, d'un OIV ou d'un OSE, l'ANSSI pourrait obtenir d'eux les informations techniques nécessaires à la seule caractérisation de la menace [(2)].

À l'initiative du rapporteur du projet de loi, les débats à l'Assemblée nationale ont permis de compléter le dispositif proposé par le Gouvernement, la modification la plus substantielle ayant trait à la détermination du régime de contrôle des nouvelles dispositions [(3)]. Ce contrôle sera ainsi confié à l'Autorité de régulation des communications électroniques et des postes (ARCEP) et à sa formation de règlement des différends, de poursuite et d'instruction.

3. La consécration officielle du « cyber-combattant » : l'extension du bénéfice de « l'excuse pénale »

Si la protection pénale des « cyber-espions » avait été traitée par la loi de juillet 2015 sur le renseignement, tel n'était pas encore le cas des « cyber-combattants » agissant dans le cadre d'opérations extérieures.

L'article 23 de la prochaine LPM étend donc le régime protecteur de « l'excuse pénale » aux cyber-combattants en ajoutant les actions numériques à la liste des actions au titre desquelles la responsabilité pénale des militaires

(1) Réseau d'un opérateur de communications électroniques ou système d'information d'un fournisseur d'accès ou d'un hébergeur.

(2) Les adresses IP source et destination ou encore le type de protocole utilisé, par exemple.

(3) Qui, aux termes de l'article 20 du projet de loi, devait initialement être élaboré par voie d'ordonnances.

concernés ne saurait être engagée, dès lors que de telles actions sont assimilables à un recours à la force et qu'elles sont réalisées dans le cadre d'opérations extérieures. Les critères et limites traditionnels [1] de « l'excuse pénale » sont naturellement applicables aux nouveaux bénéficiaires de ce régime.

En définitive, l'article 23 de la LPM consacre l'intégration pleine et entière de l'action cyber et des cyber-combattants dans le champ de la confrontation militaire.

(1) Notamment, le recours à la force doit s'effectuer dans le respect des règles du droit international applicables et son usage doit être nécessaire à l'exercice de la mission conduite.

IV. AU-DELÀ DES AVANCÉES RÉALISÉES ET DU RENFORCEMENT DES MOYENS DÉJÀ OPÉRÉ, D'AUTRES PISTES D'ÉVOLUTION SONT ENVISAGEABLES

Le cyber étant par nature un espace mouvant, protéiforme et en recomposition permanente, il suppose une adaptation constante de la part de l'ensemble des acteurs afin d'augmenter la résilience globale de la société, de renforcer ses capacités d'anticipation de la menace, de défense et de riposte, et de promouvoir un certain nombre de valeurs au niveau international.

A. POUR UNE LOI « CYBER »

Au-delà des observations et préconisations présentées ci-après, les rapporteurs estiment que, par principe, il conviendrait d'envisager l'élaboration d'une loi « cyber », à l'image des lois « informatique et liberté » [(1)] ou encore « bioéthiques » [(2)].

En effet, le caractère global de la question cyber, qui touche l'ensemble des acteurs publics comme privés et l'ensemble des secteurs socio-économiques justifie, selon eux :

– une analyse approfondie et complète du sujet à l'échelle de notre pays, laquelle devrait probablement être menée sur plusieurs mois compte tenu de l'ampleur d'un tel travail ;

– la mise en place d'un cadre global et adapté, au-delà des dispositions qui ont été élaborées jusqu'alors et qui ne concernent qu'un nombre réduit d'acteurs très spécifiques (certaines personnes publiques, OIV, opérateurs de communications électroniques, certaines industries, etc.).

Une telle loi permettrait d'établir, à l'échelle nationale, une cartographie précise des vulnérabilités et des besoins, d'évaluer les ressources financières, matérielles et techniques nécessaires, et de déterminer les politiques et orientations à mettre en œuvre (politique industrielle, de recherche, adaptation du cadre juridique, etc.), de la part des autorités publiques comme des acteurs privés, pour adapter notre modèle.

Comme les lois « bioéthiques », cette loi « cyber » pourrait faire l'objet d'un suivi et de mises à jour régulières. À cet effet, un comité consultatif national du cyber pourrait être créé, qui rassemblerait l'ensemble des acteurs, de toutes qualités : politiques de tous niveaux (national, local), experts (chercheurs dans le domaine du cyber « dur » comme dans le champ des sciences sociales,

(1) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) Notamment les lois du 29 juillet 1994 n° 94-653 relative au respect du corps humain et n° 94-654 relative au don et à l'utilisation des éléments et produits du corps humain, à l'assistance médicale à la procréation et au diagnostic prénatal.

techniciens, juristes, etc.), représentants de l'administration, représentants des acteurs économiques (en s'appuyant, par exemple, sur les syndicats ou les fédérations professionnelles), associations, citoyennes et citoyens, etc.

Une telle instance n'aurait pas nécessairement vocation à présenter un caractère permanent, à l'image du Comité consultatif national d'éthique, et pourrait n'être saisie que dès lors qu'une révision de la loi « cyber » serait envisagée. Le comité serait alors chargé des travaux préparatoires à une telle révision, dans le but d'éclairer les pouvoirs publics. Compte tenu du caractère extrêmement mouvant des questions cyber, la réactivité et l'agilité devraient être recherchées. Aussi, et contrairement aux dispositions prévues pour les lois « bioéthiques », il semblerait préférable de ne pas déterminer, par la loi, un délai maximal entre les révisions (sept ans maximum pour les lois « bioéthiques »), mais de privilégier des révisions en tant que de besoin. À l'issue du processus de révision, après la promulgation de la nouvelle loi « cyber », le suivi du texte pourrait être assuré par des structures existantes, à l'image de l'ANSSI.

B. RECOUVRER NOTRE SOUVERAINETÉ NUMÉRIQUE, AUX NIVEAUX NATIONAL EN PREMIER LIEU ET EUROPÉEN EN SECOND LIEU

1. Garantir la souveraineté s'agissant des données en créant des espaces de stockage souverains nationaux et européens

● Affirmer la nécessité de créer des espaces de stockage souverains, permettant de rapatrier et de stocker des données sur des territoires sous juridiction nationale ou européenne.

Les rapporteurs ont acquis une certitude à l'occasion de leurs travaux. Il est nécessaire de rapatrier et de stocker les données les plus sensibles relatives à des acteurs européens (citoyennes et citoyens ou personnes juridiques) en France et en Europe, sur des territoires sous juridiction européenne.

En effet, les données stockées à l'étranger ne bénéficient d'aucune garantie quant à leur sécurité. Par ailleurs, la prétention à l'extraterritorialité de certaines législations nationales aboutit à attraire dans le champ du droit d'un pays donné des éléments qui seraient pourtant stockés sur le territoire d'un autre État. Tel est le cas du droit américain [(1)]. Ainsi, des données stockées hors des États-Unis mais sur des serveurs appartenant à des sociétés américaines ne peuvent être considérées comme totalement sécurisées.

(1) Pour davantage de précisions à ce sujet, on se reportera au rapport sur l'extraterritorialité de la législation américaine, fait par Mme Karine Berger (rapporteure) et M. Pierre Lellouche (président) au nom des commissions des Affaires étrangères et des Finances (Assemblée nationale, rapport n° 4082, XIVe législature).

Dès lors, il conviendrait de développer des espaces de stockage à distance – en *cloud* [(1)] – ou des centres de stockage « en dur », en premier lieu sur le territoire national pour les données considérées comme sensibles. Même si, intuitivement, au regard des géants que sont les États-Unis, la Chine et la Russie, le niveau européen peut apparaître comme le niveau de référence pour la constitution de tels espaces compte tenu de la « taille critique » du territoire européen, il est en effet évident que certaines données devraient rester sous souveraineté nationale. S'ils sont bien conscients que le *cloud* souverain n'est qu'un levier, et non l'alpha et l'oméga de la sécurisation des données, les rapporteurs n'en sont pas moins persuadés qu'il est indispensable de travailler à l'élaboration d'un *cloud* souverain viable, en tirant les leçons des échecs récents [(2)].

Ainsi la puissance publique pourrait, dans son rôle de facilitateur, de catalyseur, de régulateur et de soutien – politique mais également financier –, s'appuyer sur des acteurs privés existants ayant fait leurs preuves pour faire émerger des solutions souveraines de stockage de données, mais également de surveillance de ces stockages, en proposant notamment des produits adaptés aux besoins des PME/PMI détenant des données sensibles.

L'utilisation des solutions de stockage souveraines pourrait être rendue obligatoire pour les autorités publiques nationales comme pour les collectivités territoriales, pour les OIV et pour les entreprises de la BITD – cas sur lequel les rapporteurs reviendront ultérieurement. Toutefois il est illusoire et inutile de vouloir protéger l'ensemble des données détenues par ces entités. Un travail préalable de classification des données, dont une partie seulement a vocation à être stockée dans un espace souverain, doit impérativement être effectué en amont. Cette évaluation de la nature des données et du niveau de protection requis est le gage de l'efficacité et, *in fine*, de la viabilité des solutions qui seront proposées. La possibilité d'utiliser ces solutions pourrait être ouverte aux autres acteurs nationaux qui le souhaiteraient. Les entreprises qui décideraient d'y recourir pourraient se voir délivrer par l'ANSSI un certificat qui témoignerait du degré de sécurisation de leurs données. La détention d'un tel certificat pourrait constituer un critère de valorisation des offres dans le cadre de l'attribution des marchés publics, sous réserve naturellement du respect de la réglementation européenne applicable et du code des marchés publics.

Sans se fondre dans un *cloud* transnational, les solutions nationales adoptées par la France et d'autres pays de l'Union européenne devront ouvrir la voie à un second niveau de stockage souverain, à l'échelle européenne, assurant aux données éligibles, qu'il conviendra de définir, un haut degré de protection.

---

(1) Technologie permettant de stocker des données habituellement contenues sur des espaces de stockage locaux (ordinateurs, serveurs locaux) sur des serveurs situés à distance.

(2) Avec les projets Cloudwatt et Numergy issus du projet de cloud *souverain Andromède lancé à l'initiative du gouvernement français en 2011.*

Au total, ces solutions de stockage souveraines permettraient, d'une part, d'assurer de manière plus efficace la protection des données de l'ensemble des citoyennes et citoyens, administrations et entreprises européens et, d'autre part, de réduire la dépendance de nos sociétés vis-à-vis de monopoles ou d'oligopoles numériques étrangers (GAFAM notamment). Au-delà de la seule question du stockage, il est également nécessaire de disposer d'une certaine maîtrise de l'ensemble de l'écosystème, qui passe notamment par l'existence de solutions techniques alternatives nationales et européennes dans le domaine des logiciels, des composants, etc.

Il est tout aussi essentiel de disposer de solutions de chiffrement robustes qui permettent non seulement d'assurer la confidentialité des données – ou des bases de données, telles que l'état civil [(1)] –, mais également leur intégrité. Il s'agit d'un enjeu essentiel, au moins aussi important que celui de la confidentialité. En effet, l'altération de certaines informations, qui serait imperceptible compte tenu de la masse globale de données, pourrait avoir des conséquences particulièrement préoccupantes. Ainsi de la modification de casiers judiciaires, par exemple.

2. Favoriser l'émergence de solutions techniques nationales et européennes de confiance

À titre liminaire, il convient de rappeler que, pour qu'un système soit souverain, il n'est pas forcément nécessaire que l'ensemble des « briques » qui le composent soient elles-mêmes souveraines. Il est seulement nécessaire que certaines d'entre elles, les plus sensibles et les plus essentielles au fonctionnement du système, le soient. Les matériels de défense en fournissent un exemple particulièrement éclairant. Tous les équipements mis en œuvre par les armées françaises ne sont pas, loin s'en faut, de fabrication nationale. Plus encore, même des matériels et équipements conçus et produits par des entreprises nationales peuvent contenir des composants non-souverains (micro-processeurs, logiciels, etc.). Pour autant, la défense demeure l'une des composantes majeures – si ce n'est la première – de la souveraineté de l'État et l'exercice de cette défense est la matérialisation la plus indéniable cette souveraineté.

Il n'en demeure pas moins que les pouvoirs publics et les acteurs économiques concernés pourraient favoriser l'émergence de solutions techniques dans les domaines de l'édition de logiciels et de la conception de produits technologiques, y compris grand public (moteurs de recherche, systèmes d'exploitation, logiciels de bureautique, d'administration, de gestion, etc.). Car, à l'heure actuelle, le secteur des infrastructures et des applications informatiques est en réalité dominé par des monopoles ou quasi-monopoles extra-européens, qu'ils soient américains ou chinois [(2)]. Dans l'idéal, les solutions en *open source*

(1) D'ores et déjà, les prestataires auxquels les mairies confient la numérisation et l'indexation des actes d'état civil doivent s'engager à ce que les données ne quittent pas le territoire français lors de leur traitement, conformément à l'article 11 du décret n° 2017-890 du 6 mai 2017 relatif à l'état civil.

(2) Avec, notamment, les entreprises Microsoft, Cisco, Huawei, HP, Lenovo, ou encore Dell.

devraient être favorisées pour permettre un accès facilité, notamment aux petites collectivités territoriales et aux PME.

Il convient également de souligner les risques liés à l'infogérance, méthode de sous-traitance des tâches informatiques (développement, conception, exploitation, hébergement des applications métier) à laquelle recourt de plus en plus régulièrement l'État. Or une telle externalisation peut constituer un risque si la sécurité ne fait pas l'objet d'attentions particulières, de la part du client comme du prestataire extérieur. Ainsi, en 2017, la Suède a subi une fuite des données de l'ensemble de sa base de gestion des permis de conduire à la suite d'une défaillance d'un prestataire.

S'agissant des solutions de cyber-protection, les grandes entreprises intervenant dans le secteur, de même que de nombreuses PME, ETI ou start-up françaises offrent déjà une large gamme de produits et de services : solutions de chiffrement, protection du poste de travail, *firewall* (1), VPN (2), audit sécurité, tests d'intrusion, etc. Toutefois, certaines technologies restent encore l'apanage de sociétés étrangères, et notamment américaines, qu'il s'agisse des antivirus, des *sandboxes* (3)ou encore des SIEM (4). En somme, dans ces domaines, il n'existe pour ainsi dire pas de produits souverains, ni nationaux, ni européens.

Dès lors que leur production serait économiquement viable, de tels outils permettraient de réduire le degré de dépendance de nos sociétés vis-à-vis de productions étrangères pouvant présenter des risques (5) et participeraient au renforcement de la souveraineté industrielle nationale, voire européenne. Une fois encore, à côté de « l'Europe du *cloud* », « l'Europe du logiciel » pourrait constituer un projet concret et fédérateur.

Les pouvoirs publics nationaux pourraient promouvoir les solutions déjà existantes, voire favoriser leur utilisation « en donnant l'exemple », dès lors que les produits considérés sont sécurisés et fiables. À titre d'exemple, combien de Françaises et de Français connaissent – et, *a fortiori*, utilisent – le moteur de recherche français Qwant, alternative à l'américain Google, plus respectueux de la

(1) Pare-feu : dispositif de filtrage des flux entre deux réseaux sur la base de règles de sécurité prédéfinies.

(2) Virtual Private Network *(réseau virtuel privé) : système permettant de construire un réseau privé au sein d'une structure informatique publique. Le VPN permet de monter un lien direct chiffré, donc sécurisé, entre des équipements géographiquement distants à travers un réseau non fiable car ouvert.*

(3) Ou « bac à sable » : dispositif permettant l'ouverture ou l'exécution d'un fichier dans un environnement virtuel isolé afin de vérifier son innocuité. Une sandbox *permet ainsi, par exemple, de prévenir l'activation de virus en les « testant » en environnement fermé.*

(4) Security Information & Event Management *: outil de gestion des journaux et événements de sécurité.*

(5) Il n'est techniquement pas exclu que certains composants puissent être piégés « à la source » et constituent ainsi des backdoors *(portes dérobées) permettant, par exemple, de prendre le contrôle à distance de certains équipements (les* backdoors *font référence aux accès dissimulés, soit logiciels soit matériels, qui permettent à un utilisateur malveillant de se connecter à une machine de manière furtive – définition ANSSI).*

vie privée de ses utilisateurs [1] et plus neutre dans l'affichage des résultats de recherche ? [2]

De fait, les produits de cyber-protection français et, plus généralement, les technologies du numérique françaises, éprouvent souvent des difficultés à « percer » en raison de prix généralement plus élevés que ceux de la concurrence, du fait notamment d'un manque de publicité et de diffusion à grande échelle [3]. À travers leur politique d'achat, et dans le respect du code des marchés publics comme de la réglementation européenne, les collectivités publiques notamment pourraient favoriser le soutien à de telles sociétés, en leur ouvrant la perspective d'un volume d'affaires susceptible d'accompagner leur croissance.

En somme, évacuer tout risque ou doute sur un matériel étranger suppose le retour et la mise en œuvre d'une politique industrielle souveraine dans certains domaines, au niveau national ou au niveau européen.

C. RENFORCER LA RÉSILIENCE DE L'ENSEMBLE DES ACTEURS NATIONAUX

1. Les autorités publiques

● Les auditions que les rapporteurs ont pu mener les amènent à estimer que, en dehors d'autorités publiques très spécifiques –sachant que, même pour elles, le « risque cyber zéro » est une illusion – nombre d'autorités publiques nationales et, *a fortiori*, locales, ne présentent pas un degré de sécurité suffisant face aux menaces cyber.

Si certains ministères, comme ceux des Armées ou de l'Intérieur, sont, par nécessité et par « culture », particulièrement conscients des enjeux et des risques, tel n'est pas forcément le cas d'autres secteurs de l'administration au sens large. Certains peuvent considérer qu'ils manipulent des « matières » moins sensibles que les secteurs régaliens. C'est oublier, d'une part, le caractère global de la menace cyber et, d'autre part, l'interconnexion et donc l'interdépendance extrême de l'ensemble de nos systèmes. Or, un attaquant ciblera plus volontiers les maillons les plus faibles d'une chaîne si cela lui permet d'atteindre, par répercussion, les plus forts.

---

(1) L'architecture technique de Qwant a été auditée par la CNIL, lequel n'utilise aucun cookie *(fichier permettant l'identification de l'utilisateur) ou dispositif de traçage et ne conserve pas les historiques de recherche de ses utilisateurs.*

(2) La Caisse des dépôts et consignations fait partie des investisseurs de Qwant.

(3) Ainsi, d'après les informations communiquées aux rapporteurs, le chiffre d'affaires de la plus grosse PME française dans le domaine cyber est équivalent au chiffre d'affaires de la centième PME israélienne du même secteur.

C'est pourquoi il semble indispensable :

– non seulement de durcir les dispositifs de prévention et de protection de l'ensemble des autorités publiques nationales en les alignant davantage – sans les faire coïncider – sur les dispositifs en place au sein des secteurs les plus sensibles ;

– mais également de diffuser plus largement une culture et une conscience du « risque cyber » au sein des administrations par des actions de formation, de pédagogie et de prévention.

● Le même constat et les mêmes conclusions s'imposent s'agissant des collectivités territoriales, qu'il convient d'accompagner plus largement. Cela vaut notamment pour les collectivités les moins importantes, qui ne bénéficient pas forcément des ressources humaines, financières et techniques nécessaires.

À cet égard, un premier travail d'analyse pourrait être conduit avec les associations représentatives des collectivités territoriales : Régions de France, Assemblée des départements de France (ADF), Association des maires de France et des présidents d'intercommunalité (AMF), Association des petites villes de France (APVF).

● Enfin, les acteurs publics de tous niveaux pourraient développer plus largement le recours à une démarche relativement originale afin de tester leurs systèmes et d'identifier leurs vulnérabilités : l'organisation de *bug bounties*.

Un *bug bounty* est le processus par lequel une entité sollicite un groupe de *hackers* de confiance chargés de tester ses systèmes pour en détecter les failles (*bug*) et offre leur une récompense (*bounty*) en retour.

Le cas échéant, il conviendrait naturellement d'encadrer strictement cette pratique, notamment de vérifier le profil et les antécédents des participants, d'imposer des clauses de confidentialité, etc.

2. Les acteurs économiques

● Alors que les grandes entreprises et les grands groupes disposent en général des ressources humaines, techniques et financières adaptées à une gestion satisfaisante du risque cyber, tel n'est pas forcément le cas des sociétés de moindre ampleur telles que les PME et les ETI. Ainsi, d'après les informations communiquées aux rapporteurs et même si une telle charge est très variable selon les structures, on estime que le coût de la cybersécurité représente entre 5 et 10 % du budget informatique d'une entité. On imagine donc aisément l'effort qu'une telle dépense peut représenter pour des sociétés de taille réduite.

Afin de les accompagner plus largement et plus efficacement dans la prise en compte de la question cyber et de les aider à renforcer leur protection et leur résilience face aux menaces potentielles, une « montée en gamme » qui,

rappelons-le, bénéficiera à l'ensemble de la société, plusieurs dispositifs peuvent être envisagés.

● Il convient d'abord de faire évoluer certaines mentalités s'agissant de la protection face aux cybermenaces. Celle-ci ne doit pas être vue uniquement comme une contrainte et une charge financière. En réalité, elle contribue à la performance économique globale et doit être considérée comme un investissement et une assurance, qui permettent notamment de prévenir le « risque réputationnel » qui touche toute entreprise qui serait victime d'une cyberattaque et pourrait ainsi perdre la confiance de ses clients et de ses fournisseurs. Le degré de cyber-protection constitue donc en définitive un avantage compétitif pour une entreprise, sur son marché national comme à l'export.

Une telle prise de conscience est d'autant plus importante que l'usine 4.0 [(1)] (ou *smart factory*) qui intégrera massivement les technologies numériques dans ses processus de fabrication sera, par nature, à risque.

● Par ailleurs, il faut renforcer les dispositifs d'assistance à destination des acteurs les « moins bien armés » face à la menace cyber. Cela passe par des actions plus nombreuses et plus fortes de l'ANSSI par le biais de son réseau régional, et par des actions de prévention et de promotion de la « cyber-hygiène » dans le milieu du travail.

3. Le renforcement du réseau régional de l'ANSSI au bénéfice des acteurs territoriaux publics et privés, en métropole comme dans les outremers

● Afin de répondre à un certain nombre d'enjeux évoqués précédemment, notamment s'agissant des petites collectivités et des PME, le réseau régional de l'ANSSI pourrait utilement être mobilisé et renforcé. En effet, les délégués de l'ANSSI en régions constituent une ressource particulièrement utile dans le domaine de la prévention et de la sensibilisation des acteurs locaux tant publics que privés.

Leurs principales missions sont les suivantes :

– la sensibilisation des collectivités territoriales et des entreprises. Les délégués de l'ANSSI leur dispensent des conseils « de premier niveau » afin de renforcer la prise en compte de la sécurité des systèmes d'information ;

– l'animation de réseaux. Les délégués identifient les différents relais (pôles de compétitivité, syndicats mixtes, etc.) et coordonnent l'action des acteurs locaux (associations, chambres consulaires, etc.) ;

– le soutien de proximité des OIV ;

(1) La révolution numérique est présentée comme la quatrième révolution industrielle après la mécanisation, la production de masse et l'automatisation de la production.

– le développement de la politique industrielle, afin d'orienter les entreprises vers les points de contact de l'ANSSI ;

– le lien avec l'enseignement supérieur et la recherche, afin d'identifier les formations supérieures et centres de recherche susceptibles de collaborer avec l'ANSSI ;

– la promotion de la protection du potentiel scientifique et technique de la Nation, notamment vis-à-vis des établissements publics et privés concernés conduisant des activités de recherche et de production.

Chacune des treize régions métropolitaines devrait compter, à terme, un délégué de l'ANSSI sur son territoire [(1)]. En dépit de leurs qualités et compte tenu de la taille des régions administratives, il semble nécessaire de renforcer la présence territoriale de l'ANSSI en augmentant le nombre de délégués dans chaque région.

Par ailleurs, il faudrait compléter le dispositif territorial de l'ANSSI au-delà de la seule métropole puisqu'aucun délégué n'est en poste dans les outremers. Il semble nécessaire de remédier à cette carence en dupliquant, dans les territoires ultramarins, le réseau régional existant en métropole. Dans un premier temps et compte tenu de la croissance des effectifs de l'ANSSI telle qu'elle est actuellement prévue, des actions de coopération pourraient être élaborées et poursuivies avec les services de l'État et les collectivités territoriales dans ces territoires.

● Les rapporteurs estiment enfin nécessaire de mettre en place des « référents cyber » au sein des collectivités territoriales, établissements publics et entreprises, en fonction de leur taille (seuil relatif au nombre d'agents ou de salariés) et de leur secteur d'activité. Les délégués du réseau régional de l'ANSSI contribueraient à la formation et à la sensibilisation de ces référents, qui n'ont naturellement pas vocation à devenir des techniciens experts, mais à constituer une « personne ressource » de premier niveau au sein de leur organisation.

4. Les citoyennes et les citoyens

● Chacun, à son niveau, doit être acteur de sa propre cybersécurité et participer ainsi à la résilience globale. C'est pourquoi il importe d'éveiller toutes les citoyennes et tous les citoyens, dès leur plus jeune âge à la « cyber-hygiène ».

À cet égard, des partenariats doivent être mis en place et renforcés tant avec les acteurs publics – l'Éducation nationale notamment – qu'avec les acteurs privés – par des actions de sensibilisation dans le milieu du travail. Cet aspect dépasse sans doute le cadre strict d'un rapport de la commission de la Défense, mais il est essentiel aux yeux des rapporteurs tant il apparaît que les citoyennes

(1) D'après les dernières informations disponibles, seuls onze sont actuellement en poste, l'un d'entre eux étant par ailleurs compétent pour la région Provence-Alpes-Côte d'Azur et la Corse.

françaises et les citoyens français semblent moins au fait que d'autres – Anglais, Américains notamment – des enjeux cyber.

Il convient à ce titre de saluer les initiatives de l'ANSSI, qui a développé un MOOC [(1)] dénommé SecNumacadémie et qui constitue un programme en ligne de sensibilisation à la sécurité du numérique. Comportant quatre modules [(2)] de cinq unités chacun [(3)], SecNumacadémie a pour but de sensibiliser les utilisateurs aux questions de sécurité dans le monde numérique en assimilant les notions de base de la sécurité des systèmes d'information. Ces premiers modules connaissent un succès très encourageant, avec 63 000 inscrits.

Les rapporteurs préconisent pour leur part la création d'une nouvelle filière menant à l'obtention d'un CAPES d'enseignement numérique dont les titulaires accompagneraient et formeraient les élèves du secondaire, au collège et au lycée, par le biais d'enseignements spécifiques. Cet enseignement à part entière comprendrait, outre celui de la matière informatique, un éveil à la « cyber-hygiène » et l'enseignement des langages informatiques et de la programmation.

Outre son bien-fondé intrinsèque, cet enseignement aurait l'avantage de développer des compétences transverses dont la capacité d'analyse, la logique et la résolution de problème. Cet enseignement permettrait également de démystifier la matière et d'attirer plus de filles vers les métiers du numérique qui demeurent aujourd'hui majoritairement masculins.

Si des modules sont apparus dans le cursus scolaire français, le Royaume-Uni a introduit en 2014 la matière *computing* dans le programme des écoles primaires et secondaires au même titre que les matières classiques. Au Japon, l'apprentissage du code informatique sera obligatoire dans les écoles primaires en 2020, au collège en 2021 et au lycée en 2022 [(4)]. Il est enseigné au lycée en Israël depuis l'an 2000.

● Des initiatives sont également envisageables à destination de la citoyenne et du citoyen consommateurs et utilisateurs de technologie. Alors que les enfants disposent de leur premier téléphone mobile à l'âge de 11 ans en moyenne, les rapporteurs estiment qu'il serait utile que la notice d'utilisation et l'emballage de chaque produit technologique et numérique grand public (*smartphones*, ordinateurs notamment) comportent une liste des principaux risques et mises en garde associés à l'usage de tels appareils à l'instar des activités ou des produits potentiellement porteurs de danger et/ou à l'origine d'addictions que sont l'alcool, le tabac ou les jeux d'argent.

(1) Massive Open Online Course *(cours en ligne ouvert et massif).*
(2) Par exemple : « Sécurité sur Internet : les bons réflexes ».
(3) Par exemple : « La sécurité du poste de travail ».
(4) http://www.japanfm.fr.

D. CONSOLIDER UNE BASE INDUSTRIELLE ET TECHNOLOGIQUE DE DÉFENSE CYBER

1. Une prise en compte spécifique du risque cyber dans les entreprises de défense

On comprend de manière intuitive en quoi les entreprises de la défense présentent des spécificités au regard de la menace cyber. Non pas que la nature et le but des cyberattaques diffèrent pour ces entreprises. Mais la confidentialité de certaines des données dont elles ont connaissance et qu'elles exploitent, la sensibilité des équipements qu'elles produisent et leur vocation première – participer directement à la construction, à la permanence et à l'exercice de la souveraineté de l'État au moyen de la mobilisation de ses forces armées – les contraint à ériger des protections encore plus robustes contre les cyberattaques.

Les cyber-menaces peuvent toucher les entreprises de la BITD à double titre : elles peuvent aussi bien affecter le processus de développement et de production des matériels et équipements que ces matériels et équipements eux-mêmes.

Ces équipements sont par nature vulnérables car ils comprennent tous des composants susceptibles de constituer des cibles, qu'il s'agisse de microprocesseurs, des logiciels utilisés ou du simple fait que ces matériels disposent d'une mémoire. Par principe, ces équipements sont en situation dite d'*air gap* : afin de rendre toute tentative de compromission à distance impossible, ils ne sont connectés qu'à des sous-réseaux internes cloisonnés et ne disposent d'aucun accès à des réseaux externes, *a fortiori* à Internet. Ils ne sont toutefois pas totalement déconnectés du monde et donc des menaces extérieures puisqu'ils restent attaquables par le biais des ports réseaux de communication, des ports USB et des interfaces utilisateurs.

Tout en restant lucide quant au niveau de la menace cyber, il convient de rappeler cette réalité, précédemment évoquée : pour qu'une cyberattaque produise tous les effets souhaités par son auteur, elle suppose une connaissance technique très fine, par celui-ci, des systèmes et des équipements attaqués ainsi que de leur fonctionnement. Or, par nature, les équipements de défense sont souvent des objets de haute technologie d'une extrême complexité dont les clés de compréhension ne sont pas à la portée de tout *hacker*, même agissant pour le compte d'un État. Sans connivence interne à l'entreprise, délibérée ou fortuite, les connaissances nécessaires sont difficiles à obtenir.

● Globalement, deux éléments essentiels doivent être pris en compte face aux cyber-menaces :

– la confidentialité : l'extrême sensibilité du traitement de la problématique cyber exige une grande confidentialité en interne sur la nature des solutions retenues ;

– l'optimisation : qu'il s'agisse de la protection du processus de développement et de fabrication ou de l'intégration de solutions de protection dans les produits finis, un compromis doit être trouvé entre protection, coût et performances. De fait, les solutions de protection retenues sont toujours le résultat de la conciliation de trois contraintes contradictoires : la performance de la protection cyber à mettre en place ; la satisfaction des exigences opérationnelles des produits (les protections ne doivent pas pénaliser outre mesure les performances) ; et la compétitivité de l'entreprise (le coût de la protection, qui peut notamment se traduire par un renchérissement du prix de vente, doit être contenu). Notamment, il convient d'éviter une approche « maximaliste » qui consisterait à intégrer systématiquement l'ensemble des options « protection cyber » sur chaque vulnérabilité potentielle et sans vision d'ensemble de l'architecture globale du système ou du produit.

Le tableau suivant, qui reprend les informations transmises par les industriels aux rapporteurs, retrace de manière schématique et non exhaustive les principaux événements résultant d'une cyberattaque et susceptibles d'affecter les systèmes d'information et les chaînes de production, ainsi que leurs potentielles conséquences.

LES POSSIBLES CONSÉQUENCES INDUSTRIELLES D'UNE CYBERATTAQUE

ÉVÉNEMENT	
Exfiltration de données sensibles (par type de données)	**Conséquences**
Données commerciales, avant la signature de contrat	• Difficulté à négocier, • Perte du contrat au bénéfice d'un concurrent
Données classifiées de défense	• Mise en danger de la sécurité de la Nation • Perte de confiance des autorités nationales • Perte de confiance des clients étrangers • Conséquences pénales
Données R&D	• Perte d'avance technologique • Perte de marché
Données relatives au potentiel scientifique et technique de la Nation	• Perte d'avance technologique • Perte de marché • Conséquences juridiques
Données produits sensibles (document de formation document de maintenance, etc.)	• Perte d'image, • Perte de confiance des clients
Données personnelles	• Perte financière directe (amende allant jusqu'à 4 % du chiffre d'affaires [(1)]) • Conséquences pénales • Perte d'image • Perte de confiance des clients et des sous-traitants

(1) En application des dispositions du RGPD.

Indisponibilité du système d'information (nature de l'atteinte)	Conséquences
Chiffrement des données par un *ransomware*	Retard dans le développement des projets
Virus rendant inopérant les infrastructures de production	Retard de production
Prise de contrôle des systèmes de production	Retard de production
Modification des données (par type de données)	**Conséquences**
Protocole de test	Perte d'intégrité du produit : risque sur sa performance
Résultats de test	Perte d'intégrité du produit : risque sur sa performance
Données de définition	Perte d'intégrité du produit : risque sur sa performance
Données de production	Perte d'intégrité du produit : risque sur sa performance

Source : informations communiquées par les industriels auditionnés.

● Naturellement, au-delà des protections techniques, il est essentiel de sensibiliser les personnels au risque cyber. Le caractère d'entreprise de défense fait qu'il existe par nature une forte culture de sécurité parmi les salariés de la BITD. Mais il convient de maintenir ce degré de vigilance, en usant de toute la palette des actions possibles : actions de formation et de sensibilisation [(1)], voire mesures contraignantes (par exemple, l'interdiction d'accès aux boîtes mail personnelles par l'intermédiaire des réseaux de l'entreprise, l'interdiction des clés USB personnelles ou promotionnelles, ou encore la diffusion d'une « liste blanche » des sites autorisés).

● Quelques statistiques, fournies par un industriel auditionné par les rapporteurs permettent d'appréhender l'ampleur de la tâche à laquelle font face les équipes en charge de la détection et de l'analyse des incidents de sécurité sur les systèmes d'information.

Ainsi, le bilan d'une année d'activité du centre opérationnel de sécurité (ou SOC, pour *Security Opérations Center*) d'une grande entreprise du secteur de la défense fait apparaître les statistiques suivantes : sur les quelque 48,5 milliards d'événements collectés, environ 27 000 constituaient des alertes potentielles. L'analyse de ces alertes potentielles par les équipes du SOC a permis d'identifier environ 4 000 attaques potentielles. Des analyses plus poussées ont réduit ce nombre à près de 1 800 cas d'attaques avérées, dont quatre ont eu un impact considéré comme faible pour la société (le reliquat n'en ayant eu aucun).

(1) MBDA France a par exemple créé une bande dessinée, « La stratégie de l'araignée », visant à prévenir les comportements à risque et disponible sur l'intranet du groupe.

2. Garantir la protection de la BITD

● Si la question de la protection des entreprises en général, et notamment des PME et ETI, a déjà été abordée, le secteur des entreprises de défense nécessite évidemment des développements particuliers compte tenu de la sensibilité de leurs productions et de leur rôle en matière de souveraineté nationale.

Au-delà des questions relatives à la protection et à la résilience des systèmes, aux aspects opérationnels ou aux moyens tant humains que budgétaires, le cyber irrigue également le champ de la conception, de la production et de la maintenance des systèmes d'armes et équipements ayant vocation à être opérés et mis en œuvre par les forces armées. L'aspect cyber doit être pris en compte nativement dans les programmes d'armement. Il s'agit d'un enjeu majeur dans le contexte de la numérisation croissante de l'environnement de combat et de l'interconnexion toujours plus poussée des différents systèmes mis en œuvre par les armées. Notamment, la numérisation des armées accroît mécaniquement leur surface d'exposition au risque cyber (1).

D'après les informations communiquées aux rapporteurs, la DGA doit prochainement notifier à chacun des grands maîtres d'œuvre industriels un contrat-cadre afin de mieux définir avec eux les menaces cyber à prendre en considération dans le développement des futurs systèmes d'armes, ainsi que les mesures à mettre en œuvre au sein des entreprises.

● Les rapporteurs estiment en premier lieu essentiel d'inciter à la « cyber-solidarité » au sein de la BITD. Celle-ci doit se matérialiser par un soutien plus prononcé des grands groupes à leurs chaînes de sous-traitants. Il peut prendre la forme d'actions de sensibilisation, mais également d'un soutien technique et financier pour assurer la « montée en gamme » de l'ensemble de la chaîne de la BITD. Il s'agit en réalité d'un investissement mutuellement profitable. Face au niveau de sécurité des grandes entreprises et grands groupes de défense, un cyberattaquant peut logiquement favoriser une attaque indirecte, par le biais d'un sous-traitant moins protégé, qu'une attaque « frontale » sur sa cible principale.

À cet égard, des négociations et des accords pourraient être conclus avec et au sein des groupements industriels : GICAN, GICAT, GIFAS, Comité Richelieu, etc. Par ailleurs, l'État aurait un rôle moteur, voire contraignant, à jouer dans les groupes et entreprises au sein desquels il détient des participations, parfois majoritaires.

En somme, et même si certaines entreprises ont déjà entrepris un tel travail vis-à-vis de leur *supply-chain* (2), il convient de soutenir et de développer la

---

(1) Pour des développements précis sur le processus de numérisation des armées, voir rapport d'information sur les enjeux de la numérisation des armées op. cit.

*(2) Avec une assistance apportée dans la gestion des vulnérabilités, dans la mise en place d'organisations, d'outils et de processus pertinents eu égard au niveau de sécurité attendu, ou encore en matière de politique d'achat, notamment s'agissant des COTS (*Components Off The Shelf – *achat de composants « sur étagère »).*

« cyber-solidarité » dans l'ensemble de la BITD, là où elle n'existe pas encore, ou trop peu. Des voies pourraient par ailleurs être utilement explorées dans le cadre du Pacte Défense PME [(1)].

Une manière, certes plus contraignante mais nécessaire, de développer cette solidarité et de renforcer la cybersécurité de toute la BITD consisterait à établir la responsabilité du donneur d'ordres sur l'ensemble de sa chaîne de sous-traitants en matière cyber.

● Le financement de la « montée en gamme cyber » des sous-traitants pourrait par ailleurs être assuré par un « fonds cyber », alimenté par des contributions des acteurs de la BITD, mais également par une partie des recettes tirées des exportations d'armement réalisées par l'industrie française. Un taux de retour pourrait ainsi être déterminé chaque année et appliqué aux recettes réalisées l'année précédente.

● Il est également nécessaire d'établir et de mettre à jour régulièrement une cartographie fine des entreprises et compétences critiques au sein de la BITD afin, d'une part, de les sécuriser de manière satisfaisante au niveau « technique » et, d'autre part, de les sécuriser « économiquement » en empêchant le cas échéant les prises de participation, voire de contrôle, par des capitaux étrangers.

À cet égard, il convient de faire un usage, raisonné mais assumé, des dispositions prévues par le décret de 2014 relatif aux investissements étrangers soumis à autorisation préalable [(2)] et codifiées à l'article R. 153-2 du code monétaire et financier. Au-delà de la BITD au sens strict, couverte par ces dispositions, il pourrait même être envisagé de renforcer ce dispositif s'agissant de certaines entreprises du secteur de la sécurité des systèmes d'information. En effet, seules sont actuellement visées les activités de production de biens ou de prestation de services de sécurité dans le secteur de la sécurité des systèmes d'information d'une entreprise liée par contrat passé avec un opérateur public ou privé gérant des installations d'importance vitale. Sans naturellement assécher toute forme de financement extérieur pour ces entreprises – parfois essentiel à leur développement – il pourrait être envisagé, après une étude d'opportunité, de viser également celles qui sont liées par contrat aux grands groupes et entreprises de la BITD.

● Enfin, la protection de la BITD française peut également passer par le recours, déjà évoqué de manière générale, à des solutions de stockage souveraines, qu'elles soient nationales ou européennes.

Au demeurant, les industriels de la défense auditionnés par les rapporteurs se sont unanimement montrés favorables à la mise en place de telles solutions,

(1) Lancé en 2012, le Pacte Défense PME traduit l'engagement du ministère de la Défense pour les PME et ETI, au service de la croissance, de l'innovation et de la compétitivité. Il se décline, concrètement, sous la forme d'une instruction ministérielle qui s'attache à mettre en place une stratégie globale en faveur de ces entreprises.

(2) Décret n° 2014-479 du 14 mai 2014 relatif aux investissements étrangers soumis à autorisation préalable.

notamment d'un *cloud*, et étant entendu que les données jugées particulièrement sensibles continueront de faire l'objet d'un stockage interne isolé de tout réseau externe.

Il conviendrait naturellement de prendre en considération les spécificités de la BITD. Considérant que de nombreux groupes du secteur de la défense ne sont pas uniquement nationaux mais européens, on pourrait ainsi imaginer la mise en place de *clouds* souverains de différents niveaux avec, d'une part et prioritairement, des *clouds* nationaux hébergeant les données classifiées strictement nationales (« Spécial France ») et, d'autre part, un *cloud* européen qui stockerait les données moins sensibles, susceptibles d'être partagées et mises en commun avec l'ensemble des sociétés et filiales, quelle que soit leur nationalité.

En tout état de cause, au-delà de la localisation physique des serveurs de tels *clouds*, il s'agit surtout d'assurer le niveau de protection informatique des données (et des réseaux associés), les données étant par essence « captables » par les acteurs malveillants, que les serveurs soient situés en France ou à l'étranger.

3. Améliorer la régulation concernant certains produits pour limiter la prolifération de technologies offensives et les risques cyber systémiques

● À titre liminaire, il convient sans doute de rappeler les limites de la comparaison, qui est parfois faite, entre le domaine nucléaire et le domaine cyber et sur les limites du raisonnement consistant à dénier à d'autres États la possibilité d'acquérir des capacités en matière de cyberdéfense.

De manière très schématique, on peut évoquer les points suivants. Le développement de l'arme nucléaire nécessite des compétences scientifiques et techniques très poussées et des ressources extrêmement importantes. Pour certaines armes cyber, les technologies sont pour ainsi dire « à portée de clic » et présentent par ailleurs un caractère immatériel. Par ailleurs, l'arme nucléaire constitue « l'arme ultime », dont l'emploi et les effets se caractérisent par leur irréversibilité. Les armes cyber, à ce stade, si elles peuvent gravement et durablement perturber le fonctionnement d'une société, ne présentent pas le même potentiel directement et massivement destructeur. Enfin, arsenal nucléaire et arsenal cyber présentent des dynamiques opposées. Le premier aurait vocation à se réduire progressivement compte tenu de l'existence d'instruments internationaux de contrôle de leur prolifération, tandis que le second a, par nature, vocation à se multiplier.

Mais si le déni d'accès aux technologies cyber pour les acteurs qui n'en seraient pas actuellement dotés semble inatteignable, il est nécessaire de contrôler autant que possible la prolifération des armes numériques afin de neutraliser ou, à tout le moins, de réduire les risques associés les plus importants.

● Même s'il s'agit d'un domaine en perpétuelle évolution, il convient de mener une analyse fine, régulièrement mise à jour, afin de cartographier les potentielles « armes numériques », tout en déterminant les produits et technologies qu'il convient de soumettre aux régimes encadrant les exportations ou transferts intracommunautaires d'armements et de biens à double usage [(1)] (BDU).

Dans ces domaines, ce sont des normes communautaires et internationales qui s'appliquent. Pour les exportations d'armement, il s'agit principalement de la Position commune 2008/944/PESC du 8 décembre 2008 qui établit les règles, communes aux États membres de l'Union européenne, régissant le contrôle des exportations de technologies et d'équipements militaires. Pour les BDU, au niveau communautaire, il s'agit du règlement (CE) n° 428/2009 du 5 mai 2009 relatif au régime de contrôle des exportations, des transferts, du courtage et du transit des biens et technologies à double usage.

Au niveau international et pour ce qui concerne les technologies, le contrôle des armes conventionnelles et des biens et technologies à double usage prend la forme d'un engagement politique dénommé « Arrangement de Wassenaar » [(2)].

Afin de prévenir de la manière la plus efficace possible la conception, voire la prolifération des « armes numériques », une mise à jour plus régulière des listes des produits et technologies susceptibles de constituer ou d'entrer dans la conception de telles armes doit nécessairement être entreprise, tout en gardant à l'esprit :

– que l'élaboration de ces listes résulte de négociations communautaires ou internationales, entre États, et que leur révision n'est pas toujours aisée ou rapide ;

– et qu'inversement, le domaine et les technologies cyber – et, potentiellement, les technologies malveillantes – sont eux en évolution permanente et rapide.

Pour autant et en restant conscient des limites d'un tel exercice, ces constats ne doivent pas conduire les autorités publiques à renoncer, par principe, à l'adaptation régulière des instruments de contrôle, non seulement de manière réactive, mais également de façon proactive.

● Un autre levier de régulation consisterait à envisager, sur le modèle applicable à certains matériels de guerre et assimilés, la prohibition de l'emploi, de

---

(1) Les biens à double usage sont les biens et équipements, y compris les technologies, les logiciels, le savoir-faire immatériel ou intangible, susceptibles d'avoir une utilisation tant civile que militaire ou pouvant aumoins partiellement contribuer au développement, à la production, au maniement, au fonctionnement, à l'entretien, au stockage, à la détection, à l'identification, à la dissémination d'armes de destruction massive.

(2) Ainsi, en 2013, la catégorie des « logiciels d'intrusion » a été intégrée à la liste des BDU de l'Arrangement de Wassenaar.

la fabrication et du commerce [1] de certains produits et logiciels qui seraient considérés parmi les plus « dangereux », notamment ceux dont l'utilisation serait susceptible d'engendrer des risques et des dommages systémiques.

Tel est le cas actuellement d'un certain nombre d'armes : armes biologiques ou à base de toxines, armes chimiques, mines antipersonnel, armes à sous-munitions [2].

Les rapporteurs ne méconnaissent pas la difficulté technique et juridique consistant à apprécier le degré de dangerosité des armes numériques. Contrairement à une arme biologique, par exemple, dont les effets destructeurs sont objectivement et immédiatement observables et quantifiables, tel n'est pas forcément le cas pour une arme numérique, dont les effets dépendent intrinsèquement de ses modalités d'utilisation (intention de l'attaquant, nature de la cible, ampleur de l'attaque, etc.), effets qui, par ailleurs, « échappent » parfois à l'attaquant (en cas de rebonds non anticipés de la cible initiale vers une « victime collatérale », par exemple).

Néanmoins, une analyse de la faisabilité d'une telle interdiction, qui viserait les « armes informatiques à effets massifs » pourrait utilement être entreprise, en concertation notamment avec nos partenaires européens et internationaux, dans les diverses enceintes concernées (COARM [3], Arrangement de Wassenaar, etc.).

● Enfin, dans le cadre d'exportations d'armement et de biens à double usage, il convient sans doute de redoubler de vigilance s'agissant des *offsets* [4], notamment en ce qui concerne les transferts de technologie.

En effet, les transferts de technologie représentent par nature un risque potentiel du point de vue cyber. Si de tels transferts font évidemment l'objet d'un contrôle rigoureux, ils peuvent présenter des risques accrus dès lors que le client aurait accès à certains éléments sensibles du point de vue cyber (codes informatiques, caractéristiques techniques des équipements, etc.). Ce contrôle s'opère en deux temps :

– en amont, par l'industriel fournisseur, qui veille à ne pas proposer à son client des éléments trop sensibles. Une analyse du risque est systématiquement menée s'agissant de la sensibilité des informations et éléments communiqués, en termes de confidentialité et d'intégrité ;

– en aval, par la commission interministérielle pour l'étude des exportations de matériel de guerre (CIEEMG) et par la commission

(1) Plus précisément, de leur : emploi, mise au point, fabrication, production, acquisition, stockage, conservation, offre, cession, importation, exportation, transfert et courtage.

(2) Dont les régimes sont codifiés aux articles L. 2341-1 à L. 2344-11 du code de la défense.

(3) Pour COnventionnal ARMs*, groupe de travail et d'échange entre les États membres de l'Union européenne sur leurs politiques d'exportation d'armes conventionnelles.*

(4) Les offsets *sont des compensations consenties par le fournisseur à son client : part de production locale, transferts de technologie, recours à des sous-traitants locaux, etc.*

interministérielle des biens à double usage (CIBDU) qui, le cas échéant, autorisent *in fine* l'exportation et donc les éventuels *offsets* qui s'y rattachent.

Il n'en demeure pas moins qu'eu égard au niveau de la menace cyber et à son évolution, une vigilance accrue s'impose en la matière.

4. Soutenir et investir, sous supervision publique, dans le développement de solutions « cyber-offensives » et d'outils de défense contre les menaces cyber

● En matière défensive, il est essentiel de maintenir l'effort dans les domaines de la cryptographie et du chiffrement, notamment au regard des ruptures technologiques à venir, en particulier le calcul quantique et le développement de l'intelligence artificielle.

La cryptographie joue un rôle majeur dans la protection de la confidentialité des échanges les plus sensibles. Elle constitue un élément indispensable dans le domaine de la cyberdéfense et une barrière essentielle dans la défense en profondeur des systèmes opérés par les armées.

À l'heure actuelle, les capacités en matière de cryptographie demeurent plus puissantes que les capacités de décryptage et la France a toujours été en pointe dans le domaine du chiffrement. Il est toutefois nécessaire de veiller au maintien et au développement de ce domaine d'excellence afin d'élaborer les capacités de demain, qui permettront d'être à la hauteur des défis posés par de nouvelles technologies susceptibles d'accélérer la vitesse de décryptage des données. À cet égard, l'avènement du calcul quantique constituera sans doute le défi majeur en la matière compte tenu de la puissance et de la vitesse de calcul des ordinateurs [(1)].

Le maintien d'un tel effort sera d'autant plus essentiel demain, au regard de la numérisation exponentielle des armées et, partant, de l'extension de leur surface de vulnérabilité aux risques cyber.

● Parallèlement, il s'agira de soutenir et d'investir, sous supervision publique, dans l'émergence des solutions « cyber-offensives » de demain dans le respect d'un cadre juridique solide et d'une doctrine d'emploi claire.

La détention de capacités cyber-offensives est en effet indispensable à plus d'un titre. En premier lieu, et comme cela a été rappelé, le cyberespace constitue un nouvel espace de confrontation. De fait, comme tout espace de conflictualité, il suppose que l'État, grâce à ses forces armées, soit techniquement et opérationnellement en mesure de répondre à des agressions, mais également de mener, le cas échéant, des actions, comme dans les milieux traditionnels. De la même manière que les forces armées disposent de capacités offensives terrestres,

(1) Sur l'informatique quantique, ses applications et ses conséquences, on se reportera au rapport d'information précité sur les enjeux de la numérisation des armées.

aériennes et maritimes, il est donc légitime qu'elles puissent disposer de capacités offensives cyber.

Par ailleurs, et un tel constat découle logiquement du premier, la détention de capacités offensives produit par nature un effet dissuasif à l'encontre de ceux qui chercheraient à agir contre la France, ses citoyennes, ses citoyens et ses intérêts. La France doit prévenir les menaces potentielles qui pèsent sur elle dans tous les milieux, y compris le milieu cyber et le nombre de « divisions cyber » constitue à cet égard un facteur essentiel de dissuasion.

Enfin, les connaissances acquises dans le processus de développement de solutions offensives permettent, parallèlement, d'améliorer les postures défensives. Dès lors que les effets d'une arme, quelle qu'elle soit, sont connus et analysés, il est possible d'améliorer en conséquence les défenses. Tel est le cas dans les milieux traditionnels – les systèmes antimissiles s'adaptent aux progrès réalisés en termes de vélocité, de furtivité et de pénétration des munitions. Tel est le cas également dans le domaine cyber. En somme, on se défend d'autant plus efficacement que l'on connaît l'ensemble des capacités offensives possibles. Et on connaît d'autant mieux ces capacités qu'on les a développées soi-même, ce qui est une quasi-obligation dans le domaine de la défense s'agissant des produits et des technologies les plus aboutis et les plus sensibles.

5. Assurer le maintien en condition de sécurité des matériels d'ancienne génération

Au-delà des nouveaux et futurs matériels et systèmes d'armes, il convient d'assurer le maintien en condition de sécurité des équipements plus anciens mais déjà très numérisés, développés à une époque où les menaces et donc les exigences en matière cyber étaient moins fortes.

Une revue de ces parcs devra ainsi être menée afin d'évaluer la nécessité opérationnelle et la faisabilité technique et budgétaire d'une « remise à niveau cyber » de certains d'entre eux.

E. AJUSTER LA « RESSOURCE HUMAINE CYBER »

Le cyber est un domaine dual en pleine expansion, qui intéresse à la fois le secteur civil et le monde militaire. De fait, le « marché de l'emploi cyber » est aujourd'hui extrêmement tendu, ce qui nécessite la mise en œuvre d'actions résolues afin de renforcer, d'attirer et de fidéliser la « ressource humaine cyber », notamment au sein des autorités publiques qui en dépendent.

1. Renforcer le « vivier cyber »

● La première mesure consiste d'abord sans doute à faire connaître les différents métiers et formations du cyber, secteur d'emploi particulièrement ouvert qui recrute aussi bien des titulaires de BTS que des ingénieurs très spécialisés ou

encore des autodidactes. L'enseignement informatique durant la scolarité primaire et secondaire devrait à terme permettre de remédier à la méconnaissance actuelle des différents métiers du secteur.

De fait, d'après les informations communiquées aux rapporteurs, le taux de remplissage dans les formations cyber ayant fait l'objet d'un suivi statistique n'est que de 76 % [(1)], alors même que les débouchés professionnels sont pour ainsi dire garantis tant les profils cyber sont particulièrement recherchés, dans le secteur public comme dans le secteur privé.

Des actions de communication ambitieuses pourraient donc être entreprises au niveau des établissements de l'enseignement secondaire, dès le lycée, et supérieur.

● Par ailleurs, une fois ces actions de promotion conduites, il conviendrait de favoriser l'augmentation du nombre de places offertes dans les formations « cyber ». En effet, ainsi que l'ont affirmé de nombreuses personnes auditionnées par les rapporteurs, notre pays accuse un déficit de plusieurs milliers de postes dans ce domaine [(2)]. Or, comme cela a été rappelé, les besoins et donc l'offre de travail sont particulièrement importants, dans tous les secteurs.

Les rapporteurs jugent ainsi nécessaire de mettre en place ou, lorsqu'elles existent, de renforcer de véritables filières cyber complètes, à la fois académiques (chercheurs) et à visée opérationnelle (techniciens et ingénieurs du cyber) du baccalauréat jusqu'à la thèse, sans oublier les sciences humaines et sociales dont l'importance semble sous-évaluée dans ce domaine, alors qu'elles sont essentielles à son appréhension. Il s'agirait également de proposer et développer des modules de formation continue en la matière.

● Il faut toutefois que les formations répondent aux besoins des différents employeurs. À cet égard, il convient de les faire certifier par l'acteur public de référence, l'ANSSI.

C'est d'ailleurs la voie qu'elle poursuit, avec les initiatives SecNumedu et CyberEdu qui visent à faire émerger des formations spécialisées et labellisées en matière de cybersécurité.

SecNumedu est le label des formations initiales en cybersécurité de l'enseignement supérieur, destinées aux futurs spécialistes. Il permet de garantir aux étudiants et aux employeurs qu'une formation délivrée par un établissement labellisé répond à une charte et des critères établis par l'ANSSI en collaboration avec les acteurs concernés (industriels, Éducation nationale, enseignement supérieur, recherche, etc.). Le label est attribué pour une période de trois ans

(1) Statistiques SecNumedu, ANSSI.

(2) Selon une étude commandée par le syndicat professionnel Syntec Numérique, le déficit atteindrait plus de 6 000 postes (Observatoire paritaire de l'information, de l'ingénierie, des études et du conseil – Opiiec – « Les formations et les compétences en France sur la cybersécurité », étude réalisée par le cabinet EY, mai 2017).

renouvelable. Actuellement 41 établissements en bénéficient. Le cas échéant, il conviendrait que les autres acteurs publics de la chaîne cyber – COMCYBER, DGSE, DRSD et DGSI – soient associés à cette initiative.

CyberEdu est un projet que l'ANSSI a imaginé à la suite de la publication du Livre blanc sur la défense et la sécurité nationale de 2013. Il vise à faciliter l'intégration et à diffuser les notions de cybersécurité dans les formations en informatique. Pour ce faire, une association spécifique a été constituée, qui propose des supports pédagogiques et a vocation à délivrer une labellisation aux formations de l'enseignement supérieur qui ne sont pas spécialisées dans les aspects relatifs à la sécurité du numérique. À l'heure actuelle et selon les données disponibles sur le site de l'association, seules sept formations ont reçu ce label. Il convient d'appuyer le développement de cette démarche dont l'intérêt est de s'adresser à un cercle plus large que celui des seuls spécialistes.

Rappelons enfin les initiatives du ministère des Armées, qui a, par exemple, soutenu la création du BTS cyber du lycée militaire de Saint-Cyr L'École, ou encore du mastère spécialisé en gestion de crise cyber de Saint-Cyr Coëtquidan.

● Plus généralement, et au-delà de son réseau régional précédemment évoqué, il paraît nécessaire de renforcer les moyens, tant humains que budgétaires, de l'ANSSI.

Certes, l'ANSSI apparaît comme une « anomalie » dans un contexte de réduction tendancielle de la dépense et du nombre d'agents publics. En effet, le nombre de personnels employés par l'agence a été multiplié par près de sept depuis sa création (546 agents aujourd'hui contre 80 en 2009). Toutefois, une telle croissance correspond à un besoin dont il est évident qu'il va se renforcer à l'avenir et qu'il convient donc d'anticiper. Par ailleurs, on notera que l'agence allemande équivalente de l'ANSSI, le BSI précédemment évoqué, compte 54,5 % de personnels en plus que son homologue française (avec 850 agents environ), une différence sans commune mesure avec les écarts objectifs de population, la structure institutionnelle, la réalité socio-économique des deux pays, ou encore le niveau de menace cyber auquel ils sont confrontés.

Selon le schéma d'emploi actuellement prévu, l'ANSSI devrait compter 570 agents à la fin 2018 et 670 agents à l'horizon 2022, soit 25 créations de postes par an. Si une telle augmentation est à saluer, elle ne paraît cependant pas à la hauteur des enjeux et des menaces. Idéalement, l'ANSSI devrait disposer de moyens humains au moins équivalents à ceux du BSI, voire davantage (au moins 850 agents donc) afin de renforcer les capacités de réponse face à une crise majeure, d'accompagner efficacement l'ensemble des acteurs, de mener l'ensemble de ses missions sur un spectre qui aura été élargi aux termes de la LPM 2019-2025 et de constituer l'un des acteurs de premier plan, tant aux niveaux européen qu'international.

2. Adapter les modèles de gestion des ressources humaines de l'État

Augmenter le « vivier cyber » ne suffira toutefois pas en ce qui concerne les autorités publiques si celles-ci ne sont pas en mesure d'attirer et surtout de fidéliser pendant une période suffisamment longue les cyber-experts. Il est normal et essentiel que ceux-ci exercent également leurs talents dans le secteur privé puisque les menaces cyber sont globales. Mais, dans le cadre du présent rapport, il est logique que les rapporteurs s'intéressent en premier lieu aux capacités publiques. Il faut toutefois souligner que même les grandes entreprises de la BITD ont également souligné les difficultés qu'elles pouvaient rencontrer en termes de recrutement et de fidélisation de leurs personnels, en particulier en matière salariale, face à la concurrence d'autres acteurs et notamment des GAFAM.

● L'ensemble des responsables de la chaîne cyber auditionnés par les rapporteurs – ANSSI, COMCYBER, DGSE, DRSD – ont été unanimes sur ce point : les ressources humaines dans le domaine cyber constituent un enjeu très lourd pour l'ensemble des autorités publiques intéressées, et en particulier pour le ministère des Armées, compte tenu des missions dont il a la charge.

La technicité du milieu cyberdéfense, l'évolution de celui-ci vers un métier à part entière au-delà de la « simple » sécurisation des systèmes d'information, l'existence d'une concurrence civile extrêmement vive dans le secteur privé, vont obliger le ministère des Armées à adapter ses modes de recrutement mais également de fidélisation pour acquérir davantage de souplesse dans ses procédures (meilleure intégration du monde civil, recours accru à la contractualisation, etc.).

Les autorités publiques n'éprouvent pas de réelle difficulté en matière de recrutement : l'attractivité des services concernés, l'intérêt des missions et la volonté, toujours bien présente parmi les jeunes, de servir leur pays (ainsi qu'en témoigne également le succès des réserves) leur permettent de maintenir un niveau satisfaisant d'emploi.

En revanche, le maintien dans l'emploi, la fidélisation des personnels constitue un enjeu de premier ordre, notamment au regard des niveaux de rémunération offerts par le secteur privé à des profils particulièrement recherchés car rares. Ainsi que le relevait le responsable d'un de ces services, si les officiers de contre-ingérence cyber exercent un travail très stimulant et bénéficient d'une grande autonomie, ils peuvent se voir proposer par le privé des niveaux de rémunération deux à trois fois plus élevés que ceux offerts dans le secteur public.

À cette concurrence s'ajoute une réalité plus structurelle tenant au désir de mobilité de jeunes générations qui n'envisagent pas de rester de nombreuses années au sein de la même structure. Ainsi, en 2017, le taux de sortie des agents de l'ANSSI avait atteint 19 %, soit le taux observé dans son domaine d'activité de manière globale. Un tel renouvellement n'est pas en soi dommageable dans le sens où il permet aux différents services de « rester à la pointe » dans un domaine où les connaissances évoluent très rapidement.

Pour autant et quelles qu'en soient les raisons, le *turnover* des experts cyber au sein des autorités publiques peut non seulement poser des questions de maintien des compétences et des capacités, mais également des questions de sécurité s'agissant d'un domaine extrêmement sensible. C'est pourquoi une politique active et efficace de fidélisation est absolument nécessaire.

Les rapporteurs, qui ne sont pas des gestionnaires d'administrations, ne possèdent évidemment pas les clés d'une telle politique. Pour autant, il apparaît que la souplesse intrinsèque permise par le recours à la contractualisation et la possibilité de verser plus facilement des primes adaptées à l'importance et la sensibilité des fonctions exercées constituent des pistes à explorer.

● Les aspects pécuniaires, bien qu'importants, ne sont toutefois pas les seuls à prendre en considération. Il convient également d'offrir davantage de perspective aux « recrutés cyber ». Cela passe notamment par le fait de favoriser les passerelles entre les différents services concernés.

Un tel rapprochement serait bénéfique :

– aux personnels, en favorisant la mobilité et les perspectives de carrière ;

– et aux services eux-mêmes en facilitant les échanges, la diffusion d'une culture et de bonnes pratiques communes, la proximité opérationnelle, la mutualisation des outils et des équipements, etc. Il contribuerait donc *in fine* au renforcement de la posture cyber globale.

Certaines structures sont déjà physiquement proches. L'exemple du CALID, qui relève du COMCYBER, et du centre opérationnel de l'ANSSI, au sein de laquelle les deux structures sont colocalisées, constitue un exemple convaincant à cet égard. Il convient toutefois d'aller plus loin, notamment s'agissant des aspects plus opérationnels.

Si les rapporteurs souscrivent à l'organisation des armées en matière cyber et au rôle du COMCYBER, évacuant ainsi la notion de quatrième armée souvent évoquée en matière de cyberdéfense, il leur semble que le dispositif pourrait toutefois être complété. L'état-major cyber compte à l'heure actuelle moins de 70 personnes. Ses effectifs pourraient être utilement renforcés par des experts de haut niveau, afin de permettre au COMCYBER de disposer de davantage de capacités techniques propres en interne.

● Il pourrait aussi être envisagé de mettre en œuvre une politique intégrée en matière de ressources humaines et de formation entre les différents acteurs de la chaîne cyber.

Pourrait ainsi être créée une École de cyberdéfense rassemblant les capacités de formation et d'entraînement à la cyberdéfense, pour l'ensemble des métiers cyber, pour l'ANSSI, le ministère des Armées et le ministère de l'Intérieur, voire pour l'ensemble des administrations gouvernementales. Là

encore, une telle structure permettrait le développement d'une culture partagée et favoriserait, par la suite, les passerelles entre les différentes institutions, contribuant ainsi à la fidélisation de personnels. À cet égard, le Royaume-Uni a récemment inauguré une telle structure, la *Defence Cyber School*, dont la France pourrait utilement s'inspirer.

● Enfin, il s'agit d'accompagner efficacement la réforme *des* réserves cyber vers *une* réserve unique. Tout d'abord, il convient de souligner que les réservistes sont désormais indispensables à l'action des armées, et que réserve et armée d'active ne constituent plus des univers étanches. Par ailleurs, comme l'a affirmé le général Olivier Bonnet de Paillerets, commandant du COMCYBER, il convient d'intégrer davantage la réserve citoyenne de cyberdéfense (RCC), actuellement cantonnée à des actions de sensibilisation et de communication, au fonctionnement quotidien et opérationnel du COMCYBER, de l'ANSSI et de la gendarmerie, qui forment la triarchie de la gouvernance de la RCC. En somme, il convient de créer des ponts entre la RCC et la réserve opérationnelle de cyberdéfense, afin de motiver l'ensemble des réservistes et d'assurer leur fidélisation.

F. ASSURER LES CONDITIONS DE LA CYBERSÉCURITÉ COLLECTIVE

1. Accompagner les efforts d'harmonisation de la certification au niveau européen

Le 13 septembre 2017, à l'occasion de son discours annuel sur l'état de l'Union, le président de la Commission européenne M. Jean-Claude Juncker a annoncé la mise en œuvre d'une série de mesures destinées à renforcer la défense de l'Europe contre les cyberattaques.

Parmi les propositions formulées figurent la création d'une Agence de cybersécurité de l'UE, issue de la transformation de l'actuelle ENISA, ainsi que la mise en place d'un cadre de certification à l'échelle européenne.

L'Agence de cybersécurité aurait notamment vocation à organiser des exercices paneuropéens et à favoriser un meilleur partage des connaissances et des informations sur les menaces.

Le système européen de certification viserait à garantir la sécurité d'utilisation des produits et services dans l'environnement numérique en s'assurant qu'ils répondent aux exigences de cybersécurité nécessaires. Les certificats délivrés seraient reconnus par et dans tous les États membres.

Il s'agit d'une initiative intéressante, qu'il convient d'accompagner, mais pas à n'importe quel prix. Les rapporteurs tiennent à insister sur ce point : cette certification harmonisée, si elle prospère, doit s'effectuer sur la base de critères exigeants et non « vers le bas », sur le plus petit dénominateur commun européen, comme c'est souvent le cas au niveau de l'UE.

À cet égard, il convient également de souligner l'importance de mener une « diplomatie normative » active afin de promouvoir le modèle et les valeurs de la France dans le domaine cyber que notre pays entend diffuser auprès de ses partenaires européens.

2. Favoriser l'émergence d'un référentiel normatif partagé

● Développer l'influence normative de la France à l'international

Le rapport sur l'influence normative de la France, publié en 2013 [(1)], l'affirmait sans détour : « *l'influence sur les règles et normes internationales, c'est-à-dire sur les règles du jeu économique, est une des composantes essentielles quoique peu visible de la compétitivité des entreprises et des États. Les régulations internationales ne sont jamais innocentes, elles déterminent des marchés, fixent des modes de gouvernance, permettent à leurs auteurs de devancer la concurrence, ou de la freiner, ou d'exporter leurs contraintes.* »

Si ce rapport centrait son analyse sur les questions économiques et commerciales, conformément à la lettre de mission de son commanditaire, la ministre du Commerce extérieur, il n'en demeure pas moins que le constat ainsi posé vaut pour l'ensemble des domaines sujets à l'élaboration de normes à vocation extra-nationale, dont le domaine cyber naturellement.

De fait, le développement de l'influence normative de la France pour diffuser son modèle et ses valeurs dans le domaine cyber apparaît essentiel, *a fortiori* face à la prétention de certains États à l'applicabilité extraterritoriale et quasi universelle de leurs propres normes. La France a d'ailleurs publié, une « stratégie internationale pour le numérique » [(2)], dont l'un des axes consiste à « développer une cybersécurité collective à l'échelle internationale », tandis qu'un ambassadeur pour le numérique a été nommé pour conduire, notamment, les négociations internationales sur la cybersécurité.

Il n'en demeure pas moins que la place de la France peut et doit encore être affermie. À titre d'exemple et d'après les informations communiquées aux rapporteurs, aucun expert français n'a été associé à la rédaction de l'édition actualisée du manuel de Tallin parue en février 2017. Or, bien qu'il fasse parfois l'objet de certaines réserves, ce manuel fait aujourd'hui référence au sein de l'OTAN notamment.

La France doit conduire une « cyber-diplomatie » active et donc faire entendre sa voix de manière plus claire, d'abord pour faire valoir, voire prévaloir, son modèle et ses valeurs dans le domaine cyber, mais également pour affirmer ses positions face à certains concepts et prises de positions.

---

(1) Rapport de Mme Claude Revel remis à Mme Nicole Bricq, ministre du Commerce extérieur, Développer une influence normative internationale stratégique pour la France, *28 décembre 2012.*

(2) Présentée par M. Jean-Yves Le Drian, ministre de l'Europe et des Affaires étrangères, le 15 décembre 2017.

Tel est le cas, par exemple, du concept américain de « légitime défense préventive », sorte d'oxymore juridique non reconnu par le droit international et qui consiste à attaquer de manière anticipée un État montrant seulement des signes d'agressivité, sans qu'aucune menace précise ne soit pourtant connue, dans le but d'affaiblir et d'empêcher toute attaque ultérieure de la part de cet État.

Tel est le cas également s'agissant de l'encadrement nécessaire des actions potentiellement offensives des acteurs privés dans le cyberespace, à l'image de la pratique du *hack back*. Celle-ci consiste à reconnaître à un acteur privé victime d'une cyberattaque le droit de se faire justice lui-même et de mener en réponse des actions cyber-offensives. Or, sans revenir sur les difficultés d'attribution d'une cyberattaque déjà évoquées, de tels comportements peuvent faire peser un risque d'instabilité supplémentaire dans le cyberespace, domaine au sein duquel il semble nécessaire de laisser le monopole de la violence légitime aux seuls acteurs étatiques, sauf exceptions expressément prévues et encadrées. Or, des initiatives de promotion du *hack back* ont pu être prises, y compris de manière officielle. En témoigne le projet de *bill*, connu sous le nom d'*Active Cyber Defense Certainty Act* (1), déposé à la Chambre des Représentants par le *Representative* républicain de Géorgie Tom Graves, et qui vise notamment à exonérer de toute poursuite judiciaire les victimes de certaines cyberattaques qui y répondraient en prenant elles-mêmes des « mesures de cyber défense active ».

Toutefois, pour faire valoir ses vues et promouvoir ses standards normatifs, la France et, au-delà, l'Union européenne, doivent s'affranchir davantage des standards technologiques aujourd'hui majoritairement étrangers. Ce qui milite pour le soutien à l'émergence de solutions techniques nationales et européennes et d'une véritable politique industrielle en la matière, ainsi que les rapporteurs ont déjà eu l'occasion de le souligner.

● Favoriser l'élaboration d'un corpus juridique international commun

Fondamentalement, le meilleur rempart contre les cyberattaques les plus massives et destructrices – car il est illusoire d'envisager un monde sans menace cyber – consiste en la construction d'un environnement juridique accepté par tous les acteurs du jeu international et qui s'accorderaient sur le non-recours à certaines pratiques.

Les rapporteurs sont lucides et ne méconnaissent pas les difficultés et limites d'une telle ambition. Il n'en demeure pas moins qu'une « cyber-diplomatie » active doit contribuer, au niveau international, à la promotion d'une telle dynamique, en favorisant l'émergence d'une conception internationale pour des comportements étatiques responsables dans le domaine cyber.

---

(1) H.R. 4036 To amend title 18, United States Code, to provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorized intrusions into their computers, and for other purposes, October 12, 2017, House of Representatives, 115th Congress, 1st session.

À cet égard, la revitalisation du groupe d'experts gouvernementaux (GGE) réuni dans le cadre de l'ONU et que la Chine et la Russie, notamment, ont quitté en 2016, est une nécessité.

3. Promouvoir la coopération internationale

Les cyberattaques potentiellement les plus importantes, celles qui présenteraient des risques systémiques pour les États et leurs populations, constituent une menace globale au même titre que celle que le monde connaît depuis maintenant près de 20 ans sous son avatar mondialisé : la menace terroriste.

Aussi, les rapporteurs ne peuvent-ils que souscrire à l'analyse du général Olivier Bonnet de Paillerets, lorsqu'il estime nécessaire d'envisager la cyberdéfense de la même manière qu'a été envisagé le contre-terrorisme, à savoir par le partage des données et de l'analyse des menaces.

Il convient notamment d'appliquer dans le domaine cyber le concept de *due diligence* en vertu duquel un État a l'obligation de ne pas laisser utiliser son territoire pour la commission d'actes illégaux contraires aux droits d'autres États.

Il s'agit d'organiser ou de renforcer cette coopération tant au sein de l'État qu'avec d'autres pays partenaires et, à cet égard, les réponses sont à rechercher auprès des pays membres de l'Union européenne. Il convient de nouer ou d'approfondir des alliances pour partager, en temps réel ou quasi-réel, les caractéristiques des principales attaques.

Au-delà, les échanges doivent s'intensifier, notamment en matière de recherche, avec nos partenaires historiques mais également avec des pays tels que la Chine et la Russie qui, pour avoir quitté le GGE, n'en demeurent pas moins des interlocuteurs incontournables dans le secteur cyber.

Certes, et les rapporteurs ont eu l'occasion de le souligner, la coopération internationale dans ce domaine – comme dans les autres – doit être conduite de manière lucide, sans naïveté. Mais face à un phénomène global, la coopération entre États n'est pas une option. C'est une nécessité.

SYNTHÈSE DES RECOMMANDATIONS

Élaborer une loi « cyber »

● **Élaborer une loi « cyber »** portant sur la globalité des problématiques et des acteurs.

Recouvrer notre souveraineté numérique

● **Créer des espaces de stockage souverains nationaux et européens** afin de rapatrier et de stocker les données sensibles dans des territoires sous juridiction nationale ou **européenne**.

● **Favoriser l'émergence de solutions techniques nationales et européennes** de **confiance**.

Renforcer la résilience de l'ensemble des acteurs nationaux

● **Durcir les dispositifs de prévention et de protection des autorités publiques** et diffuser culture et prise de **conscience** du risque cyber par des actions *ad hoc*.

● **Développer le recours aux *bug bounties*** au sein des autorités publiques.

● **Sensibiliser les acteurs économiques,** et en premier lieu les PME/PMI, à la nécessité de se protéger contre les cyber menaces.

● **Renforcer le réseau régional de l'ANSSI** au bénéfice des **acteurs** territoriaux publics et privés, en métropole comme dans les outremers.

● **Mettre en place des « référents cyber »** au sein des collectivités territoriales, établissements publics et entreprises, en fonction de leur **taille** et de leur secteur d'activité.

● **Éveiller les citoyennes et les citoyens** dès leur plus **jeune** âge à la cyber hygiène :

– **sensibiliser** les adultes sur leur lieu de travail ;

– **enseigner** la matière « informatique » en milieu scolaire ;

– **créer un CAPES d'enseignement numérique**.

● **Attirer l'attention du grand public sur les dangers inhérents à l'usage des produits numériques** par un marquage sur leur **emballage** et un développement dans leur notice d'utilisation.

Consolider une base industrielle et technologique de défense cyber

● **Encourager la « cyber solidarité »** entre grands **groupes** et sous-traitants.

● **Financer la montée en gamme cyber des sous-traitants par un fonds cyber** alimenté par les acteurs de la BITD et une partie des recettes issues des exportations d'armement.

● **Établir une cartographie régulièrement mise à jour des entreprises et compétences critiques** au sein de la **BITD**.

● **Améliorer la régulation concernant certains produits** pour limiter la prolifération de technologies offensives et les **risques** cyber systémiques.

● **Soutenir le développement de la cryptographie et du chiffrement** et **investir, dans le développement de solutions « cyber-offensives »**.

● **Assurer le maintien en condition de sécurité** des **matériels** d'ancienne génération.

Ajuster la « ressource humaine cyber »

● **Faire connaître davantage les métiers** et **formations du cyber**.

● **Augmenter le nombre de places** dans les filières **cyber**.

● **Renforcer les moyens budgétaires et humains** de **l'ANSSI**.

● **Adapter les modes de gestion des ressources humaines** de l'État **pour** mieux fidéliser les personnels.

● **Renforcer les capacités propres du COMCYBER en matière d'expertise numérique**.

● **Créer une École de cyberdéfense** permettant de développer une culture partagée entre les différents acteurs de la chaîne cyber.

● **Développer davantage les liens** entre la réserve opérationnelle de cyberdéfense et la réserve citoyenne de cyberdéfense.

Assurer les conditions de la cybersécurité collective

● **Accompagner les efforts d'harmonisation de la certification** au niveau européen.

● **Développer l'influence normative de la France** à l'échelle internationale.

● **Favoriser l'élaboration d'un corpus juridique international commun**.

● **Soutenir la coopération internationale,** par le partage des données et de l'analyse des menaces, l'approfondissement et la conclusion d'alliances.

TRAVAUX DE LA COMMISSION

La commission procède à l'examen du rapport de la mission d'information sur la cyberdéfense au cours de sa réunion du mercredi 4 juillet 2018.

Mme Alexandra Valetta-Ardisson, rapporteure. M. le Président, chers collègues, demain, est-ce qu'une succession logique de 0 et de 1 au sein d'un code informatique binaire pourra provoquer autant de dégâts qu'un missile de croisière naval ou qu'un obus tiré par un canon Caesar, en rendant inutilisables des équipements, des matériels ou des infrastructures militaires ? Est-ce qu'un virus aux effets systémiques, par la désorganisation massive qu'il provoquera, pourra aboutir à la mort d'êtres humains, y compris des civils ? Comme le souligne la Revue stratégique de cyberdéfense publiée par le SGDSN, il est probable qu'une attaque informatique consistant en des actes de blocage ou de sabotage des systèmes informatiques aura, un jour, des conséquences létales.

Ce qui, hier encore, pouvait relever de la science-fiction apparaît dorénavant comme une éventualité stratégique à prendre en considération en termes de doctrine militaire, de conduite des opérations et, plus globalement, d'organisation de la protection et de la résilience de l'ensemble de la société.

L'intérêt et la compétence de notre commission pour le « sujet cyber » sont évidents et légitimes. Les fondements de notre système de cyberdéfense ont majoritairement été posés dans le cadre des différentes LPM adoptées depuis 2009. La LPM 2019-2025, qui devrait être promulguée dans une dizaine de jours, ne fait d'ailleurs pas exception : un chapitre spécifique y est ainsi consacré.

Avant d'entrer dans le vif du sujet, je formulerai deux remarques liminaires de « méthodologie ».

Tout d'abord, notre rapport ne prétend pas à l'exhaustivité, et ce pour plusieurs raisons. Premièrement, le cyber est par nature une réalité globale, qui touche pour ainsi dire tous les champs de l'activité sociale. Il dépasse donc le champ de compétence d'une seule commission.

Deuxièmement, c'est un domaine en perpétuelle évolution. Son analyse n'est donc pas et ne sera jamais achevée.

Troisièmement, la Revue stratégique de cyberdéfense a déjà dressé un panorama très complet de la question, et il était évidemment inutile de doublonner le travail déjà effectué dans ce cadre.

Enfin, il faut rester conscient du fait que les travaux menés dans ce domaine se heurtent rapidement à l'obstacle du secret de la défense nationale. En

matière cyber comme en matière de renseignement par exemple, tout n'est pas dicible, encore moins publiable. Je vous laisse imaginer la situation lorsqu'un même service cumule compétences en matière de renseignement et en matière cyber… Si toutes nos questions n'ont pas pu trouver réponse du fait de ce nécessaire secret, nos interlocuteurs ont toujours fait preuve de la plus grande ouverture possible et permise pour éclairer nos travaux. Ils n'ont pas hésité à nous faire part d'éléments certes non couverts par le secret, mais néanmoins sensibles et nécessaires à la compréhension du sujet. Nous ne pouvons évidemment pas en faire état, mais nous tenons à souligner l'excellent état d'esprit de nos interlocuteurs, et à les en remercier.

La seconde précision méthodologique est que notre rapport n'a pas vocation à constituer le guide de référence du parfait cyber-attaquant ou du parfait cyber-défenseur. Nous ne sommes donc pas rentrés dans des considérations trop techniques, puisque telle n'est pas notre vocation et que tel n'est pas l'intérêt de ce travail.

Ce rapport étant fait au nom de la commission de la Défense nationale et des forces armées, nous nous sommes attachés plus particulièrement aux problématiques intéressant la défense. Mais pas exclusivement toutefois, puisque le cyber irrigue tous les domaines et brouille les frontières traditionnelles entre les États, entre les acteurs et entre les secteurs.

La « cyberguerre », au sens d'un conflit mené exclusivement dans le cyberespace avec l'emploi des seules armes cyber n'est sans doute pas une réalité opérationnelle. Du moins pas encore. Mais il n'y aura plus, demain, de conflit sans dimension cyber. Le cyberespace est un espace qui n'est ni en guerre ni en paix, mais en état de tension permanente. Un tel constat exige de ce fait une organisation et la mise en place de politiques et d'actions à la fois spécifiques et globales de la part des pouvoirs publics.

Nous n'allons pas abuser de votre patience avec de longs rappels sur l'organisation de la cyberdéfense en France, sur l'état de la menace ou sur les dernières cyberattaques massives qui ont eu lieu un peu partout dans le monde. Nous avons abordé ces sujets à l'occasion de l'examen de la LPM, et vous trouverez de longs développements consacrés à ces différents aspects dans le rapport écrit. Nous allons simplement revenir sur un certain nombre de points qui nous semblent importants, avant de vous présenter nos principales observations et recommandations.

Tout d'abord, de quoi parle-t-on lorsqu'on évoque la cyberdéfense ?

Le sujet étant assez technique, il semble nécessaire de définir quelques notions au préalable. Vous trouverez plusieurs définitions dans la version écrite du rapport. Dans le cadre de cette présentation, je n'en rappellerai que deux.

La cyberdéfense comprend l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes

d'information jugés essentiels. Il ne faut pas la confondre, comme on le fait souvent, avec la cybersécurité. En résumé, celle-ci est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace et susceptibles de le compromettre.

M. Bastien Lachaud, rapporteur. J'en viens maintenant à la définition du cyberespace. Elle sera un peu plus longue. Cela peut sembler évident mais un tel rappel est important : le cyberespace est un milieu artificiel, créé par l'homme. Il ne s'agit pas d'un milieu naturel, comme les milieux traditionnels. C'est aussi un milieu abstrait et global, sans consistance physique. Il ne connaît ni limites ni réalités ou caractéristiques géographiques physiques. Il ne connaît pas non plus de frontières politiques ou juridiques qui permettraient, d'une part, d'en délimiter précisément les contours et, d'autre part, de le subdiviser pour en rattacher les différentes composantes à chaque État, ou à aucun d'entre eux.

Le cyberespace est également un espace mouvant qui est en recréation constante. Il n'existe pas de carte du cyberespace, de ses « continents » et de ses limites. De fait, le cyberespace et les conflits qui s'y déroulent sont à repenser en permanence.

En dépit de ces caractéristiques – ou grâce à elles –, le cyberespace constitue un nouveau théâtre d'opérations potentiel, au même titre cette fois que les espaces traditionnels. Des acteurs, étatiques ou non–étatiques, y agissent et l'utilisent pour atteindre des buts politiques, en exploitant toutes les possibilités offertes par ce nouveau milieu. De ce point de vue, le cyberespace ne diffère pas fondamentalement des quatre autres milieux. Et les actions qui y sont menées ne se distinguent pas, dans leur nature, des actions traditionnellement conduites, en particulier par les États : espionnage, sabotage, déstabilisation.

Enfin, le cyberespace est un espace global qui, en s'y superposant, et en les englobant, contient les espaces traditionnels.

Comment le cyberespace est-il structuré ? Comme le monde physique, il n'est pas homogène ; il se compose de trois couches distinctes qui font l'objet d'une régulation plus ou moins poussée.

On trouve d'abord la couche physique. En effet, même le cyberespace n'est pas totalement abstrait. Cette couche comprend globalement deux types de « matériels ». D'une part, l'ensemble des infrastructures qui permettent l'acheminement et l'échange des données au sein du cyberespace, y compris les lieux de stockage de l'information. Il s'agit des serveurs, des câbles sous-marins, ou encore des réseaux de fibre optique terrestre. On y trouve d'autre part les appareils terminaux que nous utilisons quotidiennement : ordinateurs, téléphones, tablettes numériques, objets connectés, systèmes électroniques, etc.

La couche physique du cyberespace peut être « territorialisée » juridiquement. S'agissant d'éléments physiquement situés sur des espaces donnés, ces différentes infrastructures et la couche qui les regroupe font l'objet d'une

régulation, et sont soumises à différents niveaux de législations et de juridictions, tant nationales qu'internationales.

La couche physique et ses éléments peuvent être la cible d'actes malveillants, soit *via* le cyberespace, soit par des moyens tout à fait conventionnels et classiques : endommagement, altération, destruction, neutralisation, perturbation du fonctionnement, etc.

La deuxième couche du cyberespace est la couche logique. Elle comprend l'ensemble des programmes qui permettent d'accéder aux différents réseaux du cyberespace, de les exploiter, d'assurer le transport des données, etc. Il s'agit des différents protocoles, langages et autres logiciels mis en œuvre dans le cyberespace.

C'est cette couche qui constitue classiquement la cible des menaces cybernétiques, car elle est relativement facile d'accès. Par ailleurs, ses éléments présentent par nature des vulnérabilités. Il peut par exemple s'agir d'une erreur dans le code informatique d'un équipement, qui constitue alors une faille. À titre d'exemple, on estime qu'une erreur est présente en moyenne toutes les 1 000 lignes de code. Pour donner un ordre d'idée du nombre de failles potentielles – qui peuvent être d'importance et de gravité très diverses –, Google et l'ensemble des projets associés représenteraient deux milliards de lignes de code, Facebook plus de 60 millions, une FREMM plusieurs millions.

Dans la couche logique, le code constitue à la fois la vulnérabilité et le principal levier d'action, précisément pour exploiter les vulnérabilités adverses. L'attaquant est alors à la recherche de failles de sécurité susceptibles d'être exploitées. Les plus valorisées sont les failles dites *zero-day*. Il s'agit de vulnérabilités affectant un système, inconnues de leur concepteur, qui n'ont jamais été identifiées et répertoriées, qui n'ont jamais fait l'objet d'une publication, et dont la communauté de la sécurité informatique n'a donc pas connaissance. Elles confèrent donc à leur « découvreur » un avantage tactique certain, du moins jusqu'à ce que, une fois dévoilées, des correctifs leur soient apportés.

Mme Alexandra Valetta-Ardisson, rapporteure. Troisième et dernière couche : la couche cognitive. Il s'agit de la couche du sens et du contenu visibles sur les divers sites et pages Internet, dans les systèmes de messagerie électronique ou sur les réseaux sociaux. Si les deux premières couches sont des couches techniques, la couche cognitive est celle de la valeur « sociale et intellectuelle », qui constitue le cœur du cyberespace. C'est une couche par essence ouverte et globale, impossible à réguler totalement compte tenu de son étendue et de sa nature. Sans même évoquer le *darkweb*, on estime ainsi qu'il existe plus d'1,8 milliard de sites Internet représentant plus de 4,5 milliards de pages. Chaque minute, 400 heures de vidéos sont téléchargées sur la plateforme YouTube, 216 millions de photos sont « aimées » sur Facebook et 350 000 tweets sont publiés sur Twitter.

L'étendue de cette couche emporte un grand nombre de vulnérabilités associées, chaque élément pouvant être exploité, transformé, détourné par un acteur malveillant. Nous en avons encore eu la preuve à l'occasion de grands rendez-vous démocratiques récents. Je pense aux cyberattaques subies par le *Democratic National Committee* lors de la campagne présidentielle américaine de 2016, ou à celles qui ont ciblé le site Internet du mouvement En Marche ! lors de la campagne présidentielle française de 2017.

C'est sur cette couche que se déploient l'information, mais également la désinformation, les activités de propagande ou encore les rumeurs et autres *fake news*. Si de telles réalités sont anciennes, la numérisation et l'interconnexion des sociétés permettent la production et la diffusion des contre-vérités à l'échelle industrielle.

Je souhaiterais maintenant présenter les spécificités du milieu cyber comme espace de conflit, du point de vue de la défense nationale.

Le cyberespace écrase les distances et le temps. Nous l'avons souligné : le cyberespace ne connaît pas de frontières. Il n'existe pas de cyberespace français dont la violation constituerait une atteinte. Aussi et pour reprendre un terme militaire : il n'y a pas de front dans le cyberespace, ou alors il s'agit d'un front global. De fait, l'espace cyber pousse à l'extrême la disjonction entre, d'une part, la présence physique d'un acteur et le lieu de déclenchement de son action et, d'autre part, les effets de cette action.

Inversement, une attaque ciblée *a priori* peut, du fait de l'interconnexion des différents acteurs, également toucher une « victime collatérale ». Tel fut le cas pour la société française Saint–Gobain, victime indirecte mais bien réelle de la cyberattaque NotPetya qui avait ciblé l'économie ukrainienne en 2017. Le groupe français a ainsi été touché par le biais d'une filiale située dans ce pays, laquelle utilisait un logiciel de comptabilité dont la mise à jour avait été piégée, et qui a servi de canal à la dissémination du virus.

Par ailleurs, le cyberespace offre une protection naturelle aux auteurs d'actes malveillants. Un attaquant situé dans un pays donné peut parfaitement déclencher son action à partir d'un équipement situé dans un pays tiers, voire effectuer de multiples « rebonds » afin de masquer la véritable origine de l'attaque. C'est l'une des difficultés à laquelle se heurtent les autorités et services chargés d'attribuer une cyberattaque. Nous y reviendrons.

En s'affranchissant de l'une des barrières les plus contraignantes qui soit – la distance, et donc le temps – l'attaquant dispose dans le milieu cyber, d'un avantage stratégique non négligeable : l'effet de surprise.

Le temps est un autre facteur classique déterminant dans les espaces traditionnels de conflits. Là encore, le cyberespace s'en distingue puisque la dimension temporelle devient secondaire. Une cyberattaque peut présenter un caractère foudroyant. En une seule commande, en un « clic » de souris, un

attaquant peut obtenir de manière quasi instantanée l'effet recherché : corruption d'un système, défiguration, blocage, ou encore déni de service.

Toutefois, si la transmission des ordres informatiques se caractérise par sa rapidité extrême, l'action cybernétique peut également favoriser le temps long. Certaines formes de corruption de systèmes, notamment les bombes logiques, peuvent en réalité être présentes dans ces systèmes pendant une longue période avant d'être déclenchées ou de se déclencher de manière automatique.

Par ailleurs, les attaques informatiques nécessitent une phase de préparation parfois longue afin d'analyser la cible de la manière la plus fine possible. Après le déclenchement de l'attaque, les phases d'intrusion au sein d'un système puis d'exploitation de celui-ci peuvent également nécessiter du temps, surtout si l'architecture du système visé est complexe. À titre d'exemple, la cyberattaque qui a affecté TV5 Monde s'est déroulée sur près de trois mois, entre l'intrusion dans les réseaux de la chaîne et la production des effets de l'attaque.

Enfin, l'attaquant ne cherche pas systématiquement à conférer une publicité à son acte. Car l'efficacité de certaines atteintes repose au contraire sur le caractère indétectable de celles-ci. On pense notamment au vol de données.

Le cyberespace permet par ailleurs un certain nivellement des rapports de force. Cela tient d'abord à la relative facilité d'accès aux technologies cyber. Alors qu'il est assez malaisé de se procurer des armes « classiques », compte tenu de l'existence de régimes de régulation et d'interdiction, l'accès aux potentielles armes cyber est relativement ouvert. Par ailleurs, même « rustique », un programme malveillant répliqué des centaines de milliers de fois peut produire des conséquences massives. Soulignons enfin la disproportion entre la « taille » d'une arme cyber et ses effets : on estime ainsi que le virus Stuxnet, qui a affecté le fonctionnement de certains sites nucléaires iraniens en 2010, « pesait » entre 500 kilo-octets et 1 méga-octet selon les versions, soit l'équivalent d'une simple photographie numérique de qualité raisonnable.

En second lieu, ce nivellement est la conséquence d'une imbrication entre les milieux civil et militaire, qui brouille la ligne de partage traditionnelle des conflits. Dans le cyberespace, le rapport entre cibles civiles et militaires s'inverse puisque les premières représentent la « norme ». Elles sont, du reste, comparativement moins bien protégées que les secondes et constituent à cet égard des cibles de choix pour les attaquants. Or même ciblées sur des éléments exclusivement civils, des atteintes peuvent mettre en danger le fonctionnement normal d'une société, voire la survie de la Nation. Le cyberespace produit donc une confusion entre les sphères civiles et militaires, à rebours de la pensée stratégique traditionnelle et des régimes juridiques applicables aux conflits. En effet, ceux-ci reposent sur une distinction claire, même si elle n'est pas toujours respectée en pratique, entre ces deux champs.

M. Bastien Lachaud, rapporteur. Troisième spécificité : l'attribution d'une cyberattaque est très complexe. Pour faire usage de la force de manière légitime, adaptée et proportionnée à l'égard d'un agresseur, il convient de l'avoir préalablement identifié et d'être en mesure de lui imputer de manière certaine l'acte qui justifie l'action exercée en retour. Or dans le cyberespace, l'attribution s'avère particulièrement difficile, ce qui complique singulièrement les capacités de réponse à une cyberattaque. Plusieurs raisons l'expliquent :

– les actions malveillantes menées dans ce milieu font très rarement – voire jamais – l'objet d'une revendication. Par ailleurs, l'attaquant originel, s'il peut être identifié, n'est pas nécessairement le commanditaire de l'action ;

– on l'a dit, rares sont les attaques directes déclenchées à partir d'un point A pour affecter immédiatement et sans détour un point B. Les cyber–attaquants s'efforcent de faire « rebondir » leurs attaques de serveur en serveur et de pays en pays afin de « masquer leurs traces » ;

– au-delà des victimes expressément ciblées, une cyberattaque peut également affecter des victimes « collatérales », que l'attaquant ne cherchait pas spécifiquement à atteindre ;

– le cyberespace offre à ses acteurs un degré d'anonymat sans équivalent, et remonter la « chaîne d'anonymisation » représente un défi majeur. C'est d'autant plus vrai s'agissant des entités, groupes ou individus qui agissent non pas sur les réseaux ouverts, mais sur le *darkweb* ;

– les effets de certaines atteintes peuvent se déclencher longtemps après la pénétration effective d'un système.

Il convient toutefois de souligner un aspect essentiel. Au-delà des aspects purement techniques, la décision d'attribuer une cyberattaque relève, en dernière analyse, d'une appréciation et donc d'une décision de nature politique. Plutôt que sur des certitudes absolues et des preuves irréfutables, une telle décision s'appuie sur un niveau suffisamment bas d'incertitudes, sur un faisceau d'indices à la lumière desquels l'autorité politique prend la responsabilité d'attribuer un acte. Contrairement à d'autres pays – États-Unis ou Royaume-Uni, par exemple –, la France n'attribue jamais officiellement les cyberattaques qui pourraient la cibler.

Comme l'affirmait Napoléon de manière particulièrement imagée mais très pertinente : « *En guerre comme en amour, pour en finir, il faut se voir de près.* » Or, le cyberespace empêche précisément de voir distinctement son adversaire. L'anonymat n'y est pas absolu et toute action numérique peut finir par être tracée. Mais les délais nécessaires pour lever cet anonymat et obtenir la parfaite traçabilité d'une action peuvent s'avérer incompatibles avec la conduite d'une action de représailles.

Une conséquence majeure de cette difficulté d'attribution est de rendre partiellement inopérants les mécanismes de défense collective existants :

article 51 de la Charte des Nations unies, article 5 du traité de l'Atlantique Nord, article 42-7 du traité sur l'Union européenne. Vous trouverez dans le rapport écrit des développements à ce sujet.

Nous ne reviendrons pas sur les mesures qui ont déjà été prises en matière de cyberdéfense ces dernières années. Là aussi, vous trouverez toutes les éléments nécessaires dans le rapport publié. Nous allons maintenant vous faire part de nos principales réflexions, que nous avons choisi de présenter autour d'une grande recommandation « de principe » et de six grands thèmes. Nous les exposons en toute modestie, compte tenu du caractère global et extrêmement mouvant de la question.

Notre recommandation de principe est l'élaboration d'une grande loi cyber, à l'image de la loi « informatique et libertés » de 1978 ou encore des lois « bioéthiques ». En effet, le caractère global de la question cyber justifie :

– d'une part, une analyse approfondie et complète du sujet à l'échelle de notre pays ;

– et, d'autre part, la mise en place d'un cadre global et adapté, au–delà des dispositions qui ont été élaborées jusqu'alors, et qui ne concernent qu'un nombre réduit d'acteurs très spécifiques, à l'image des opérateurs d'importance vitale (OIV).

Une telle loi permettrait d'établir, à l'échelle nationale, une cartographie précise des vulnérabilités et des besoins, d'évaluer les ressources financières, matérielles et techniques nécessaires, et de déterminer les politiques à mettre en œuvre, qu'il s'agisse de politique industrielle, de recherche, ou encore d'adaptation du cadre juridique.

Comme les lois « bioéthiques », cette loi « cyber » pourrait faire l'objet d'un suivi et de mises à jour régulières. Un comité consultatif national du cyber, non permanent, pourrait être créé. Il serait chargé des travaux préparatoires à la révision de la loi cyber. À l'issue du processus de révision, le suivi du texte pourrait être assuré par des structures existantes, comme l'ANSSI.

J'en viens maintenant à la première série de recommandations, qui visent à nous permettre de recouvrer notre souveraineté numérique. Certaines rejoignent les observations qu'ont pu faire nos collègues Becht et Gassilloud à l'occasion de leur rapport sur la numérisation des armées.

Nous pensons avant tout nécessaire de créer des espaces de stockage souverains qui permettraient de rapatrier et de stocker nos données sur des territoires sous juridiction nationale ou européenne. Car les données stockées à l'étranger ne bénéficient d'aucune garantie quant à leur sécurité. Par ailleurs, certains États prétendent à l'application extraterritoriale de leurs législations. C'est le cas du droit américain. Ainsi, des données stockées hors des États-Unis mais sur

des serveurs appartenant à des sociétés américaines ne peuvent pas être considérées comme totalement sécurisées.

Il convient donc de développer des espaces de stockage à distance – en *cloud* –, ou des centres de stockage « en dur ». Nous sommes bien conscients que le *cloud* souverain ne constitue pas l'alpha et l'oméga de la sécurisation des données. Il reste toutefois un levier puissant à ne pas négliger, pour peu que l'on tire les leçons des échecs du passé dans ce domaine.

L'utilisation de ces solutions souveraines pourrait être rendue obligatoire pour certains acteurs : personnes publiques, OIV, entreprises de la BITD. Un travail préalable de classification des données, dont une partie seulement a vocation à être stockée dans un espace souverain, devra impérativement être effectué en amont. Cette évaluation de la nature des données et du niveau de protection requis est le gage de l'efficacité et, en définitive, de la viabilité des solutions qui seront proposées.

Ces solutions souveraines seraient aussi ouvertes aux autres acteurs, qui pourraient se voir délivrer un certificat par l'ANSSI qui attesterait du degré de sécurisation de leurs données. Un tel certificat pourrait même constituer un critère de valorisation des offres dans le cadre de l'attribution des marchés publics, sous réserve du respect de la réglementation européenne applicable et du code des marchés publics.

Sans se fondre dans un *cloud* transnational, les solutions nationales adoptées par la France et d'autres pays de l'Union européenne devront ouvrir la voie à un second niveau de stockage souverain, à l'échelle européenne. Celui-ci assurera un haut degré de protection aux données éligibles, qu'il conviendra de définir.

Mme Alexandra Valetta-Ardisson, rapporteure. Au-delà de la question du stockage, il est également nécessaire de disposer d'une certaine maîtrise de l'ensemble de l'écosystème numérique. Cela passe notamment par l'existence de solutions techniques alternatives, nationales et européennes, dans le domaine des logiciels et des composants, y compris grand public : moteurs de recherche, systèmes d'exploitation, logiciels de bureautique. Car, à l'heure actuelle, ces secteurs restent dominés par des monopoles ou quasi-monopoles non-européens, qu'ils soient américains ou chinois.

De telles solutions permettraient de réduire notre exposition au risque numérique. En effet, certains logiciels et composants peuvent parfaitement être piégés « à la source », intentionnellement ou non, et constituer des *backdoors* – ou portes dérobées –, qui sont autant de vulnérabilités potentielles. Par ailleurs, ces outils participeraient au renforcement de la souveraineté industrielle européenne, voire nationale. À cet égard, à côté de « l'Europe du *cloud* », « l'Europe du logiciel » pourrait constituer un projet concret et fédérateur.

Deuxième thème : le renforcement de la résilience de l'ensemble des acteurs. Si certaines administrations sont particulièrement conscientes des enjeux et des risques, par nécessité comme par « culture », tel n'est pas forcément le cas de toutes. Or, un attaquant ciblera plus volontiers les maillons les plus faibles d'une chaîne si cela lui permet d'atteindre, par répercussion, les plus forts.

C'est pourquoi il semble indispensable :

– de durcir les dispositifs de prévention et de protection de l'ensemble des autorités publiques nationales ;

– et de diffuser plus largement une culture et une conscience du « risque cyber » au sein des administrations, par des actions de formation, de pédagogie et de prévention.

Le même constat et les mêmes conclusions s'imposent s'agissant des collectivités territoriales. Cela vaut notamment pour les collectivités les moins importantes. Un premier travail pourrait être mené avec leurs associations représentatives : Régions de France, Assemblée des départements de France, Association des maires de France, Association des petites villes de France.

Les acteurs économiques, en particulier les PME et les ETI, doivent également être mieux accompagnés. Cela passe d'abord par une évolution des mentalités. La protection contre le risque cyber ne doit pas être vue uniquement comme une contrainte et une charge financière. En réalité, elle contribue à la performance économique globale. Elle doit être considérée comme un investissement et une assurance, qui permettent notamment de prévenir le « risque de réputation » en cas d'attaque réussie. Le degré de cyber–protection constitue en définitive un avantage compétitif pour une entreprise, sur son marché national comme à l'export. Une telle prise de conscience est d'autant plus importante que l'usine 4.0 intégrera massivement les technologies numériques dans ses processus de fabrication et sera, par nature, à risque.

Afin de répondre à un certain nombre de ces enjeux, notamment s'agissant des petites collectivités et des PME, nous pensons que le réseau régional de l'ANSSI devrait être renforcé. Actuellement, un délégué de l'ANSSI doit être présent dans chacune des 13 régions métropolitaines. Cela semble insuffisant au regard des enjeux. Par ailleurs, ce réseau n'existe que dans l'hexagone, aucun délégué ne représentant l'ANSSI dans les outre-mer. Il est nécessaire, à terme, d'y remédier.

Enfin, les citoyens eux-mêmes doivent évidemment prendre davantage conscience du risque cyber. Chacun, à son niveau, doit être acteur de sa propre cybersécurité et participer ainsi à la résilience globale. C'est pourquoi il importe d'éveiller tous les citoyens à la « cyber-hygiène ». Nous suggérons plusieurs pistes de réflexion dans ce domaine. Nous préconisons ainsi la création d'une nouvelle filière menant à l'obtention d'un CAPES d'enseignement numérique, dont les titulaires formeraient les élèves par le biais d'enseignements spécifiques. Cet

enseignement à part entière comprendrait, outre celui de la matière informatique, un éveil à la « cyber-hygiène » ainsi que l'enseignement des langages informatiques et de la programmation.

Au-delà de son bien-fondé intrinsèque, cet enseignement aurait l'avantage de développer des compétences transverses dont, par exemple, la capacité d'analyse, la logique et la résolution de problèmes. Il permettrait également de démystifier la matière et d'attirer plus de filles vers les métiers du numérique, qui demeurent aujourd'hui majoritairement masculins.

Des initiatives sont également envisageables à destination du citoyen consommateur et utilisateur de technologie. Alors que les enfants disposent de leur premier téléphone mobile à l'âge de 11 ans en moyenne, nous pensons que l'emballage et la notice d'utilisation de chaque produit technologique et numérique grand public devraient être complétés par une liste des principaux risques et mises en garde associés à leur usage.

Notre troisième série de recommandations vise à consolider une base industrielle et technologique de défense cyber. Car le cyber irrigue évidemment le champ de la conception, de la production et de la maintenance des systèmes d'armes et équipements qui ont vocation à être opérés par les armées. Cet aspect doit être pris en compte nativement dans les programmes d'armement, à plus forte raison dans le contexte de la numérisation croissante de l'environnement de combat. En effet, comme l'ont rappelé nos collègues Becht et Gassilloud, la numérisation des armées accroît mécaniquement leur surface d'exposition au risque cyber.

Nous estimons tout d'abord essentiel d'inciter à la « cyber–solidarité » au sein de la BITD. Celle-ci doit se matérialiser par un soutien plus prononcé des grands groupes à leurs chaînes de sous-traitants. Il peut prendre la forme d'actions de sensibilisation, mais également d'un soutien technique et financier pour assurer la « montée en gamme » de l'ensemble de la chaîne de la BITD. Des négociations et des accords pourraient être conclus avec les groupements industriels. L'État aurait un rôle moteur, voire contraignant, à jouer dans les groupes et entreprises au sein desquels il détient des participations, parfois majoritaires.

Une manière, plus contraignante, de développer cette solidarité consisterait à établir la responsabilité du donneur d'ordres sur l'ensemble de sa chaîne de sous-traitants en matière cyber.

M. Bastien Lachaud, rapporteur. S'agissant du financement de cette « montée en gamme » des sous-traitants, nous suggérons la constitution d'un « fonds cyber ». Il pourrait être alimenté par des contributions des acteurs de la BITD, mais également par une partie des recettes tirées des exportations d'armement réalisées par l'industrie française. Un taux de retour pourrait ainsi être déterminé chaque année en fonction des recettes réalisées l'année précédente.

Il convient également d'établir et de mettre à jour régulièrement une cartographie fine des entreprises et compétences critiques au sein de la BITD. Cela permettrait, d'une part, de les sécuriser de manière satisfaisante au niveau « technique » et, d'autre part, de les sécuriser « économiquement », en empêchant si nécessaire les prises de participation par des capitaux étrangers. Il convient donc de faire un usage, raisonné mais assumé, des dispositions prévues par le décret de 2014 relatif aux investissements étrangers soumis à autorisation préalable. Au-delà de la seule BITD, il pourrait même être envisagé de renforcer ce dispositif s'agissant de certaines entreprises du secteur de la sécurité des systèmes d'information.

Naturellement, il est nécessaire de continuer à soutenir et investir dans l'élaboration de solutions tant défensives qu'offensives. Pour les premières, il faut notamment maintenir l'effort dans les domaines de la cryptographie et du chiffrement. C'est essentiel au regard des ruptures technologiques à venir. Nous pensons en particulier au calcul quantique et au développement de l'intelligence artificielle qui accéléreront et faciliteront les opérations de déchiffrement.

Quant aux secondes, elles sont indispensables à plus d'un titre. Le cyberespace étant un espace de confrontation, nos armées doivent être capables d'y mener des actions, comme dans les milieux traditionnels. Par ailleurs, la détention de capacités offensives produit un effet dissuasif à l'encontre de ceux qui chercheraient à agir contre la France, ses citoyens et ses intérêts. Enfin, les connaissances acquises à l'occasion du développement de solutions offensives permettent, parallèlement, d'améliorer les postures défensives.

Sans que cela soit contradictoire avec ce qui précède, nous proposons d'améliorer la régulation de certains produits pour limiter la prolifération des technologies offensives et contrer les risques cyber systémiques. Cela suppose d'abord de mieux connaître les potentielles « armes numériques ». Une analyse fine et régulièrement mise à jour devrait permettre de déterminer les produits et technologies qu'il faudrait soumettre aux régimes encadrant les exportations ou transferts d'armements et de biens à double usage.

Un autre levier de régulation consisterait à envisager, sur le modèle applicable à certains matériels de guerre, la prohibition de l'emploi, de la fabrication et du commerce de certains produits et logiciels. Seraient concernés ceux qui seraient considérés comme les plus « dangereux », notamment ceux qui pourraient engendrer des risques et des dommages systémiques. Nous sommes conscients de la difficulté technique et juridique d'une telle initiative. Néanmoins, une analyse de la faisabilité d'une telle interdiction, qui viserait les « armes informatiques à effets massifs » pourrait utilement être entreprise, en concertation avec nos partenaires européens et internationaux.

Notre quatrième champ de préconisations vise à ajuster la « ressource humaine cyber », compte tenu des besoins actuels et prévisibles. Le cyber est un domaine dual en pleine expansion, qui intéresse à la fois le secteur civil et le

monde militaire. Le « marché de l'emploi cyber » est aujourd'hui extrêmement tendu, ce qui nécessite la mise en œuvre d'actions résolues afin de renforcer, d'attirer et de fidéliser la « ressource humaine cyber », notamment au sein des autorités publiques qui en dépendent.

La première mesure consiste à faire connaître les différents métiers et formations du cyber. D'après les informations qui nous ont été communiquées, le taux de remplissage des filières faisant l'objet d'un suivi n'est que de 76 %, alors que les débouchés professionnels sont pour ainsi dire garantis. Des actions de communication ambitieuses pourraient donc être entreprises au niveau des établissements de l'enseignement secondaire, dès le lycée, et supérieur.

Une autre mesure est l'augmentation du nombre de places offertes dans les formations « cyber ». Les dernières études publiées estiment ainsi que notre pays accuse un déficit de 6 000 postes dans ce domaine.

Nous jugeons également nécessaire de renforcer les moyens humains et budgétaires de l'ANSSI, au-delà de la question de son réseau territorial précédemment évoqué. Il est vrai que l'ANSSI a déjà bénéficié d'efforts substantiels dans un contexte de réduction tendancielle de la dépense et du nombre d'agents publics. Toutefois, il est évident que les besoins vont se renforcer à l'avenir et qu'il convient donc d'anticiper cette évolution.

Il est intéressant de noter que l'agence allemande équivalent de l'ANSSI, le BSI, compte près de 55 % de personnels en plus, avec 850 agents environ. Or cette différence est sans rapport avec les écarts objectifs de population, la structure institutionnelle, la réalité socio-économique des deux pays, ou encore le niveau de menace cyber à laquelle nos deux pays sont confrontés. Dans l'idéal, l'ANSSI devrait disposer de moyens humains au moins équivalents à ceux du BSI. Cela permettrait de renforcer les capacités de réponse face à une crise majeure, d'accompagner efficacement l'ensemble des acteurs, de mener l'ensemble de ses missions sur un spectre qui aura été élargi par la LPM 2019-2025, et de constituer l'un des acteurs de premier plan aux niveaux européen et international.

Au-delà de la seule question quantitative, les autorités publiques doivent adapter leurs méthodes de gestion des ressources humaines afin de fidéliser les personnels du cyber. Toutes les personnes auditionnées l'ont souligné : si l'État n'éprouve pas de difficultés particulières à recruter et continue à attirer les talents, il lui est moins facile de les fidéliser, notamment au regard des niveaux de rémunération offerts par le secteur privé.

L'État ne sera probablement jamais en mesure de concurrencer les grandes entreprises dans ce domaine. Mais il peut s'efforcer d'offrir des perspectives de carrière plus nombreuses et plus variées. Cela passe notamment par le fait de favoriser les passerelles entre les différents services concernés. Un tel rapprochement serait bénéfique :

– aux personnels, en favorisant la mobilité et les perspectives de carrière ;

– et aux services eux-mêmes en facilitant les échanges, la diffusion d'une culture et de bonnes pratiques communes, la proximité opérationnelle, la mutualisation des outils et des équipements, etc.

À cet égard, nous pensons qu'une politique intégrée pourrait être mise en œuvre en matière de ressources humaines et de formation entre les différents acteurs de la chaîne cyber. Nous préconisons ainsi d'étudier la création d'une École de cyberdéfense. Elle rassemblerait les capacités de formation et d'entraînement pour l'ensemble des métiers cyber et pour l'ensemble des services et ministères concernés au premier chef, voire pour l'ensemble des administrations gouvernementales. Cette école permettrait le développement d'une culture partagée et favoriserait, par la suite, les passerelles entre les différentes institutions, contribuant ainsi à la fidélisation de personnels. Il faut souligner que le Royaume-Uni s'est récemment engagé dans une voie similaire avec sa *Defence Cyber School*.

Enfin, notre pays doit jouer un rôle moteur pour assurer les conditions de la cybersécurité collective au niveau international. La France doit développer son influence normative à l'international afin de promouvoir son modèle et ses valeurs, et ainsi proposer des alternatives à des positions qu'elle ne partagerait pas. On peut penser au concept américain de « légitime défense préventive », totalement étranger à la pensée française. On peut également évoquer le concept de *hack back*. Celui-ci consiste à reconnaître à un acteur privé victime d'une cyberattaque le droit de se faire justice lui-même, et de mener en représailles des actions cyber-offensives. Or une telle reconnaissance pourrait prospérer si l'on n'y prend garde, au risque déstabiliser encore davantage le cyberespace. Sans parler du fait qu'elle contreviendrait au monopole de l'exercice de la violence légitime par les États.

Naturellement, il est important que la France continue de travailler dans les instances internationales à l'émergence d'un corpus juridique partagé. En effet, le meilleur rempart contre les cyberattaques les plus massives reste la construction d'un environnement juridique accepté par tous les acteurs du jeu international et qui s'accorderaient sur le non-recours à certaines pratiques.

Enfin, il faut continuer de promouvoir la coopération internationale en matière cyber. À cet égard, il semble nécessaire d'envisager la cyberdéfense de la même manière qu'a été envisagé le contre-terrorisme, à savoir par le partage des données et de l'analyse des menaces. Cela passe par la conclusion ou l'approfondissement d'alliances pour partager, en temps réel ou quasi-réel, les caractéristiques des principales attaques. Dans le domaine cyber comme dans les autres, la coopération doit être conduite de manière lucide, sans naïveté. Mais face à un phénomène global, la coopération entre États n'est pas une option. C'est une nécessité.

Le cyber transcende les secteurs et les frontières nationales. Nous sommes la preuve qu'il transcende également les frontières politiques, puisqu'une

rapporteure de la République en Marche et un rapporteur de la France Insoumise ont réussi à élaborer un rapport consensuel, tant au niveau des constats que des préconisations !

Telles sont les lignes directrices qui ressortent de nos travaux. Nous vous remercions.

M. le président. Je ne sais pas si c'est un miracle mais, en tout cas, c'est une réalité. Il y a vingt-deux questions, mes chers co-rapporteurs et chers collègues. Je vais commencer par les autres membres de la mission d'information.

M. Thibault Bazin. Je veux tout d'abord saluer le travail des deux co-rapporteurs et leur implication dans cette mission. Nous avons eu beaucoup d'éléments d'information.

D'abord, la menace cyber est réelle, en nombre et en intensité, avec des risques en termes de pertes de contrats, de marchés, de confiance, d'image, de protection et de performance. Les citoyens, les entreprises et les institutions ne sont pas assez « cyber-conscients ». Une hygiène numérique est nécessaire. Il n'y a pas assez de procédures de dépôt de plaintes. Il se pose également la question de la transparence pour mieux détecter les failles.

Nous avons eu des témoignages indiquant qu'on ne peut faire confiance à personne, même à nos amis et voisins. La réalité est qu'il est indispensable de protéger les systèmes d'inventions mais, surtout, cela a été dit, les données.

Les co-rapporteurs ont raison de questionner notre souveraineté. Des pans entiers d'infrastructures et d'applications informatiques sont dominés par des monopoles américains et chinois. De même, les technologies de « cyber-protection » sont largement dominées par les Américains.

Face à cela, la France ne dispose pas de produits souverains dans le domaine de l'antivirus, de l'« anti-malware » ou de « *sand boxes* », ces mécanismes permettant de détecter les « malwares ». Pour rattraper le retard pris, il est nécessaire de consacrer des moyens pour favoriser le développement de solutions françaises.

Il y a aussi un besoin de « *cloud* » étatique souverain et de serveurs en Europe. En effet, c'est le cadre juridique qui protégera la donnée estimée souveraine. Pour cela, l'opérateur de *cloud* doit se trouver sous juridiction française.

En matière de ressources humaines, la répartition des effectifs sur l'ensemble du territoire constitue un autre défi essentiel. Aujourd'hui un vrai pôle qualitatif existe en Bretagne, mais il est nécessaire d'avoir des pôles de formation sur tous les territoires.

Enfin, nous devons monter en puissance en matière de cyber-offensive et de cyber-riposte afin de pouvoir aveugler l'adversaire sur les théâtres d'opération contestés.

M. Philippe Michel-Kleisbauer. Merci de m'avoir accueilli en cours de route dans cette mission. Partie prenante de la commission « Science et technologie » de l'Assemblée parlementaire de l'OTAN, qui traite de ces questions, il était opportun que je suive avec vous ces travaux.

Dans le meilleur des cas, les cyberattaques sont simplement coûteuses. C'était le cas de « NotPetya » en Ukraine qui, en contaminant un logiciel de compatibilité, a touché un groupe français, Saint-Gobain, qui a provisionné 250 millions d'euros de pertes à l'automne, et peut-être davantage. Cela avait été le cas de « Cabarnak » qui avait touché le système de virement « Swift » avec détournement de plus d'un milliard de dollars.

Les cyberattaques peuvent également consister en un grave sabotage tel que Stuxnet qui visait les centrifugeuses d'enrichissement d'uranium en Iran. Les cyberattaques peuvent aller très loin dans la déstabilisation. Ainsi en Ukraine, des comptes Facebook de soldats sont détournés pour créer une dissonance cognitive grave qui déstabilise l'armée. Enfin, vous y avez fait référence, la Revue stratégique de cyberdéfense envisage le fait que, très rapidement, ces cyberattaques puissent devenir létales.

Je souhaite savoir si vous avez abordé dans votre rapport la question du déni d'accès aux technologies permettant des cyberattaques à ceux qui ne disposent pas encore de ces technologies, qu'il s'agisse de personnes physiques ou de personnes morales, privées ou publiques, et notamment des États ?

M. Yannick Favennec Becot. Dans le rapport, vous préconisez un « cyber-enseignement ». Je souscris totalement à cette volonté. À partir de quelle classe, de quel âge peut-on préconiser ce « cyber-enseignement » ?

Mme Patricia Mirallès. La mission d'information a permis de dessiner une cartographie de la cyberdéfense au niveau de la France. À Montpellier, nous avons aussi un diplôme sur la cybercriminalité. Par ailleurs, la ville de Montpellier aide beaucoup les start-up innovantes en matière de problématiques de cyberdéfense.

Je souhaite poser trois questions. Comment améliorer l'accompagnement de l'innovation par l'ANSSI et la Commission nationale de l'informatique et des libertés (CNIL) afin de faciliter la certification des nouvelles technologies pouvant bénéficier à la défense qui sont développées dans le secteur privé ?

Quid d'un fonds d'investissement souverain pour l'innovation en matière de technologie, à l'image du fonds In-Q-tel financé par la NSA ou du fonds Libertad ?

De quelle manière l'agence pour l'innovation créée en mars 2018, qui s'oriente avant tout vers l'intelligence artificielle (IA), pourrait comprendre un département « cyberdéfense » ?

Mme Marianne Dubois. Hier s'est tenue la seconde édition du forum « Cyberdéfense & Stratégie » au Cercle national des armées sur le thème « Quelles ruptures et quelles innovations pour la cyberdéfense ? ». L'IA et l'hyperconnectivité ont été au centre des discussions. Que pensez-vous de la tenue de ce genre de colloques sur des sujets aussi pointus et confidentiels, comme les capacités d'action futures dans le cyberespace et les outils et les dispositifs d'innovation en matière de cyberdéfense ? Est-ce qu'on peut légitimement débattre de ces sujets dans un colloque en toute confidentialité et en toute sécurité ?

M. Olivier Becht. Dans le combat permanent du glaive et du bouclier, l'arme du cyber dispose à la fois de la faculté de percer le bouclier et de neutraliser le glaive.

Avez-vous abordé la question de la résilience, notamment au niveau des OIV ? Si oui, quelles conclusions en tirez-vous ?

En effet, aujourd'hui, si les « bombes logiques » sont mises dans les composants d'un certain nombre de systèmes numériques, un risque important de ne pas pouvoir s'en prémunir par les systèmes de pare-feu existe. Les chinois sont aujourd'hui en train de doubler complètement leur système électrique pour faire en sorte que tous les systèmes d'électricité puissent fonctionner en manuel et hors numérique.

M. Joaquim Pueyo. Je voudrais bien évidemment saluer le travail des deux rapporteurs. Toutefois vous avez abordé trop rapidement, à mon sens, la question de la coopération européenne. Je pense en effet que les pays de l'UE, et je parle sous le contrôle de la présidence de la commission des Affaires européennes, devraient davantage travailler ensemble en matière de cyberdéfense suite aux cyber-attaques multiples et croissantes contre des cibles civiles et militaires. Ne pensez-vous pas que les États membres devraient renforcer la capacité de collaboration de leurs forces armées et améliorer la cyber-coopération au niveau européen ? Que pensez-vous également d'une meilleure coopération avec l'OTAN ? Car je crois savoir qu'entre la France Insoumise et l'OTAN, on ne peut pas parler d'une grande amitié… Puisque vous avez parlé de « coopération », je serais d'avis d'aller jusqu'au bout en la matière. Enfin, ne pourrions-nous pas intégrer d'autres partenaires ? Certains pays ont en effet de bonnes connaissances sur le sujet, l'Allemagne et le Royaume-Uni, par exemple.

Dans le cadre de la coopération structurée permanente, quel est votre point de vue concernant le lancement du cyber-projet relatif à la mise en place d'une plateforme d'information sur les cyber-incidents ? Celle-ci mettrait également à disposition des équipes pouvant intervenir rapidement en cas de problèmes

informatiques. Il s'agirait donc de partager nos compétences et nos connaissances dans le domaine du numérique sur une plateforme d'envergure européenne.

Ce sont des questions qui m'intéressent car vous avez certes soulevé des problèmes de fond, mais je pense que nous ne pourrons pas travailler correctement et efficacement intra-muros, c'est-à-dire cloisonnés dans un contexte purement hexagonal.

M. Jacques Marilossian. Je souhaiterais revenir sur la manière de faire émerger une communauté nationale de cyberdéfense en s'appuyant sur un cercle de partenaires mais aussi sur les réseaux de la réserve. Le Pacte de cyberdéfense de 2004 prévoyait de développer une réserve de cyberdéfense à vocation opérationnelle pour assister l'État et les armées en cas de risque majeur. Ce projet, développé en étroite coopération avec l'ANSSI et la gendarmerie nationale, prévoit que la réserve comprenne 4 440 personnes en 2019 soit 40 postes permanents, dont une vingtaine en régions et outre-mer. Elle comprendrait également 400 réservistes opérationnels dont 200 en régions et outre-mer et 4 000 réservistes citoyens, mobilisables sur l'ensemble du territoire national. Que pensez-vous de la situation de la réserve de cyberdéfense aujourd'hui et de son avenir ?

Mme Laurence Trastour-Isnart. Le cyberespace est devenu un domaine stratégique et au vu de l'intensification des attaques informatiques et des cyber-menaces, on peut aujourd'hui parler de « cyberguerre ». Vous avez évoqué les start-up qui ont une place stratégique et essentielle dans l'innovation, avez-vous pu analyser la part du budget consacrée à la R&D spécifique au domaine de la cyberdéfense ?

M. Christophe Blanchet. Vous proposez dans votre rapport l'idée d'une grande loi concernant la cyber-sécurité et je partage totalement votre avis quant à cette proposition. J'avais d'ailleurs déjà évoqué cela auprès du ministère en décembre dernier et je suis convaincu qu'il y a une véritable urgence à agir. À présent, pensez-vous qu'il soit du ressort et du devoir de la représentation nationale de légiférer en ce sens ? Avons-nous le temps d'attendre un projet de loi ou devons-nous écrire une proposition de loi ensemble ? Enfin, quelle devrait être la position de notre commission vis-à-vis de ces initiatives ?

M. Christophe Lejeune. Il y a deux jours, le commandant de la base de défense de Nancy a signé un contrat pour l'installation d'un laboratoire d'entraînement en matière de cyberdéfense, qui sera implanté à la caserne Verneau pour des questions évidentes de sécurité. Ce laboratoire fait partie du dispositif de cyberdéfense voulu par le Premier ministre, doté, à l'échelon national, de 300 ingénieurs. Ce laboratoire, qui fera notamment appel à des réservistes opérationnels, s'appuiera sur un partenariat avec Cyber-Detect et Airbus.

En matière de cyberdéfense, il est fondamental de s'assurer du parcours sur le long terme des futurs opérateurs, ainsi que vous l'avez d'ailleurs évoqué dans votre rapport.

Aussi le recrutement est-il particulièrement pointu, utilisant des critères militaires de sélection. La deuxième phase de développement de cet outil indispensable serait ensuite la finance et la santé. Le Grand Est est d'ailleurs une aire d'importants flux financiers. Ma question est donc la suivante : le problème majeur demeurant le recrutement, la mise en place de dispositifs indemnitaires particuliers pour faire face aux salaires élevés du civil est-elle envisageable ?

Mme Émilie Guerel. La cyber-sécurité est un sujet hautement sensible dans la sphère aérienne. Aussi, j'aimerais savoir si, réellement, un avion a déjà fait l'objet d'une cyber-attaque. En 2013, un chercheur spécialiste du hacking a évoqué la possibilité de pénétrer les cockpits d'avions, mais n'a jamais pu en apporter la preuve. En 2015, un autre chercheur assurait être parvenu à hacker le système de divertissement d'un avion de ligne mais sans en apporter, là encore, la confirmation. Lors de la dernière conférence *Black Hat* (réseau de conférences sur la sécurité de l'information), un hacker a évoqué la possible pénétration du système d'information d'un avion de ligne en vol en utilisant ses communications satellites. J'aimerais donc savoir si ces menaces sont réelles et réalistes et, si oui, de quelle manière la France s'en prémunit-elle ?

M. Charles de la Verpillière. Ma question concerne ce que vous avez appelé les OIV, c'est-à-dire les « opérateurs d'importance vitale ». On pense évidemment à tout ce qui concerne l'électricité avec EDF, RTE pour le transport et la distribution, la SNCF, les syndicats des eaux, les opérateurs de communication et les hôpitaux. Avez-vous le sentiment qu'il y a désormais chez tous ces opérateurs une certaine prise de conscience quant aux questions de cyber-sécurité et, qu'en conséquence, des mesures efficaces ont été prises ?

M. Jean-Philippe Ardouin. La Revue stratégique de la cyberdéfense, publiée le 12 février 2018, met en lumière le danger des attaques informatiques susceptibles de porter gravement atteinte aux intérêts de notre pays. Il convient de développer et de structurer le dispositif national de protection notamment contre l'espionnage informatique et la cybercriminalité. La France inscrit son modèle de cyberdéfense dans une vision de stratégie européenne et internationale, notamment par le canal d'organisations telles que l'Union européenne, l'OTAN et l'ONU. Aussi, quels sont les accords internationaux s'appliquant dans ce cas ? D'autre part, quelles sont les relations qui s'instaurent entre les différents protagonistes du numérique tels que les États, les acteurs publics et privés ?

M. Pieyre-Alexandre Anglade. Je tiens à saluer moi aussi la qualité du rapport qui nous est présenté. Je souhaite revenir, à la suite de notre collègue Joaquim Pueyo, sur la dimension européenne des enjeux de cyberdéfense. Comme les rapporteurs l'ont bien dit, le cyberespace ne connaît pas de frontières politiques ou juridiques ; c'est un espace aux contours impalpables, difficiles à cerner

concrètement. En revanche, certains États y mettent en œuvre des stratégiques politiques et conduisent à cette fin, directement ou non, des actions visant à déstabiliser nos États et nos entreprises. Dans ce contexte de menaces asymétriques visant tous les États européens, l'Europe est en première ligne. En effet, s'il appartient à chaque État de mettre en place à son niveau des réponses à ces menaces, il nous faut aussi construire un véritable bloc européen, animé d'un esprit de souveraineté européenne dans le domaine cyber, face à d'autres grands blocs de puissances actives dans cet espace. La France a-t-elle l'ambition de jouer un rôle moteur en la matière ? Au fil de vos auditions, avez-vous perçu un mouvement collectif de prise de conscience européenne en ce sens ?

M. Alexis Corbière. On rappellera que l'Union européenne et l'OTAN coopèrent en matière de cyberdéfense alors que, comme vous nous l'avez bien dit, les États n'ont guère d'amis dans ce domaine. La France dispose avec l'ANSSI d'un outil de cyberdéfense relativement indépendant, mais poursuit-elle néanmoins des coopérations internationales en matière de cyberdéfense ? Avec quels autres États, et en quoi consistent-elles ? Par ailleurs, outre les coopérations déjà mises en œuvre, avec quels autres États la France aurait-elle intérêt à coopérer en ce domaine ?

Je tiens aussi à saluer le travail conjoint de nos deux rapporteurs ; merci pour ce cyber-moment.

M. Jean-Michel Jacques. On mesure bien quels progrès les Européens doivent encore accomplir pour atteindre un niveau technologique suffisant en matière cybernétique, notamment dans le traitement du *big data*. D'ailleurs, la DGSI sous-traite le traitement de certaines informations à une société américaine du nom de Palantir. Peut-être est-il difficile de développer un Palantir français ; mais, à tout le moins, ne faudrait-il pas soutenir le développement d'un Palantir européen ?

M. Fabien Gouttefarde. Ma question s'adresse particulièrement à notre collègue rapporteur Bastien Lachaud. En effet, si l'on passe en revue les compétences de pointe en matière de cyberdéfense, on ne peut pas ne pas évoquer le centre d'excellence de l'OTAN en matière de cyberdéfense, situé à Tallin. À vos yeux, vaut-il mieux pour la France trouver sa place au sein d'une telle organisation – même parrainée par l'OTAN –, ou se tenir en dehors, surtout quand on tient compte des enjeux de normalisation des standards technologiques pour la cybersécurité ?

Mme Séverine Gipson. Voilà un intéressant rapport, qui nous ouvre l'esprit. Fondamentalement, comment s'assurer qu'un système cybernétique est sûr ?

M. Thomas Gassilloud. Je salue la qualité du travail de nos rapporteurs ; même si notre collègue Alexandra Valetta-Ardisson y a peu fait allusion, nous nous connaissons depuis longtemps. J'en viens à ma question, qui s'inscrit à la

suite de celles de nos collègues Pueyo, Anglade et Jacques. Le 6 juin dernier, la Commission européenne a annoncé le lancement d'un plan d'investissement numérique de neuf milliards d'euros en faveur de l'Europe numérique. Outre les fonds destinés au développement du calcul intensif et de l'intelligence artificielle, ce plan prévoit un investissement de deux milliards d'euros dans la cybersécurité. Est-ce suffisant, et quels projets européens vous paraissent prioritaires, en complément de ceux des États membres ?

M. Laurent Furst. Vous avez évoqué les moyens limités de l'ANSSI : cette agence est aujourd'hui un service du Premier ministre ; ce statut juridique est-il satisfaisant ? Gagnerait-elle à un statut plus autonome ?

Par ailleurs, si l'on considère que le cyberespace constitue un milieu d'opération à part entière au sens militaire du terme, cela n'a-t-il pas d'implications juridiques, peut-être constitutionnelles ?

Enfin, on sait que pour nuire à un pays et le déstabiliser profondément, le plus efficace est de viser ses infrastructures énergétiques, mais aussi bancaires. Avec la numérisation croissante des opérations bancaires, cette vulnérabilité va en augmentant. Suffit-il à vos yeux de laisser aux banques le soin de se protéger seules, ou l'État doit-il agir ?

M. Philippe Chalumeau. À la lumière de vos travaux, dont je tiens à souligner la qualité, quelle appréciation portez-vous sur les dispositions de la loi de programmation militaire que nous venons d'adopter concernant la cyberdéfense ?

Par ailleurs, si cyberdéfense et cybersécurité sont bien deux domaines distincts, une étroite coordination entre ces deux champs d'action de l'État n'est-elle pas nécessaire ?

M. Florian Bachelier. Je m'associe aux félicitations adressées à nos deux rapporteurs, sans oublier notre collègue Thomas Gassilloud. Votre intervention met bien en exergue les nouvelles menaces et leur caractère hybride. Elle montre bien que la cybersécurité ne concerne pas seulement les armées, mais toutes les institutions, toutes les organisations. C'est en outre à juste titre que votre rapport replace ces questions dans l'optique de la souveraineté, y compris à l'échelle européenne.

Dans ce contexte, les Parlements eux-mêmes sont visés par des attaques de plus en plus nombreuses et de plus en plus dures. À cet égard, je tiens à signaler à nos collègues que l'Assemblée nationale a changé de doctrine et conclu un partenariat avec l'ANSSI pour mettre en œuvre des mesures de protection, dont la pose de sondes.

Ma question porte sur les nouvelles opportunités qu'offre le domaine de la cybersécurité : on évalue à trois millions le nombre d'emplois qui seront créés

d'ici 2021 dans ce secteur en Europe. Comment mobiliser l'ensemble des filières de formation, notamment les filières courtes ?

Mme Alexandra Valetta-Ardisson, rapporteure. Mon collègue Bastien Lachaud et moi nous partagerons les réponses à ces questions, et même si certaines sont délicates, il y a une grande convergence de nos vues depuis le début de nos travaux.

Monsieur Chalumeau, s'agissant des moyens consacrés à la cyberdéfense dans la programmation militaire 2019–2025, il faut reconnaître que l'investissement consenti est très important et en adéquation avec les besoins et les demandes des acteurs concernés. L'ANSSI, pour sa part, méritera une attention particulière. S'agissant de la coordination des efforts accomplis dans les champs civil et militaire, celle-ci est déjà à l'œuvre et mérite d'être approfondie.

Monsieur Michel-Kleisbauer, interdire l'accès de certains acteurs aux technologies permettant de mener des cyberattaques est par nature difficile, car il s'agit de technologies duales, avec lesquelles n'importe qui peut se muer en cyber-attaquant. Notre rapport présente des développements plus précis, mais pour faire simple, il faut certainement affermir autant que possible le cadre légal applicable et les contrôles. C'est pour cela que nous plaidons pour l'adoption d'une loi sur le cyber.

Quant au forum sur la cybersécurité dont j'ai prononcé le discours de clôture hier, il m'a donné l'occasion d'intéressantes discussions avec tous types d'acteurs. De tels événements ont l'avantage de favoriser une large prise de conscience des enjeux de cybersécurité, qui concernent la société dans son ensemble. Je ne doute absolument pas du respect du secret de la défense nationale par les autorités présentes. Enfin, ce type de rassemblement permet aux civils et aux militaires de se parler, ce qui est bénéfique.

Concernant l'Europe, notre collègue Bastien Lachaud va vous répondre en détail. Je tiens simplement à dire que je ne suis pas opposée par principe à des initiatives européennes, et j'estime que l'échelle européenne est bien sûr pertinente. Mais on sait comment l'Union européenne fonctionne : le consensus est la règle en de telles matières, mais il est souvent lent à mûrir, et rien ne garantit même qu'il soit possible. Le risque est donc qu'un texte européen sur la cybersécurité ne devienne l'arlésienne. Mieux vaudrait pour la France coopérer avec un nombre plus restreint d'États plus allants que les autres en la matière.

Monsieur Blanchet, l'idée d'une loi sur le cyber, qui formalise une doctrine française sur le cyber, nous paraît excellente. Cela répond d'ailleurs à une demande unanimement exprimée par les responsables que nous avons entendus. C'est pourquoi cette idée constitue la première de nos recommandations. Notre commission mériterait d'ailleurs à mes yeux d'être saisie au fond d'un tel texte, mais ce n'est pas à moi d'en décider !

Quant à l'idée de créer un enseignement sur le cyber dans la scolarité, qui tient particulièrement à cœur à Bastien Lachaud, elle vise à la fois à généraliser des pratiques de cyber-hygiène et à susciter des vocations pour les métiers du cyber.

Recruter des spécialistes du cyber est une nécessité, et les conserver, les fidéliser, en est une autre. Or les rémunérations offertes pour ce type de compétences dans le secteur public sont souvent insuffisantes pour cela. L'ANSSI ou nos armées investissent dans la formation de jeunes spécialistes du cyber, mais les industriels leur offrent au bout de quelques années des postes deux à trois fois plus rémunérateurs. Faut-il le regretter ? Peut-être pas, lorsque ces spécialistes sont recrutés par des industriels français ; mais c'est assurément plus regrettable lorsqu'ils quittent le service public pour de grands industriels américains du numérique. Le problème est aujourd'hui réel, et les autorités publiques en sont réduites à d'invraisemblables acrobaties administratives pour conserver leurs spécialistes du cyber. Notre rapport formule plusieurs propositions d'ajustements statutaires visant à mieux rémunérer les agents de l'État, par exemple au moyen de primes ou de contrats de droit privé.

Concernant les opérateurs d'importance vitale, ce sont les opérateurs les plus protégés du pays, dont les dispositifs de sécurité font l'objet d'audits réguliers. Mais le risque zéro n'existe pas. Plusieurs de nos préconisations visent à réduire encore les risques, par exemple dans le cadre d'une loi sur le cyber, du développement de *clouds* souverains, ou de coopérations plus étroites entre le secteur public et le privé.

Madame Guerel, vous nous interrogiez sur la cybersécurité des avions. Nous avons entendu des représentants de l'industrie aéronautique et il en ressort que, ce secteur, comme d'autres, subit de multiples attaques. Mais ne soyons pas alarmistes : il y a différents degrés d'attaques et différents types de cibles. Des avions ont pu subir, par exemple, des attaques portant sur les systèmes de gestion des vidéos. Quant aux attaques portant sur les systèmes vitaux, les opérateurs concernés sont capables de les traiter.

M. Bastien Lachaud, rapporteur. Le Royaume-Uni a mis en place en 2014 un enseignement d'informatique dès l'école primaire, le Japon a prévu de faire de même au début des années 2020 pour tous les niveaux d'enseignement primaire et secondaire, et Israël a rendu un tel enseignement obligatoire au lycée. Selon nous, c'est le plus tôt possible dans la scolarité qu'il faut inculquer aux enfants les bonnes pratiques en matière cyber. Il suffit pour s'en convaincre de se rappeler que c'est en moyenne à onze ans que les jeunes Français se voient offrir leur premier téléphone intelligent : c'est avant cet âge qu'ils doivent être conscients des risques afférents à la protection de la vie privée et des données, ce qui contribuerait d'ailleurs à la lutte contre le cyber-harcèlement dans le secondaire.

S'agissant de la résilience de nos armées, Monsieur Becht, nos armements ne sont par nature pas invulnérables à des attaques cyber. Il est donc impératif que les nouveaux équipements soient systématiquement conçus pour pouvoir fonctionner en mode dégradé.

Concernant la coopération entre membres de l'Union européenne ou de l'OTAN, les États ont des capacités et des niveaux de compétence aujourd'hui très hétérogènes. Le risque est donc que des standards communs de protection soient moins ambitieux que les nôtres. De plus, un « bouclier cyber européen » pourrait même être contre-productif pour les États les plus vulnérables. En effet, il n'encouragerait pas ces États à développer leurs propres capacités de défense, alors même qu'un tel bouclier aurait nécessairement ses limites : en la matière, un peu comme pour la dissuasion, aucun État n'ouvre jamais la totalité de ses connaissances à ses partenaires, même les plus proches. Et ce n'est pas moi qui le dis, mais le directeur général de l'ANSSI. En somme, la coopération est nécessaire pour faire cesser les cyberattaques, mais on ne peut pas tout en attendre ; nous partageons des intérêts avec nos partenaires, mais la souveraineté reste la règle. Il existe à l'ONU une instance qui constitue un cadre approprié pour une telle coopération, le *Group of Governmental Experts*, mais celui-ci a dû interrompre ses travaux du fait de la défection des Russes et des Chinois. C'est dans un tel cadre que la France pourrait utilement faire la promotion de sa vision des rapports de droit international dans le cyberespace.

Quant à savoir s'il vaut mieux se placer au sein de l'OTAN ou en dehors pour faire prévaloir les vues françaises en matière de cybersécurité, encore faudrait-il que la France établisse une doctrine claire et que celle-ci trouve un écho parmi ses partenaires. Rien n'est certain en la matière. D'ailleurs, pour assurer le rayonnement d'une telle doctrine, les moyens dont dispose aujourd'hui notre ambassadeur pour le numérique, qui se limitent à trois collaborateurs, sont à l'évidence insuffisants.

En réponse à l'interrogation de Mme Mirallès sur la fiabilité des systèmes, les certifications délivrées par l'ANSSI permettent de s'assurer de la robustesse d'un produit. Nous formulons d'ailleurs le vœu, dans notre rapport, de conforter le processus de certification et de l'amplifier.

Pour revenir au plan de deux milliards d'euros proposé par l'Union européenne, la seule question qui vaille est : pour quoi faire ? Une nouvelle fois, nous avons le sentiment que l'argent est prêt à être dépensé mais qu'aucune stratégie n'a été établie afin de définir des priorités. Aujourd'hui, nul ne sait ainsi s'il faut investir dans la constitution d'un *cloud* européen ou dans un autre système. En somme, il est difficile de savoir si la somme engagée est suffisante dans la mesure où nous ne savons pas précisément ce qu'il faudrait financer.

Comme d'autres puissances, la France dispose de la capacité de mener des actions cyber-offensives dans le respect du droit international.

S'agissant du financement des activités de recherche et de développement, la loi de programmation militaire prévoit un investissement de 1,6 milliard d'euros. De plus, les entreprises investissent en moyenne entre 5 % et 8 % de leur chiffre d'affaires dans la sécurité de leurs systèmes d'information. Au-delà, nous n'avons pas eu accès à des informations plus précises, couvertes du reste par les dispositions législatives et réglementaires relatives au secret industriel.

La question de M. Pueyo me permet de rappeler que l'Union européenne dispose d'une agence spécialisée : l'ENISA (*European Network and Information Security Agency*). Cette agence a vocation à évoluer dans le cadre de la mise en place du système de certification à l'échelle européenne que j'évoquais précédemment. Pour la France, l'enjeu sera de veiller à ce que notre propre niveau de certification ne soit pas abaissé en raison d'un éventuel nivellement par le bas des normes de certification.

M. Marilossian nous a interrogés sur les réserves. Nous préconisons en effet un rapprochement des différentes réserves et le renforcement de leur rôle dans le cadre de la cyberdéfense.

Enfin, en réponse à l'interrogation de Mme Guerel, les flottes aériennes subissent quotidiennement des tentatives de piratage. Il semble relativement facile de *hacker* la bibliothèque de films mise à disposition des passagers. En revanche, accéder au système de navigation est beaucoup plus complexe, notamment parce que l'immense majorité de la flotte ayant été construite au début des années 2000, les avions sont assez peu connectés. Demain, les enjeux seront tout autres !

Pour conclure, j'évoquerai Palantir. Nous recommandons que les questions les plus sensibles restent protégées par les dispositifs garantissant la préservation de la souveraineté nationale. S'agissant de Palantir en particulier, il nous a été indiqué que lorsque les services de renseignement utilisaient les solutions proposées par cette société, une barrière hermétique était abaissée afin de garantir que les données ne s'échappent pas des serveurs sur lesquels le logiciel est installé. En d'autres termes, normalement la NSA n'a pas accès aux données de la DGSI. J'ajoute que les solutions de Palantir sont utilisées par divers acteurs, dont des avionneurs pour le traitement des données prédictives. Le mot de la fin sera la reprise du mantra de l'ensemble des acteurs rencontrés : en ce domaine, nous avons des alliés mais pas vraiment d'amis…

M. le président. Je remercie les rapporteurs pour toutes ces précisions et pour ce travail que l'ensemble de la commission semble avoir apprécié.

Mes chers collègues, dès lors que tout le monde s'est félicité de la qualité de ce rapport, je vous propose de le rendre public !

*

* *

*La commission **autorise** à l'unanimité le dépôt du rapport d'information sur la cyberdéfense en vue de sa publication.*

ANNEXE :

AUDITIONS DE LA MISSION D'INFORMATION

(Par ordre chronologique)

➢ **Séminaire relatif à la Revue stratégique de cyberdéfense organisée par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) – M. Louis Gautier**, secrétaire général de la défense et de la sécurité nationale, **M. l'ingénieur général de l'armement Guillaume Poupard**, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), **M. le colonel Emmanuel Germain**, directeur général adjoint de l'ANSSI, **M. l'ingénieur en chef de l'armement Frédéric Valette**, rapporteur de la Revue stratégique de cyberdéfense, **M. l'ingénieur en chef de l'armement Jean-Marie Desmartis**, conseiller du SGDSN pour l'industrie et les questions numériques, **M. Julien Barnu**, directeur de cabinet du directeur général de l'ANSSI, **M. Gwénaël Jézéquel**, conseiller du SGDSN pour les relations institutionnelles.

➢ **Direction générale de la gendarmerie nationale – M. le colonel Éric Freyssinet**, chef de la mission numérique de la gendarmerie nationale.

➢ **MBDA – M. Olivier Martin**, secrétaire général, **M. Jean-Paul Defransure**, directeur groupe information management, et **Mme Patricia Chollet**, chargée des relations avec le Parlement.

➢ **Institut de recherche stratégique de l'École militaire – M. le colonel Olivier Passot**, directeur du domaine « pensée stratégique », et **M. François Delerue**, chercheur « cyberdéfense et droit international ».

➢ **Direction générale de l'armement – M. Frédéric Valette**, chargé de mission cyberdéfense auprès du Délégué général pour l'armement, rapporteur de la Revue stratégique de cyberdéfense.

➢ **Airbus Group – M. Gérard Moisselin**, conseiller sécurité et territoires du président d'Airbus, **M. Pascal Andrei**, directeur de la sécurité, **M. Philippe Bottrie**, directeur des affaires publiques France, et **Mme Annick Perrimond du Breuil**, directeur des relations avec le Parlement.

➢ **Direction du renseignement et de la sécurité de la Défense – M. le général de corps d'armée Jean-François Hogard**, directeur du renseignement et de la sécurité de la défense.

➢ **Naval Group – M. Jean-Michel Orozco**, directeur de la cybersécurité Groupe et mission navals, et **Mme Carole Putman**, adjointe au directeur des affaires publiques et européennes.

➢ **Direction générale de la sécurité extérieure –M. Patrick Pailloux**, directeur technique.

➢ **Direction générale des systèmes d'information et de communication du ministère des Armées** – **M. le vice-amiral d'escadre Arnaud Coustillière**, directeur général des SIC.

➢ **Commandement de la cyberdéfense de l'état-major des armées – M. le général de brigade Olivier Bonnet de Paillerets**, commandant du COMCYBER, **Mme Isabelle Valentini**, adjointe « stratégie », **Mme le capitaine de frégate Audrey Hérisson**, responsable « développement national » du pôle « stratégie et développement ».

➢ **CyberTaskForce – M. Sébastien Garnault**, fondateur de la CyberTaskForce, fondateur du cabinet Garnault & Associés, **M. Florent Skrabacz**, PDG de Shadline, **Mme Coralie Héritier**, PDG d'IDnomic, **M. Jean Larroumets** PDG d'EGERIE, **M. Guillaume Vassault-Houlière**, PDG de YesWeHack.

➢ **Kaspersky Lab France – M. Tanguy de Coatpont**, directeur général, **M. Félix Aimé**, *security researcher*, et **M. Arnaud Dechoux**, directeur de clientèle chez Burson-Marsteller.

➢ **Fédération Européenne des Experts Cybersécurité (FEEC) – M. Olivier Feix**, président de la FEEC, président de Zenon Public Affairs, **M. Olivier de Maison-Rouge**, vice-président de la FEEC, avocat au cabinet Lex Squared.

➢ **Comité Richelieu – M. Jean Delalandre**, délégué général**,** et **M. Thierry Rouquet**, administrateur du Comité Richelieu et membre de la commission défense, PDG de Sentryo.

➢ **OTAN – M. le général d'armée aérienne Denis Mercier**, commandant suprême allié Transformation de l'OTAN, **M. Mathieu Hédoin**, conseiller diplomatique du SACT et **Mme le capitaine Adeline Blanvillain**, aide de camp du SACT.

➢ **Mme Anne Cammilleri,** professeure des universités, Université Paris 13 – Sorbonne Paris Cité, co-directrice du Master Sécurité Défense et Intelligence Stratégique, de Sciences Po Rennes, et **M. le général Philippe Boone**, co-directeur du Master.

➢ **Agence nationale de la sécurité des systèmes d'information – M. l'ingénieur général de l'armement Guillaume Poupard**, directeur général, et **M. Christian Daviot**, chargé de mission stratégie.

➢ **M. le colonel Olivier Kempf**, officier cyberdéfense à l'état-major de l'armée de terre.

➢ **M. Kavé Salamatian**, professeur des universités, Université de Savoie et chercheur associé à la Chaire Castex de cyberstratégie.

➢ **Groupe Ziwit** – **M. Mohamed Boumediane**, fondateur et président directeur général.

➢ **Thales** : contribution écrite.