Revue stratégique de cyberdéfense

12 février 2018

SGDSN

SOMMAIRE

Introduction - L'affirmation d'une nouvelle ambition pour la France dans la cyberdéfense

A l'heure où les attaques informatiques sont susceptibles de porter à tout moment gravement atteinte aux intérêts de la Nation, notre pays doit adapter sa posture de cyberdéfense avec l'ambition de mieux faire respecter sa souveraineté numérique.

A des cyberattaques croissantes en nombre, en intensité et en sophistication, il convient d'opposer un dispositif national de protection et de défense informatique robuste. Celui-ci requiert la mobilisation de capacités et de compétences diverses, au sein de l'Etat mais aussi au cœur de la société.

Mieux intégrer nos moyens de défense cybernétique

Face aux menaces numériques, le degré de résistance d'une Nation et son aptitude à la résilience reposent tout autant sur les moyens que sur l'organisation de sa cyberdéfense. Celle-ci suppose une bonne coordination des différents services de l'Etat concernés, une coopération de ceux-ci avec les opérateurs d'importance vitale[1] et de services essentiels, la diffusion auprès des acteurs économiques et dans la population de bonnes pratiques préventives et, en cas de crise, l'adoption rapide de mesures adaptées.

Or, par rapport aux quatre autres pays qui partagent avec elle des responsabilités internationales particulières (les Etats-Unis, la Russie, la Chine et le Royaume-Uni[2]), la France accuse encore, en dépit d'un effort récemment accentué, un déficit en matière de sécurité numérique.

C'est pourquoi la revue stratégique de cyberdéfense propose de mieux structurer et de développer notre dispositif national de protection. A cette fin, elle recommande d'élaborer une programmation spécifique des moyens publics consacrés à la cyberdéfense.

Renforcer la résilience des systèmes vitaux de la France

Notre pays doit avoir comme premier objectif le durcissement de ses dispositifs de cyberprotection et le renforcement de la résilience des réseaux de l'Etat et des opérateurs d'importance vitale et de services essentiels. Il faut en effet pouvoir garantir avant tout la continuité de fonctions primordiales.

[1] En France, sous la dénomination d'opérateurs d'importance vitale (OIV) sont regroupés 249 organismes indispensables à la vie de la Nation.

[2] Tous membres permanents du Conseil de sécurité des Nations unies et Etats nucléaires officiellement dotés au sens du Traité de non-prolifération (TNP).

A l'image du corps humain qui, en situation de stress, préserve d'abord ses organes vitaux, les fonctions et les missions essentielles à la survie de la Nation doivent pouvoir résister à un choc cyber massif. Cette résistance au choc dépend du niveau de protection, de redondance et de résilience de certains systèmes d'information de l'Etat et de quelques délégataires de services publics. Il convient de pouvoir assurer la permanence opérationnelle de certaines fonctions et la continuité territoriale des réseaux de communication.

Au premier rang des priorités figure, à côté des impératifs de défense nationale, la protection des secteurs des communications électroniques et de l'approvisionnement en énergie électrique. Alors que ces secteurs fournissent des services indispensables, une cyberattaque à leur encontre peut entrainer des répercussions pour l'ensemble des activités vitales et des effets potentiellement catastrophiques sur l'aptitude à la résilience de la Nation.

Il s'agit ensuite de garantir le fonctionnement, le cas échéant en mode dégradé, des services chargés de la protection civile, de la sécurité publique, des urgences médicales et des hôpitaux[3].

Il faut, en outre, être en mesure de rétablir aussi rapidement que possible le fonctionnement des principales infrastructures de transport, qu'un incident informatique, même d'ampleur limitée, peut désorganiser de façon massive[4]. Nos infrastructures de transport doivent également être protégées contre d'éventuelles attaques informatiques conduites à des fins de sabotage.

Enfin, plusieurs activités sont indispensables au bon fonctionnement de notre vie démocratique, de notre société et de notre économie. La protection de grandes institutions qui sont les piliers de notre démocratie comme le Parlement, le Conseil constitutionnel ou l'autorité judiciaire doit, ainsi, être considérée comme de toute première importance. La sécurisation de nos processus électoraux et du service public de la communication audiovisuelle requiert également une attention particulière.

Œuvrer internationalement pour la stabilité du cyberespace

Afin de contribuer pleinement à la stabilisation du cyberespace, l'action internationale de la France devrait viser trois objectifs :

[3] En 2015, en France métropolitaine et dans les DROM, 723 services d'urgences situées dans 644 établissements de santé ont traité 20,3 millions d'actes. Aux côtés des structures des urgences hospitalières, 104 SAMU et 410 SMUR assurent l'orientation, la prise en charge préhospitalière et le transport des malades (DRESS, *Les établissements de santé*, édition 2017, http://drees.solidarites-sante.gouv.fr/IMG/pdf/28-2.pdf).

[4] A titre d'exemple, la panne d'un seul poste de signalisation ferroviaire à l'été 2017 affecta plus de 50 000 usagers de la SNCF. S'agissant du transport aérien, notre pays doit pouvoir garantir le maintien d'un flux minimal de trafic domestique et international à la suite d'une attaque informatique. Ceci suppose de disposer d'une capacité à restaurer, rapidement et dans des conditions acceptables au regard de la sécurité des vols, l'activité d'au moins une des deux plateformes aéroportuaires parisiennes, lesquelles représentent à elles seules plus de la moitié du trafic aérien national.

- travailler à la régulation du cyberespace, via le respect et la mise en œuvre du droit international existant et des normes de comportement agréées, ainsi que via l'adoption, le cas échéant, de nouvelles normes applicables au comportement des Etats comme à celui des acteurs privés dans le cyberespace. C'est un modèle de régulation concertée de l'espace cyber à l'échelle européenne et internationale qui devrait être recherché ;
- prévenir les attaques informatiques par le renforcement de nos coopérations techniques, organiques et opérationnelles avec nos alliés et partenaires, notamment au sein de l'Union européenne et de l'Organisation du traité de l'Atlantique Nord (OTAN) ;
- être en capacité de gérer une crise internationale liée à une attaque cyber contre elle ou l'un de ses alliés ou partenaires, en définissant des modalités de réaction qui prendraient pleinement en compte les volets politico-diplomatiques et internationaux de celle-ci.

Sept principes pour une ambition de cyberdéfense renforcée

Le cyberespace apparaît aujourd'hui comme un catalyseur de progrès mais aussi un lieu de confrontation, de domination et de trafics en tout genre. Cette évolution n'est ni inéluctable ni irréversible. Ce qui était sans doute illusoire ou trop idéaliste était de croire qu'un tel territoire, offert à l'activité humaine, pourrait s'autoréguler, résister aux forces économiques et politiques l'accaparant, rester sans loi ni juge.

C'est pourquoi l'objet de la présente revue, une fois présenté l'état de la menace et de nos vulnérabilités, est de décrire une stratégie de cyberdéfense robuste et d'exposer les propositions que pourrait faire la France pour une régulation internationale du cyberespace. Elle propose, dans cette logique, de placer au cœur de l'ambition française en matière de cyberdéfense sept grands principes :

1. accorder une priorité à la protection de nos systèmes d'information ;
2. adopter une posture active de découragement des attaques et de réaction coordonnée ;
3. exercer pleinement notre souveraineté numérique ;
4. apporter une réponse pénale efficace à la cybercriminalité ;
5. promouvoir une culture partagée de la sécurité informatique ;
6. contribuer à une Europe du numérique confiante et sûre ;
7. agir à l'international en faveur d'une gouvernance collective et maîtrisée du cyberespace.

Pour suivre l'avancée des différentes recommandations, la revue stratégique de cyberdéfense préconise la mise en place d'un rapport semestriel d'avancement et de mise en œuvre à la charge du SGDSN, transmis au comité de pilotage cyber.

Partie I. Les dangers du monde cyber

Comme le soulignait le Livre blanc sur la défense et la sécurité nationale de 2013, *« les systèmes d'information sont désormais une donnée constitutive de nos sociétés »*[5]. Dès lors, il est impératif que le cyberespace demeure un espace de confiance pour les acteurs publics, les entreprises et les particuliers. Or, si l'espace numérique est un lieu de communication et d'échanges favorables au progrès, il est également devenu un lieu de confrontation. Les actions offensives à l'encontre des systèmes informatiques de l'État, des infrastructures critiques ou des grandes entreprises sont quotidiennes, sans que l'on puisse toujours en saisir l'origine et en comprendre les motivations, ni même distinguer avec certitude qui, acteurs étatiques ou non étatiques, en sont les commanditaires et les exécutants.

Force est de constater que la plupart des crises intérieures ou internationales et des conflits inter ou intra-étatiques ont désormais une dimension cyber. Le constat d'une exposition accrue de nos sociétés de plus en plus numérisées et interconnectées au risque de crises cyber majeures résultant d'attaques massives ou produites par des contaminations systémiques s'impose sans conteste.

A ce jour, rares sont les analyses de la menace cyber émanant de sources publiques. Les Etats, dont la France, sont en effet réticents à établir ouvertement un diagnostic qui révélerait pour partie leurs capacités de cyberdéfense. En revanche, plusieurs entreprises privées, notamment des éditeurs de solutions antivirus, disposent du fait de leur activité de très nombreuses données sur l'état de la menace cyber et en ont produit des évaluations pertinentes. Si ces évaluations doivent être prises avec précaution dans la mesure où elles peuvent servir des intérêts commerciaux, une fois « objectivées » elles se révèlent utiles pour se former une opinion et comprendre certains concepts communément diffusés. Il y sera fait référence en tant que de besoin dans la suite de la revue pour appréhender, illustrer et mieux cerner les dangers du monde cyber.

Les caractéristiques, le mode de propagation, les évolutions et l'intensification de la menace cyber sont des facteurs dont la compréhension est en effet indispensable pour construire un dispositif national de protection et de défense informatique efficace et pour consolider un modèle pertinent de cybersécurité pour la société.

D'origine étatique ou non, à visée universelle ou non, émanant d'organisations ou de simples individus, la principale caractéristique de la menace cyber est son caractère polymorphe. Elle peut s'en prendre de façon déterminée à un pays tout entier dans le but de lui nuire gravement, comme elle peut causer tort à tout un chacun - utilisateurs d'ordinateurs, d'objets connectés - de façon indistincte et avec une nocivité limitée. C'est pourquoi la présente revue opère nécessairement des distinctions, en se préoccupant

[5] *Livre blanc sur la défense et la sécurité nationale*, 2013 (http://www.livreblancdefenseetsecurite.gouv.fr/).

prioritairement des menaces qui peuvent affecter de façon absolue notre défense et notre sécurité nationale et de celles qui peuvent causer des effets systémiques sur le fonctionnement de notre société.

1.1. Des menaces en évolution rapide

Le constat est connu et partagé : la menace d'origine cyber ne cesse de croître dans ses formes et son intensité. Les attaquants informatiques poursuivent quatre types d'objectifs, non exclusifs entre eux : l'espionnage, les trafics illicites, la déstabilisation et le sabotage.

Dans la poursuite de ces objectifs, les attaquants informatiques peuvent être amenés à conduire aussi bien des opérations très ciblées que des actions massives et indiscriminées. Avec des objectifs divers, les attaques ont des effets également très variables : elles peuvent être invisibles - lors d'une exfiltration discrète de données par exemple - ou à l'inverse paralyser totalement l'activité de l'entité visée ; les éventuels dommages causés peuvent être facilement réversibles ou, au contraire, nécessiter de longs travaux de reconstruction.

1.1.1. L'espionnage informatique

Pénétrant au cœur des systèmes d'information qu'elles visent, les attaques informatiques présentent pour leurs auteurs le double avantage d'être particulièrement efficaces pour dérober des données de façon massive et d'être très difficilement attribuables, ce qui limite les risques d'être poursuivi sur le plan judiciaire.

L'objectif d'espionnage informatique est d'abord à la portée des services de renseignement des pays techniquement avancés qui, depuis plus d'un demi-siècle, ont développé des systèmes d'interception des communications à des fins d'espionnage économique, technologique ou politique. L'espionnage informatique n'est qu'une transposition dans le monde numérique d'activités traditionnelles de renseignement. Cette forme d'espionnage n'est cependant plus l'apanage quasi exclusif des services spécialisés des Etats du fait de la diffusion des technologies et des compétences opératoires.

La transformation numérique du renseignement s'est accélérée dans les années 2000 avec la prise de conscience par les pouvoirs publics, mais aussi par certaines entreprises, du rendement redoutablement efficace des attaques informatiques dans une société de plus en plus numérisée. De nombreux pays ont ainsi développé des capacités cyber offensives pour récupérer, par le biais d'attaques informatiques, des renseignements devenus plus difficiles à obtenir par des moyens traditionnels. Les premières cyberattaques d'envergure révélées le furent aux Etats-Unis et avaient pour objectif le pillage de savoir-faire industriels. Outre-Atlantique, elles furent régulièrement attribuées à la Chine. Dévoilée publiquement en janvier 2010, l'opération *Aurora* a ainsi touché au moins une trentaine d'entreprises américaines, parmi lesquelles *Google*, *Microsoft*, *Yahoo* et *Adobe*. En 2013, la société américaine de sécurité informatique *Mandiant* révéla une campagne d'attaque encore plus massive qu'elle a imputé à un groupe d'attaquants chinois identifié. Ce groupe aurait pénétré

plus de 150 institutions et industriels dans les pays occidentaux pendant près d'une dizaine d'années.

Aujourd'hui, 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.

1.1.2. La cybercriminalité

Jusqu'au milieu des années 1990, la cybercriminalité se réduisait à des actions ponctuelles conduites par des *hackers* isolés, pour lesquels la prouesse technique elle-même, au-delà de toute motivation politique ou financière, constituait souvent une finalité en tant que telle. Si ces actions pouvaient impliquer des intrusions dans des systèmes d'information sensibles, publics ou privés, leurs effets restaient néanmoins très limités. Les liens entre *hackers* et certains régimes politiques étaient alors anecdotiques et leurs actions se limitaient surtout à des campagnes de « défacement » de sites Internet.

Au cours des années 2000, les réseaux cybercriminels se sont peu à peu développés et professionnalisés. L'apparition en 2010 du bitcoin puis d'autres monnaies virtuelles, associée à la mise en place du réseau d'anonymisation *Tor*, a créé les conditions propices à une véritable explosion de la cybercriminalité. S'il existe peu de statistiques précises en raison du faible taux de déclaration des cybercrimes, la multiplication du nombre d'outils d'attaque informatique en vente sur le *darkweb* (*cf. glossaire*) témoigne de cette contagion.

Les cybercriminels parviennent dorénavant à capter des sommes très importantes d'argent. Pour cela, ils utilisent deux principales méthodes, véritables transpositions dans le monde numérique de pratiques criminelles traditionnelles. La première consiste à voler directement, via Internet, de l'argent ou des informations sensibles à des entreprises, à des banques ou à des particuliers, par exemple en dérobant des informations bancaires, en procédant à des virements frauduleux, ou en exfiltrant puis en revendant sur le *darkweb* des informations précieuses. Les données des entreprises et des particuliers représentent en effet une véritable manne financière. Des groupes cybercriminels se livrent ainsi à des vols d'envergure comme celui des données de plusieurs milliards de compte de la société YAHOO en 2013. La seconde méthode utilisée par les cybercriminels consiste à rançonner leurs victimes, soit en les menaçant de dévoiler des informations qu'ils ont préalablement exfiltrées de leur système d'information, soit en paralysant leur activité. Si la technique du déni de service, qui permet de rendre temporairement indisponible un site Internet, a longtemps été utilisée à cette fin, on constate aujourd'hui une utilisation croissante de rançongiciels (*cf. glossaire*). Enfin, au-delà des attaques informatiques, l'espace numérique est également utilisé pour mener de façon anonyme des activités criminelles (ventes sur Internet de produits illégaux, diffusion de contenus illicites, etc.).

Au cours des dernières années, on constate en outre un effacement progressif de la frontière entre lutte contre cybercriminalité et objectifs de cyberdéfense, en raison soit de la nature

ambiguë de certaines attaques, soit de l'ampleur de leurs effets. On observe en effet l'apparition d'attaques informatiques conduites à des fins de cybercriminalité mais qui, par leur caractère indiscriminé et leurs importantes capacités de propagation, sont susceptibles de paralyser des activités critiques et constituent donc une menace en matière de sécurité nationale. En outre, la frontière entre les groupes cybercriminels et les Etats est de plus en plus difficile à établir, notamment en raison de l'utilisation croissante par les cybercriminels d'outils développés par des agences de renseignements puis divulgués sur Internet à la suite de piratages informatiques. Le marché noir des failles informatiques intéresse autant les services de renseignement que les groupes cybercriminels.

1.1.3. La déstabilisation

Le troisième type d'objectif poursuivi par les attaquants informatiques est la déstabilisation. Récemment observé, notamment lors des dernières élections présidentielles américaines et françaises, mais déjà repéré dans des actions de propagande ou de défiguration (*cf. glossaire*) de sites politiques à l'occasion de conflits ou de crises, ce type d'opérations est lié au développement d'Internet et des réseaux sociaux. Longtemps, l'essor d'Internet et des services en ligne a été considéré comme un facteur favorisant la liberté d'expression ainsi que la diffusion du savoir et de l'information. Ces nouveaux moyens de communication, échappant a priori au contrôle des Etats et s'affranchissant des frontières, devaient favoriser la liberté d'opinion. Cette vision n'est pas erronée. Internet a ainsi joué un rôle indéniable dans les « printemps arabes » et, dans certains cas, il a permis à des *lanceurs d'alerte* de dénoncer utilement certains abus.

Nouvel espace d'expression, l'espace numérique est aussi exploité dans une logique de propagande politique et de propagation d'idéologies aux contenus très contestables. Nombre de groupes extrémistes se sont ainsi appropriés non seulement l'espace des réseaux sociaux, mais aussi les outils mis en œuvre par les moteurs de recherche ou certaines applications, dans le but de diffuser largement leurs idées et atteindre de nouvelles cibles. Mise en ligne en mars 2016, l'expérience de l'intelligence artificielle développée par MICROSOFT, afin d'apprendre à partir du comportement des internautes comment interagir avec eux sur le réseau social *Twitter*, a ainsi été rapidement détournée de son but, au demeurant contestable. Manipulée, cette « intelligence artificielle » a contribué à la diffusion de plus en plus fréquente de messages racistes, haineux et négationnistes. Si, dans ce cas particulier, la cause et l'impact du détournement sont mesurables, il n'en est pas de même des actions d'influence conduites au quotidien auprès des utilisateurs des réseaux sociaux.

Des actions de propagande et d'influence peuvent aisément être conduites sur les réseaux sociaux, ceux-ci, contrairement aux médias traditionnels, ne cherchant ni à cautionner ni à contrôler systématiquement les contenus auxquels ils donnent accès. Des faits non vérifiés, voire délibérément faux, peuvent ainsi être massivement relayés sur Internet, aux côtés des informations produites par les médias traditionnels, sans que les uns soient facilement distinguables des autres. Les *fake news* se diffusent même beaucoup plus vite que les faits réels, notamment parce que le seul critère de diffusion d'une information sur les réseaux

sociaux est l'engagement des utilisateurs, ce qui donne une prime aux contenus qui émeuvent, choquent ou font réagir. Quelques opérateurs acceptent cependant de coopérer avec les autorités publiques pour entraver la diffusion de contenus relevant de la pédopornographie et de la propagande terroriste. Pour autant, au nom de la liberté d'expression et de leur neutralité, quand ce n'est pas par facilité, de nombreux autres acteurs du numérique laissent libre cours à la diffusion d'idées ou de messages, fussent-ils des incitations à la haine et au crime.

Tous les outils classiques de la publicité sur Internet (diffusion ciblée de messages, analyse des données échangées sur les réseaux sociaux...) sont très facilement retournables à des fins de propagande et d'influence. Des techniques élémentaires comme le *flooding* (*cf. glossaire*), qui consiste à diffuser massivement de l'information inutile pour diminuer la visibilité d'un contenu ciblé, peuvent accompagner ces opérations. En sus de ces méthodes il est également aisé pour manipuler l'opinion de fabriquer l'information, de défigurer des sites Internet ou d'usurper des comptes de réseaux sociaux. Le vol de données à la suite d'une intrusion informatique puis leur publication sur Internet, parfois accompagnée de fausses informations, sont de plus en plus utilisés pour semer le doute, jeter le discrédit sur un individu, une entreprise, une organisation, un parti, voire pour déstabiliser un processus politique ou un procès.

Dans ce contexte, certains Etats ont développé une cyberstratégie qui ne se limite pas aux systèmes d'information mais s'étend à l'ensemble de la sphère informationnelle. Leur action peut aller jusqu'à la censure des contenus des échanges dans l'espace numérique, voire à la conduite d'actions d'influence. Ainsi, de nombreux pays ont imposé des conditions draconiennes aux pourvoyeurs d'accès afin de pouvoir contrôler les messages échangés sur Internet et les réseaux sociaux et certains agissent aussi à l'extérieur de leurs frontières pour influencer les opinions publiques. On assiste ainsi à des actions de propagande ou de déstabilisation menées à grande échelle, soigneusement préparées et orchestrées, mettant en œuvre différents vecteurs tels que la manipulation des réseaux sociaux, l'exfiltration puis la divulgation massive de données sensibles sur Internet. Ainsi, à l'occasion de la campagne présidentielle américaine de 2016, la compromission des messageries électroniques et la divulgation massive d'informations confidentielles concernant des membres de l'équipe démocrate ont suffisamment perturbé le processus électoral pour que le président Barack OBAMA accuse ouvertement la Russie d'avoir orchestré les attaques ayant ciblé la candidate démocrate. *FACEBOOK* a par ailleurs confirmé au Congrès américain en octobre 2017 que des campagnes publicitaires massives avaient été achetées par des acteurs russes sur ce réseau pour peser sur le débat électoral aux Etats-Unis, sans d'ailleurs que cette pratique ne soit jugée contraire au règlement de la plateforme.

La problématique de la propagande numérique, comme de la propagande en général, est délicate à traiter de manière exhaustive et déborde largement le cadre d'une revue de cyberdéfense. C'est pourquoi, en la matière, la présente revue ne s'est intéressée qu'aux seules activités menées par des groupes terroristes et des puissances étrangères dans l'objectif de provoquer des actions violentes ou déstabilisatrices pour notre société.

1.1.4. Le sabotage informatique

Les attaques informatiques, dont les effets restaient autrefois confinés à l'espace numérique, peuvent désormais avoir des impacts, potentiellement catastrophiques, dans le monde physique. La numérisation des systèmes de production et leur interconnexion croissante les exposent en effet de plus en plus au risque cyber. Une attaque informatique est dorénavant susceptible de paralyser l'activité d'une entité non seulement en bloquant ses réseaux, mais aussi en détruisant ses équipements les plus critiques. Ces actions de sabotage peuvent avoir des conséquences permanentes ou réversibles, locales ou systémiques, et offrent aux attaquants une gamme d'effets produits extrêmement large. Des attaques récentes, dont certaines ont servi de tests, révèlent une évolution inquiétante, notamment par la nature des cibles visées (sites industriels et infrastructures critiques).

L'attaque informatique subie par l'Estonie en avril 2007 a précipité une prise de conscience de ce type de risque. Cette attaque a en effet paralysé des activités essentielles au fonctionnement de ce pays pendant plusieurs semaines : s'appuyant sur la technique du déni de service distribué (DDOS - *cf. glossaire*), l'offensive a bloqué des sites Internet gouvernementaux ainsi que des médias, des partis politiques et des activités bancaires ; des numéros d'urgence sont même restés indisponibles pendant de courtes périodes. Le gouvernement estonien avait alors accusé la Russie d'être à l'origine de l'attaque. L'année 2010 et les révélations concernant le logiciel *Stuxnet*, déployé pour entraver le programme iranien d'enrichissement d'uranium, a constitué un tournant dans l'appréciation des usages possibles et de l'efficacité de l'arme cyber. Premier « ver informatique » utilisé pour enrayer un système industriel, *Stuxnet* ne procédait pourtant pas de techniques nouvelles mais d'une combinaison unique et extrêmement sophistiquée de plusieurs techniques, dont l'exploitation de multiples vulnérabilités *zero-day* et le recours à des modes d'infection multiples. Cette attaque s'est appuyée sur une préparation minutieuse et une connaissance précise des procédés industriels mis en œuvre dans le programme nucléaire iranien. Moins destructrice et surtout moins explicite, mais néanmoins fortement démonstrative, l'attaque par sabotage informatique de la chaine de télévision *TV5 Monde* en avril 2015 a constitué la première action de cette nature affectant les intérêts français[6]. La remise en état du système, qui a justifié une intervention en urgence de l'ANSSI, a coûté plusieurs millions d'euros et pris plusieurs jours. De la même façon, l'attaque *NotPetya*, qui a paralysé de nombreuses sociétés ayant des intérêts en Ukraine en 2017, a été particulièrement rapide et violente. Les attaquants ont pris le contrôle des serveurs de la société qui conçoit le logiciel *M.E.doc* pour y insérer une porte dérobée (*backdoor - cf. glossaire*) plus de deux mois avant de déclencher cette attaque fulgurante. Ce logiciel, qui équipe 80 % des entreprises ukrainiennes, a permis aux attaquants, par le biais d'une mise à jour transportant un logiciel malveillant destructeur, de contaminer simultanément de nombreuses entreprises présentes en Ukraine et ainsi de

[6] Le site Internet de la chaîne et ses comptes sur les réseaux sociaux diffusaient de la propagande djihadiste, son système de production d'images était inutilisable et la diffusion interrompue. *TV5 Monde*, qui émet dans deux cents pays pour cinquante millions de téléspectateurs, affichait un écran noir.

paralyser leur activité. Sa propagation à la France, heureusement peu touchée, par les réseaux d'entreprises disposant de filiales ukrainiennes, montre la dangerosité de ce type d'attaques massives et indiscriminées qui, par ricochet, sont susceptibles de paralyser des activités essentielles de notre pays sans que celui-ci soit directement ciblé.

Le sabotage informatique, avec des conséquences destructrices dans le monde physique, est aujourd'hui une réalité. Il représente la menace la plus préoccupante, que celle-ci vise directement notre pays comme dans le cas de *TV5 Monde*, ou que nous en subissions les effets collatéraux[7]. De surcroît, la possible collusion de groupes terroristes et d'acteurs possédant de fortes capacités techniques dans ce domaine, fait craindre qu'un jour un sabotage informatique perpétré par de tels mouvements soit possible. Ces actions pourraient être conduites entièrement depuis l'étranger en assurant une plus grande protection de leurs auteurs. Cette hypothèse souligne encore la nécessité de renforcer la protection cyber des infrastructures les plus critiques.

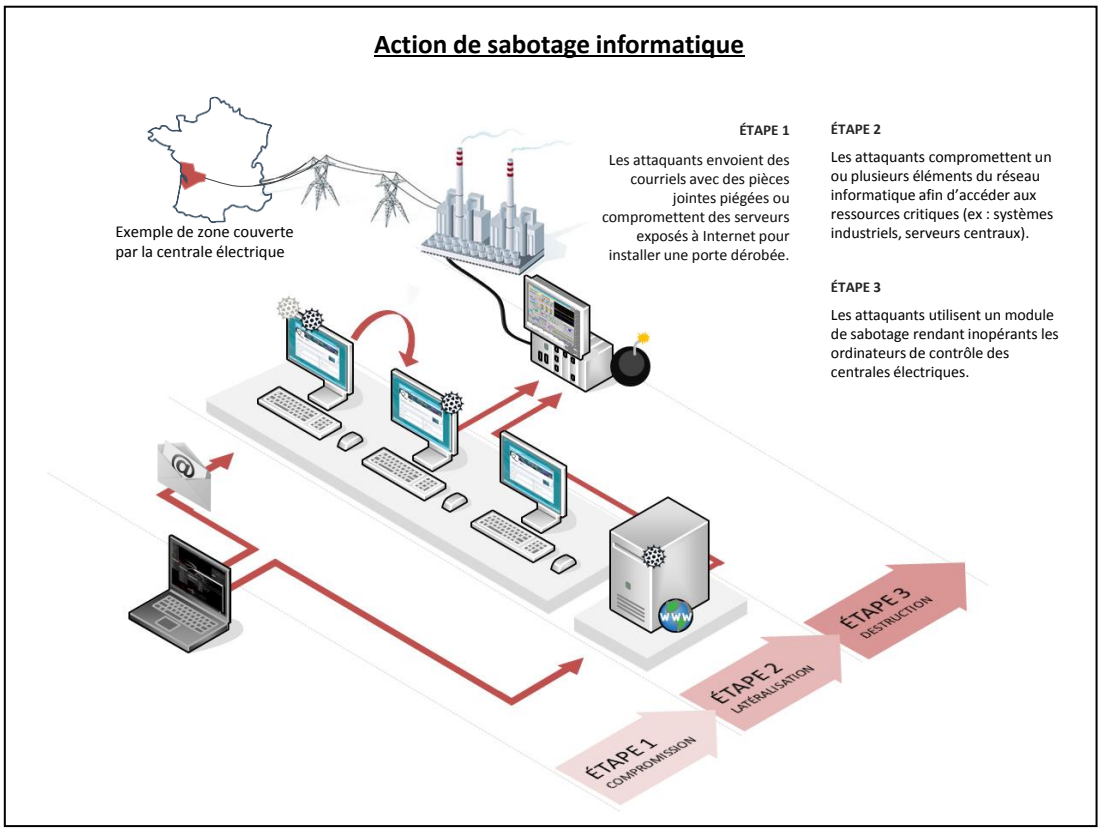


Figure n°1 : Action de sabotage informatique

1.2. Les grands principes d'action et les modes opératoires des attaques informatiques

La plupart des attaques informatiques obéissent à des principes d'action généraux. Le processus suivi par un attaquant informatique a été modélisé en 2011 par des travaux

[7] La société *Saint-Gobain* a été victime en 2017 du rançongiciel NotPetya qui visait l'Ukraine.

académiques sponsorisés par *LOCKHEED MARTIN*[8] et alors désigné sous l'appellation de « *kill chain cyber* ». Si ces premiers travaux méritent aujourd'hui d'être approfondis, comprendre ce processus demeure essentiel pour appréhender les modes d'action des attaquants et proposer des parades.

Schématiquement, une attaque informatique comporte quatre phases successives. Elle suppose la mise au point de toute une gamme d'outils qui seront utilisés pour pénétrer le système cible, s'installer durablement sur ses réseaux et réaliser toutes les opérations techniques nécessaires. Elle s'appuie par ailleurs sur des infrastructures de pilotage et d'exploitation utilisant différents équipements informatiques compromis, achetés ou loués et qui constituent un véritable complexe informatique.

1.2.1. Les quatre phases d'une attaque

Le déroulement d'une attaque informatique est articulé en quatre phases susceptibles d'être répétées autant de fois que nécessaire pour atteindre l'objectif recherché.

La première étape est celle de la reconnaissance de la cible. Elle consiste en une prise d'empreinte qui permet de comprendre l'organisation des systèmes informatiques de la victime, d'identifier les technologies que celle-ci utilise pour mieux pénétrer son système. Ce travail préparatoire peut s'effectuer à partir de données disponibles en source ouverte, par exemple sur les réseaux sociaux tels que *LINKEDIN*. Les services de renseignement disposent de moyens plus intrusifs pour récupérer l'information utile, que ce soit par de l'espionnage humain ou par les techniques d'interception. Un autre moyen pour collecter ces informations utiles est de réaliser un « scan de ports ». Cette technique consiste à envoyer un message précis à une machine ciblée et à observer la réponse faite par cette machine. Cette réponse automatique peut en effet fournir à l'attaquant des indications précieuses sur sa configuration. Les attaquants peuvent réaliser eux-mêmes ces scans de port, mais également utiliser des bases de données de scans disponibles sur Internet. Si de telles bases de données sont légitimement utilisées par des sociétés vendant des objets connectés (qui peuvent être aussi variés que des caméras ou des réfrigérateurs connectés) pour avoir des informations sur l'utilisation de leurs produits, elles peuvent ainsi être détournées par des attaquants pour sélectionner des cibles.

Après la prise d'empreinte, l'attaquant va tenter de s'introduire dans le système cible. A cette fin, il va chercher à exploiter certaines vulnérabilités de ce système. Pour s'introduire dans un système informatique, un attaquant peut procéder de différentes façons. Il s'appuie souvent pour cela sur un utilisateur qu'il amène à lui fournir, par manque de vigilance, un accès au système d'information ciblé, par exemple en ouvrant une pièce jointe piégée, en cliquant sur un lien malveillant ou en connectant une clé USB infectée. Ces actions d'hameçonnage (*cf. glossaire*) peuvent se révéler particulièrement efficaces. Néanmoins, il existe d'autres techniques d'intrusion plus évoluées qui ne nécessitent aucune erreur de l'utilisateur et se

[8] "*Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*" par Eric M. HUTCHINS, Michael J. CLOPPERT et Rohan M. AMIN, de *LOCKHEED MARTIN Corp.*

font à son insu. C'est le cas par exemple des intrusions qui utilisent des mises à jour piégées de logiciels légitimes (cas de l'attaque *NotPetya*) ou des cas où l'attaquant est capable de modifier les communications électroniques échangées entre sa cible et Internet, par exemple en prenant le contrôle d'un routeur.

Les vulnérabilités CVE et les vulnérabilités « zero-day »

Les vulnérabilités CVE sont des fragilités mises en évidence dans des programmes informatiques pour lesquelles existent des moyens de détection voire de remédiation (*cf. glossaire*) développés par les éditeurs du produit. Elles sont identifiées par l'année de leur publication et un numéro d'identifiant unique et permettent au travers d'une base maintenue par l'association américaine *MITRE* [9] de connaitre le produit impacté, une description de la vulnérabilité et ses conséquences. Ce standard de fait permet par exemple de faire le lien entre une vulnérabilité et un correctif ou une mise à jour de sécurité.

Les vulnérabilités « zero-day », inconnues de l'éditeur du produit, sont en revanche redoutables car elles semblent imparables pour la victime. Elles font l'objet d'une lutte entre défenseurs et attaquants à qui les découvrira le premier. Afin d'empêcher leur exploitation malveillante, des primes sont fournies par exemple à l'occasion de « bug bounty », c'est-à-dire de compétitions organisées avec le soutien de l'éditeur, pour trouver ces vulnérabilités « zero-day » et récompenser financièrement leurs découvreurs. Les attaquants se livrent aussi à des recherches internes ou se fournissent auprès de plateformes plus ou moins licites qui servent d'intermédiaire. Cette « ubérisation » de la détection des failles de sécurité est un phénomène d'ampleur significative en raison des profits dégagés par la vente des « zero-day ». Ces derniers atteignent en effet aujourd'hui plusieurs centaines de milliers de dollars à en croire la plateforme spécialiste des failles critiques *ZERODIUM*[10]. La découverte des failles informatiques n'induit pas toujours, loin s'en faut, leur correction.

A partir du moment où elles sont connues, les vulnérabilités « zero-day » sont désignées comme des vulnérabilités « one-day » ou des CVE. Ces vulnérabilités connues sont souvent toujours présentes sur les systèmes après leur divulgation. La société *EDGESCAN*, dans son rapport de 2016, souligne que les vulnérabilités sur les systèmes sont corrigées en moyenne deux mois après leur divulgation, mais pas de façon systématique. Pour les systèmes anciens, certaines fragilités peuvent perdurer, surtout si le système n'est plus maintenu par l'éditeur.

[9] https://cve.mitre.org/

[10] Zerodium.com. Cette plateforme a été fondée par l'homme d'affaires français Chaouki BEKRAR.

Exfiltration de données par envoi d'un courriel piégé

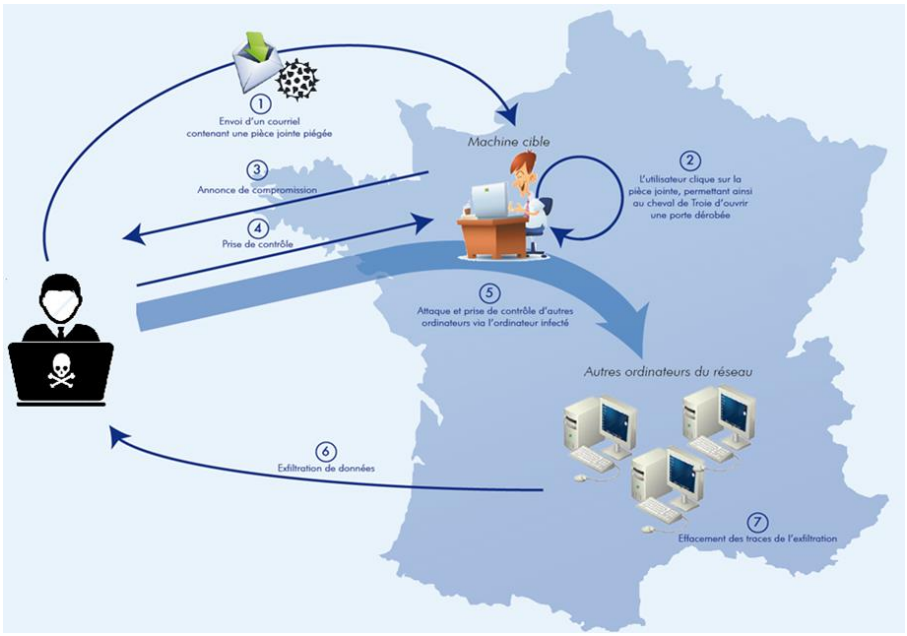


Figure n°2 : Exfiltration de données par envoi d'un courriel piégé

Une fois l'intrusion réalisée, l'attaquant va installer des implants (*cf. glossaire*) sur la machine compromise pour la piloter à distance. Il va établir dans ce but une ou plusieurs connexions à son infrastructure d'attaque. Il cherchera à être le plus discret et furtif possible, souvent en chiffrant ses communications et en les camouflant dans des flux légitimes afin de demeurer indétectable. Il pourra aussi prendre le contrôle de l'équipement compromis afin de maintenir ses accès malgré les redémarrages ou les mises à jour du système. A ce stade avancé de son attaque, l'intrus peut étendre encore son emprise sur le réseau et les bases de données de sa cible. Ce processus, qui correspond à la troisième phase d'une attaque, est souvent appelé latéralisation (*cf. glossaire*). Il va permettre à l'attaquant de maîtriser durablement le système infiltré et d'en prendre définitivement possession.

L'ultime phase d'une attaque consiste en l'exploitation du système compromis, c'est-à-dire au déclenchement des effets recherchés par l'attaquant. Elle peut durer quelques secondes dans le cas d'une exfiltration ponctuelle de données ou d'un sabotage informatique, ou à l'inverse se prolonger pendant plusieurs années pour des opérations de renseignement. Elle peut être plus ou moins automatisée. L'attaquant peut aussi pendant cette étape particulièrement sensible surveiller s'il n'est pas détecté et, en cas de doute, procéder à un effacement des parties les plus visibles de son intrusion pour revenir plus tard.

Il convient de noter que les attaques informatiques sophistiquées nécessitent une phase de préparation assez longue, souvent de plusieurs mois, pour déclencher des effets qui sont, eux, quasi instantanés. La phase d'intrusion nécessite du temps, à la fois pour comprendre l'architecture du système cible et pour en prendre le contrôle complet, y compris du réseau

de sauvegarde. L'offensive contre *TV5 Monde* en 2015 est un cas d'école. Elle s'est déroulée sur trois mois, de l'infiltration des réseaux au blocage des émissions, début avril 2015.

1.2.2. Les infrastructures de l'attaquant

La réalisation d'une attaque informatique suppose la détention de certaines capacités et infrastructures techniques :

- une « armurerie de logiciels » (détecteurs de failles, implants, canaux de communication et outils de pilotage) ;
- une infrastructure de commande-contrôle, regroupant l'ensemble des serveurs contrôlés par l'attaquant et utilisés pour piloter ses logiciels malveillants ;
- une infrastructure d'exploitation pour exfiltrer des données et les analyser.

Pour pouvoir être utilisés de manière cohérente au cours d'une attaque informatique, les différents logiciels malveillants utilisés doivent être intégrés, par exemple au sein d'un outil d'attaque spécifique dans un but précis.

Avec l'avènement du web à la fin des années 1990, des outils d'attaque utilisables par des non spécialistes, dits « script kiddies » (*cf. glossaire*), apparaissent. Ces outils, dont les ancêtres s'appellent *AOHell*, *Metasploit* ou bien encore *MPack*, sont principalement d'origine américaine, russe ou chinoise. Leur prolifération a favorisé la multiplication d'attaques cyber de bon niveau. Particulièrement bien conçus et modulaires, ils permettent d'intégrer très facilement de nouvelles fonctionnalités ou l'exploitation de nouvelles vulnérabilités. Des versions plus évoluées de ces outils sont depuis quelques années vendues sur le marché sous couvert de « test de sécurité » ce qui accroît leur niveau de performance et leur nocivité.

L'emploi de ces logiciels malveillants nécessite une infrastructure informatique permettant de les piloter de façon discrète : l'infrastructure de commande-contrôle de l'attaquant. L'attaquant peut par exemple s'appuyer sur « machines zombies » dont il a pris le contrôle ou compromettre des serveurs mal sécurisés pour les utiliser comme relais. Des réseaux d'anonymisation comme *Tor* peuvent quant à eux lui permettre de créer de façon discrète un lien logique entre ses équipements et ceux de ses cibles. En choisissant bien les localisations géographiques des relais qu'il utilise, l'attaquant peut s'assurer qu'il sera très difficile de remonter jusqu'à lui. Dans les cas les plus complexes, cette infrastructure peut être constituée de milliers d'équipements compromis qui peuvent être utilisées de manière alternative ou simultanée. L'infrastructure de l'attaque *Mirai*, qui a paralysé en 2016 plusieurs services Internet pendant quelques heures, s'est appuyée sur un réseau de plusieurs centaines de milliers de camera IP pour réaliser une attaque massive en déni de service.

En complément des capacités de commande-contrôle, l'attaquant peut recourir à une infrastructure d'exploitation différente pour exfiltrer et traiter des données, ou encore pour récupérer des rançons. Cette infrastructure doit être discrète et garantir les débits de transmission nécessaires au volume d'informations extrait. Les attaquants peuvent utiliser des moyens d'exploitation semblables à ceux mis en œuvre pour les infrastructures de commande-contrôle. D'autres solutions sont possibles. Ainsi, les cybercriminels utilisent

fréquemment des chaînes de conversion financières en diverses crypto-monnaies, ce qui rend la traçabilité des rançons quasi-impossible. Tous ces procédés, alternativement ou simultanément employés, rendent très difficiles les investigations sur les cyberattaques et plus problématique encore une attribution au vu des seuls éléments techniques disponibles.

1.2.3. Une structuration de la menace

Durant les années 1990, bon nombre de hackers ou groupes de hackers américains, allemands ou russes se firent connaitre par leurs exploits ou à l'occasion de leur arrestation. Néanmoins, cette forme d'activisme restait l'affaire de quelques spécialistes. A partir des années 2000, la vision quelque peu « romantique » du hacker solitaire va laisser place au constat d'une structuration planétaire de la menace autour de certains groupes d'attaquants qui vont à la fois se spécialiser et capitaliser sur leurs compétences, leurs outils et leurs modes opératoires. C'est ainsi qu'apparait, en 2010, la notion d'*Advanced Persistent Threat* (APT - *cf. glossaire*)[11] pour caractériser un ensemble d'outils et de techniques utilisés par un groupe structuré étatique ou privé.

L'implication des Etats transforme aussi en profondeur la nature de la menace cyber. Celle-ci est désormais incarnée par des organisations publiques et privées puissantes et structurées qui se sont substituées aux petits groupes d'experts des débuts. Certains pays, cherchant à anonymiser leurs actions dans le cyberespace, délèguent à des entités privées le soin de les mener. A titre d'exemple, de nombreux éditeurs d'antivirus relient aujourd'hui publiquement une vingtaine d'APT à la Chine :

- *APT1*, le premier groupe connu sous cette dénomination Depuis 2006, ce groupe est à l'origine de la compromission des systèmes informatiques de plus de 140 entreprises dans de nombreux secteurs industriels ayant pour but de dérober des données sensibles, qu'il s'agisse de brevets, de procédés de fabrication, de stratégies commerciales ou bien encore de contenus de contrats. Après avoir méthodiquement pénétré les réseaux informatiques de ces entreprises en y restant tapi parfois plusieurs années, ce groupe est parvenu à exfiltrer régulièrement des masses considérables d'informations. Pour y parvenir, *APT1* a utilisé un millier de serveurs en industrialisant à la fois les phases d'intrusion mais surtout les phases d'exploitation. Plusieurs centaines de personnes seraient employées pour maintenir cette infrastructure et pour guider les recherches de documents, leur traduction et leur exploitation.
- Les attaques sur *TV5 Monde* (*APT28*[12]) et *Notpetya* sont là encore une illustration de la structuration de groupes d'attaquants sous l'impulsion d'un Etat. le groupe *APT28*, qui sévit depuis 2008, aurait successivement attaqué des institutions en Géorgie, en Europe orientale, mais aussi l'OTAN ou des salons d'armement comme *EUROSATORY*. Orienté vers le vol de données dans un premier temps, *APT28* s'est ensuite spécialisé

[11] Appellation introduite par la société *MANDIANT*.

[12] Aussi connu sous le nom de *Fancy Bear* ou *Pawn Storm*.

dans l'influence grâce à la publication de données exfiltrées. Les Etats-Unis ont attribué au groupe *APT28* l'exfiltration de données du parti démocrate pendant les élections américaines de 2016. De même, l'Agence mondiale antidopage a relié à ce groupe le vol en 2016 des données relatives aux athlètes de haut-niveau qu'elle détenait.

Le groupe *Lazarus*, relié par de nombreux acteurs de la sécurité à la Corée du Nord, mène des opérations d'envergure depuis 2009. Après avoir ciblé des infrastructures en Corée du Sud, il s'est rendu célèbre par l'attaque des systèmes d'information de la société *SONY* où il a eu accès à des films non encore diffusés mais surtout aux données personnelles de l'ensemble des employés. Plus tard, cet APT semble s'être orienté vers les institutions financières, les casinos et les systèmes de crypto-monnaies afin de dérober un maximum d'argent. Le lien fait entre le rançongiciel *Wannacry* et ce groupe, notamment par le gouvernement anglais puis par les gouvernements américain, canadien et australien, ne fait que confirmer les nouvelles orientations de cet APT : récupérer des liquidités pour le compte du gouvernement nord-coréen. Difficile dans ces conditions de faire la part des choses entre cet APT, supposé gouvernemental et dont les motivations ne semblent que financières, et le groupe de cybercriminel dénommé *Carbanak* qui, entre 2013 et aujourd'hui, est soupçonné d'avoir dérobé pas moins d'un milliard de dollars en attaquant plus d'une centaine de banques dans plus de 30 pays.

Le tableau ci-dessous présente un historique non exhaustif des attaques attribuées à des APT. Pour sa part, la France a choisi de ne pas rendre publics les éléments dont elle dispose.

Nom	Type d'attaque	Effet de l'attaque	Cible	Période
Titan Rain	Espionnage	Extraction de nombreuses informations	Administrations et entreprises américaines et britanniques	2003 à 2006
Shady Rat	Espionnage	Extraction de données visant plus de 72 entités principalement aux Etats-Unis	Gouvernements ou associations	2006 à 2009
Comment Crew	Espionnage	Extraction d'informations sensibles de plus de 141 entreprises de haute technologie	Entreprises mondiales	2006 à 2013
Nuit de Bronze	Sabotage	DDOS sur de nombreux sites web gouvernementaux et industriels estoniens	Estonie	27 avril 2007
DarkHotel	Espionnage	Vol de mots de passe de clients d'hôtels de luxe en Asie	Hôtels de luxe en Asie	2007 à 2014
Opération Aurora	Espionnage	Pillage pendant deux ans d'informations sensibles	Entreprises américaines du web	2009 à mi 2010
Stuxnet	Sabotage	Dysfonctionnements et usure prématurée des centrifugeuses de l'usine iranienne d'enrichissement d'uranium de Natanz	Iran	23 juin 2009 au 13 mai 2010
Shamoon	Sabotage	Effacement de plus de 30 000 disques durs d'ordinateurs par un fichier contenant une image de drapeau américain en flamme	Compagnie nationale	15 août 2012 au 1er septembre 2012

Nom	Type d'attaque	Effet de l'attaque	Cible	Période
			saoudienne d'hydrocarbures (*SAUDI ARAMCO*)	
Yahoo	Cybercriminalité ou espionnage	Les attaquants, qui ont pénétré les systèmes de *YAHOO* une première fois en 2013 puis en 2014, ont dérobé les informations de 3 milliards d'utilisateurs. Deux premières mise en vente de ces données ont été détectées en août 2017 mais les motivations du ou des groupes ne sont pas clairement identifiés.	*YAHOO*	2013 et 2014
Carbanak	Cybercriminalité	En prenant le contrôle de nombreuses banques et institutions financières (plus d'une centaine), les attaquants ont réussi à dérober jusqu'à 1 milliard de dollars en réalisant frauduleusement des virements et des retraits d'espèces aux distributeurs	Banques	2013 à 2014
Sony Picture Entertainement	Déstabilisation	Vol de nombreuses données et divulgation de films non encore diffusés et de données confidentielles	*Sony Picture Entertainment*	Novembre 2014
TV5 Monde	Sabotage	Paralysie de l'ensemble des moyens de diffusion de la chaîne TV5 Monde pendant 2 jours.	TV5 Monde	8 au 9 avril 2015
Parti démocrate	Déstabilisation	Vol et divulgation de nombreux emails du parti démocrate (20 000 emails) et tentative de	Parti démocrate américain	Eté 2015 à juillet 2016

Nom	Type d'attaque	Effet de l'attaque	Cible	Période
		déstabilisation de la candidate démocrate aux élections présidentielles américaines de 2016		
Banque du Bangladesh	Cybercriminalité	Vol, par le biais de virements frauduleux, de 81 millions de dollars.	Banque du Bangladesh	Février 2016
Dyn	Sabotage	L'attaque par le biais d'un DDOS a bloqué les services de la société *DYN* rendant l'internet indisponible pendant quelques heures.	Internet	21 octobre 2016
WannaCry	Cybercriminalité	Chiffrement de plus de 300 000 ordinateurs et demande de rançons pour restauration des données	Non ciblé	12 au 15 mai 2017
NotPetya	Sabotage	Destruction de nombreux systèmes informatiques utilisant le logiciel de comptabilité ukrainien *ME.DOC*	Ukraine	27 juin 2017

Figure n°3 : Historique d'attaques attribuées à des APT

1.3. Des systèmes toujours plus vulnérables

L'accroissement du niveau général de la menace n'est que faiblement compensé aujourd'hui par l'amélioration du niveau de sécurité des systèmes. Face à l'explosion du nombre d'attaques, la prise de conscience du risque informatique reste aujourd'hui très insuffisante. Dans un contexte marqué par la numérisation massive des données et l'inter-connectivité croissante des réseaux, la sécurisation des systèmes informatiques devient un impératif et un enjeu crucial pour nos sociétés, dorénavant exposées à de véritables risques systémiques.

1.3.1. Un état de sécurité insuffisant

Les premiers logiciels malveillants suivent de près la création en 1969 de l'Arpanet (réseau militaire américain ancêtre de l'Internet). Le logiciel *Creeper*, dès 1971, est ainsi le premier programme à se répliquer de serveur en serveur avec pour intention plus malicieuse que malveillante l'affichage sur l'écran d'un message parasite « *I'm the creeper, catch me if you can* ».

Durant les années 1980, le développement de l'informatique domestique, avec les ordinateurs *Apple II* et les premiers PC sous MS-DOS, favorisa la multiplication de logiciels malveillants, qui ne représentaient cependant pas encore un véritable danger. Les dégâts causés étaient limités et souvent non intentionnels, comme le déni de service causé par le ver (*cf. glossaire*) *Morris*, du nom de son inventeur qui fut aussi le premier condamné en vertu de la loi américaine « *Computer Fraud and Abuse Act* » adoptée par le Congrès en 1986[13]. C'est aussi à la fin des années 1980 que les premiers antivirus firent leur apparition. Les entreprises qui les développaient alors - *McAfee*, *Symantec*, *Trendmicro* et *Kaspersky* - sont toujours aujourd'hui les leaders du domaine (*cf. annexe 6*).

C'est au tournant des années 1990 et 2000, avec l'essor du web, qu'apparurent des logiciels vraiment toxiques tels que le vers *Iloveyou* créé par deux étudiants philippins ou le malware *Klez* qui infecta des ordinateurs par millions en se propageant via la messagerie de leurs victimes. Face à ces attaques de grande ampleur, l'administration Clinton prit une série de mesures pour renforcer la sécurité informatique de l'administration américaine et lança un plan de 1,5 milliards de dollars pour mieux assurer la sécurité des agences fédérales. En parallèle, la première sonde de détection *Snort* était proposée en projet « open-source » par Martin Roesch. Ce dernier fonda ensuite, sur la base de ce projet, la société *Sourcefire*, qui devint la première entreprise mondiale du domaine avant d'être rachetée par *Cisco* en 2013.

On assiste depuis à une course poursuite entre l'invention de malwares et d'antivirus, entre le déploiement d'attaques de plus en plus sophistiquées et le durcissement des protections des systèmes informatiques. Souvent en retard par rapport aux avancées des attaquants, les parades et les défenses informatiques demeurent trop faibles. Rares sont en effet les

[13] En France, la loi Godfrain du 5 janvier 1988 a été la première loi relative à la fraude informatique et aux intrusions informatiques (Loi n°88-19). Cette loi a notamment introduit la notion de système de traitement automatisé de données (STAD).

entreprises ou les administrations qui disposent aujourd'hui de systèmes d'information robustes et sécurisés « à l'état de l'art ». A cela, trois raisons principales. : le niveau de protection initial souvent insuffisant des équipements et logiciels informatiques proposés à la vente, l'absence de mise à jour de sécurité pour les produits anciens et, enfin, la prise en compte insuffisante par les entreprises de la cybersécurité comme composante stratégique de leur transformation numérique.

1.3.2. Les risques associés à la transformation numérique

L'informatisation des systèmes n'est pas un phénomène récent. Les premiers automates programmables industriels sont apparus dès la fin des années 1970 pour répondre aux besoins des constructeurs automobiles de moderniser et d'automatiser leurs chaînes de production. Ces équipements permettaient de faire le lien entre le monde numérique et le monde analogique. C'est pourquoi ils se sont imposés dans l'ensemble des chaînes de production, dans les bâtiments modernes pour gérer par exemple les systèmes de climatisation, ou à bord des aéronefs et des navires dans les fonctions propulsion ou navigation. Le déploiement en masse de dispositifs informatiques embarqués est intervenu à partir de 1980, lorsque *GENERAL MOTORS* fut le premier constructeur automobile à utiliser un processeur à 50 000 lignes de code pour améliorer le fonctionnement de ses moteurs. Il fut rapidement imité par ses concurrents et, aujourd'hui, on dénombre communément sur les véhicules automobiles entre 20 et 100 processeurs exécutant plusieurs millions de lignes de code.

Devenus omniprésents dans tous les systèmes, les produits informatiques n'échappent pas aux lois du marché. Or, celles-ci tendent à substituer, dans une logique de maîtrise des coûts, aux produits spécifiques des produits plus polyvalents dont la personnalisation est aisée mais qui comportent, *sui generis*, de nombreuses fonctions superflues. Il n'est, dès lors, pas surprenant de trouver dans des automates industriels utilisés dans un environnement pourtant totalement isolé, des services tels qu'un serveur « web », simplement parce que le composant générique utilisé comprenait cette fonctionnalité. Cette tendance se traduit aussi par une convergence technologique qui tend à placer dans des systèmes, pourtant très différents, les mêmes composants informatiques. Il résulte de ce genre de situation une vulnérabilité accrue des systèmes car d'éventuels attaquants peuvent avoir facilement accès sur le marché aux composants informatiques en question pour préparer leurs méfaits.

L'autre évolution notable de nos systèmes est l'interconnexion croissante dont ils font l'objet. A l'image de ce que l'on peut observer avec l'installation de compteurs électriques intelligents, de nombreux systèmes présents dans la vie courante sont désormais interconnectés via internet ou des connections spécifiques afin de faciliter et de réduire le coût de leur exploitation et permettre de nouveaux services. Le fonctionnement de certains systèmes est même parfois dépendant de leur bonne connexion avec un serveur extérieur. Dès lors, interrompre celle-ci suffit à rendre inopéraont le système. Leur interconnexion est

une source de vulnérabilité nouvelle[14] qui offre à un éventuel attaquant deux opportunités à exploiter :

- elle offre une infrastructure, ou « botnet »[15] (*cf. glossaire*), permettant de conduire des attaques massives comme celle opérée par le malware *Mirai* qui, en prenant le contrôle d'un ensemble de caméras vidéo connectées sur Internet, a réalisé un déni de service massif sur une partie du *web* ;
- elle expose les systèmes à un risque d'attaque informatique via leur connexion à un réseau extérieur. Ainsi, des chercheurs américains ont réussi en 2015 à prendre le contrôle d'un véhicule à partir d'un smartphone et la CIA a pu espionner des cibles à l'aide de caméras et de micros incorporés dans des téléviseurs.

Si elle permet d'envisager une amélioration des conditions de vie des populations et une meilleure gestion des ressources, la perspective de la mise en place de villes et de territoires intelligents dans lesquels se superposeront et seront interconnectées les grilles énergétiques, de communications électroniques, de transport, de gestion de l'eau et des déchets accroîtra sensiblement les possibilités offertes aux attaquants. A cet égard, le choix ambitieux de faire de la capitale française une ville numérique en 2024 à l'occasion des Jeux olympiques doit s'accompagner d'une réflexion de fond sur la sécurité des systèmes d'information qui soutiendront la transition numérique parisienne et la gestion de l'événement. Substrat de ces futurs déploiements, les *clouds* qui permettront le recueil des données de ces villes connectées constitueront des cibles potentielles, tout comme les algorithmes qui traiteront ces données.

Le nombre des objets connectés sera de plusieurs dizaines de milliards à l'horizon 2020 (les estimations sur ce nombre varient de 26 à 212 milliards[16]). Ces objets faciliteront la vie courante tout en apportant de nouvelles fonctionnalités à des coûts réduits. « L'internet des objets » qu'ils constitueront pourra cependant être la cible d'attaques informatiques avec des conséquences allant jusqu'à la perte de vies humaines lorsque, par exemple, des objets connectés utilisés dans le domaine de la santé seront visés. Ce risque est aggravé par le fait que de nombreux fabricants ne sécurisent pas leurs objets connectés afin d'en réduire le coût de développement et d'en accélérer la commercialisation. Si la dynamique de développement actuelle se maintient, des « botnets » d'objets connectés viendront ainsi compléter en masse les « botnets » traditionnels d'ordinateurs déjà existants, fragilisant un peu plus le niveau de sécurité dans l'espace numérique.

Une prise de conscience de ces dangers apparait nécessaire. Elle devra ensuite rapidement conduire à la mise en place d'une véritable stratégie de développement d'objets connectés

[14] Pour cette raison, un travail solide de sécurisation des compteurs électriques ENEDIS a par exemple été réalisé en lien étroit avec l'ANSSI.

[15] Réseaux de robots compromis qui sont à la main d'un groupe d'attaquants pour conduire ses attaques.

[16] Source : « Cyberattaques. Prévention-réactions : rôle des États et des acteurs privés », Karine BANNELIER, Théodore CHRISTAKIS, in *Les Cahiers de la revue Défense nationale,* avril 2017.

présentant un niveau minimal de sécurité. A défaut, la confiance des utilisateurs se dégraderait et l'avenir du numérique deviendrait plus incertain. La revue stratégique de cyberdéfense présente plusieurs pistes en ce sens dans sa troisième partie.

1.3.3. L'existence d'un risque systémique

En dehors des attaques traditionnelles sur les cartes bancaires, les premières attaques informatiques d'envergure sur le système financier ont été réalisées en détournant le système *Swift*[17]. Ce système, qui permet les échanges entre établissements bancaires en garantissant l'authenticité des transactions et en les archivant, est un des piliers nécessaires au bon fonctionnement du système financier international. Les attaques menées par les APT *Lazarus Group* ou *Carbanak* leur ont permis de dérober jusqu'à un milliard de dollars, peuvent sembler dérisoire si l'on compare leurs gains au montant des transactions journalières réalisées par *SWIFT* (chaque jour, plus de 8 millions de transactions représentant des milliers de milliards de dollars). Pour leurs auteurs, elles se sont néanmoins révélées très lucratives et elles pourraient donner des idées à d'autres groupes criminels, voire à des pays, qui pourraient par ce moyen récupérer des financements pour mener des activités clandestines ou même faire disparaître une partie des avoirs financiers de leurs adversaires ou opposants.. Dans ce contexte, la confiance accordée au système actuel de transactions financières par les acteurs du marché pourrait se trouver significativement dégradée et le risque d'un effondrement d'ensemble du système ne peut être écarté.

Les attaques via les chaines d'approvisionnement, comme dans le cas du logiciel malveillant *NotPetya* en 2017, relèvent d'autres scenarii qui peuvent aussi produire des effets en cascade échappant à tout contrôle. Ces attaques se révèlent très efficaces puisque le piège arrive chez la cible par la chaîne d'approvisionnement usuelle ou par les mises à jour légitimes des systèmes, ce qui ne suscite pas la méfiance de celle-ci. S'il est efficace, ce piégeage de masse présente toutefois deux risques majeurs :

- celui de produire des dégâts collatéraux qui peuvent eux-mêmes engendrer une riposte et une escalade non maîtrisée en raison d'un ciblage initial imprécis ;
- celui de voir un autre groupe d'attaquants découvrir les vulnérabilités introduites et de les détourner pour son propre usage, le cas échéant à l'encontre de l'instigateur du dispositif[18].

Atteinte grave à la crédibilité du système financier international, incapacité des attaquants à circonscrire dans le temps et dans l'espace les dommages collatéraux de leurs attaques, constituent les ferments d'un risque systémique majeur pour le fonctionnement de l'économie et de la société.

---

[17] *SWIFT* est administré par la société du même nom : *Society for Worldwide Interbank Financial Telecommunication.*

[18] C'est ainsi qu'en 2005, à la suite de la vente de la branche « ordinateur personnel » d'*IBM* à la société chinoise *LENOVO*, plusieurs services de renseignement anglo-saxons ont décidé d'interdire l'utilisation des ordinateurs de cette marque au sein de leur organisation craignant leur piégeage par l'Etat chinois.

1.3.4. L'accroissement de la menace d'origine cyber

Les États sont aujourd'hui confrontés à une évolution de la menace d'origine cyber s'articulant autour de trois facteurs :

- la dangerosité de la menace, sous l'effet de la multiplication des acteurs, de l'accroissement des capacités offensives de certaines puissances étrangères, de la prolifération des armes informatiques et de la banalisation des techniques d'attaque ;
- l'imbrication des enjeux de cybercriminalité et de sécurité nationale. Les outils traditionnellement utilisés à des fins de fraude et d'extorsion de fonds, tels que les rançongiciels, peuvent causer des dommages aux systèmes d'information de l'Etat et des opérateurs en charge d'infrastructures critiques, paralysant ainsi la continuité de leurs activités. C'est ce qui a été notamment observé avec les effets de l'attaque *WannaCry* sur le système de santé britannique ;
- une exposition accrue de notre société à la menace du fait d'une numérisation plus étendue de celle-ci et une utilisation à grande échelle d'objets connectés (*cf. 1.3.2*).

S'ajoutant aux innombrables opérations d'espionnage informatique très régulièrement détectées et aux risques bien documentés de pillage des données ou de déni d'accès, des actes de blocage ou de sabotage des systèmes informatiques (pouvant aussi relever de la cybercriminalité), sont de plus en plus souvent constatés. Il est probable qu'une attaque informatique de cette nature aura, un jour, des conséquences létales.

Nos sociétés démocratiques sont par ailleurs de plus en plus souvent confrontées aux mésusages d'Internet et des réseaux sociaux à des fins de manipulation de l'opinion et de déstabilisation institutionnelle.

De plus en plus d'attaques combinant différents modes d'action et semblant poursuivre plusieurs finalités, révèlent un travail de planification et d'infiltration en amont mené par des acteurs ayant des capacités avancées.

Nous sommes en outre collectivement confrontés à l'essor d'une sorte de *Golem* informatique, qui, à partir de la manipulation de vecteurs dévoyés (ordinateurs zombies, objets connectés compromis…), est susceptible de déclencher des phénomènes imprévisibles de grande ampleur, allant par exemple de la divulgation d'une quantité considérable de données au *blackout* électrique d'une ville.

Face à l'évolution de la menace, il est nécessaire que notre pays consolide et mette en cohérence ses objectifs et ses capacités de cyberdéfense.

Vers un « Far-West » cybernétique ?

Peu de travaux de prospective existent dans le domaine cyber, qu'ils concernent les évolutions technologiques futures ou les doctrines d'emploi. Les évolutions imaginées à l'heure actuelle sont souvent liées à l'apparition à moyen terme de l'ordinateur quantique,

qui pourrait donner aux Etats en leur possession une supériorité significative dans le domaine de la sécurité en leur permettant de « casser » les algorithmes de cryptographie actuels. Il est cependant difficile de donner une date, même approximative, de l'entrée en service de tels ordinateurs, qui suppose l'avènement d'une véritable révolution technologique, probable mais à ce jour encore incertaine. Les premiers exemplaires de ces machines existant aujourd'hui sont encore sans commune mesure avec ce qui serait nécessaire pour apporter une suprématie véritable.

Il est certain en revanche que la menace va s'aggraver dans la prochaine décennie avec pour conséquence un espace cyber plus dangereux et moins stable, où les attaques informatiques seront monnaies courantes forçant les institutions publiques, les entreprises et les individus à se protéger plus fortement qu'aujourd'hui. Ce scénario, est décrit par le « Center for Long-Term cybersecurity » de l'université de Berkeley sous le nom de « la nouvelle normalité ». Dans ce contexte, nous pouvons faire le choix d'une plus grande maîtrise des risques, grâce à une cyberdéfense renforcée et une hygiène plus robuste de cybersécurité dans notre société, ou au contraire de nous laisser dériver vers une sorte de « Far-West » cybernétique.

Cet avenir est moins conditionné dans l'immédiat par la technologie cyber que par le développement de nouvelles applications d'autodéfense durcies et prenant en compte plus efficacement les enjeux de sécurité. A cet égard, le niveau de protection et de contrôle de l'Internet des objets et de l'intelligence artificielle[19] apparait un élément d'ores et déjà déterminant pour la sécurité de notre société.

1.4. Comment résister aux attaques ?

Sous le double effet d'un accroissement de la menace d'origine cyber et d'une vulnérabilité accrue de nos systèmes d'information, les voies et moyens d'assurer notre cyberdéfense constituent désormais des enjeux essentiels pour notre société.

Après avoir posé les principaux enjeux en termes de gouvernance et d'analyse des risques (1.4.1.), la présente revue souligne la nécessité de prendre en compte la sécurité tout au long du cycle de vie des systèmes (1.4.2.) et de bien connaître les technologies disponibles pour faire face à la menace (1.4.3.), puis évoque ensuite les techniques de défense active (1.4.4.).

1.4.1. Intégrer à bon niveau les enjeux de cybersécurité dans les organisations

Avec plusieurs années de recul, il apparait que la prise en compte des menaces cyber et la mise en œuvre des contre-mesures adaptées au sein d'une entité publique ou privée ne sont véritablement efficaces que si elles relèvent du plus haut niveau de responsabilité. Ainsi, le niveau de risque portant sur les systèmes d'information, compte tenu des mesures de protection mises en place, doit à tout moment être connu et accepté par la direction de l'entité. Pour l'assister dans ce suivi, celle-ci peut nommer un responsable de la sécurité des

[19] Une mission sur l'intelligence artificielle a été confiée au député Cédric VILLANI (*cf. Partie 3*).

systèmes d'information, éventuellement assisté d'un ensemble de personnels constituant une chaîne fonctionnelle SSI. En vertu du principe de séparation des rôles, il est primordial que cette chaîne fonctionnelle ne soit pas soumise à l'autorité hiérarchique de la direction des systèmes d'information de l'entité. Par ailleurs, son rôle dans le suivi du niveau de sécurité du système d'information et la préparation des décisions afférentes ne doit en aucun cas conduire à déresponsabiliser l'échelon de direction de l'entité.

Pour conduire leur transformation numérique, les entreprises ou les services de l'Etat mettent en place une organisation spécifique avec un responsable chargé de conduire ces évolutions. Ces directeurs du numérique ou « chief digital officer » sont souvent intégrés au comité de direction et s'appuient sur les traditionnelles directions informatiques pour mener à la fois l'évolution des systèmes numériques dans l'entreprise, la digitalisation des différents processus métier, l'acculturation des personnels à cette digitalisation mais aussi pour transformer les « Business modèles » de leur entité en profitant pleinement des opportunités offertes par le numérique. Aussi, lorsque de tels responsables existent au sein d'une structure, il est indispensable de leur confier aussi la responsabilité de la cybersécurité de leur projet et surtout l'analyse des risques associés. L'intégration dès les phases de réflexion et à haut niveau d'éléments de cybersécurité permet en effet d'évaluer *ab initio* les risques des différentes options de la transition numérique et d'en améliorer considérablement la sécurité, souvent pour un surcoût négligeable.

1.4.2. Prendre en compte la sécurité tout au long du cycle de vie des systèmes d'information

Face à des attaques de plus en plus avancées et évolutives, le concept prévalant pendant de nombreuses années d'une défense fondée uniquement sur des mesures de prévention périmétriques a démontré ses limites. Ainsi, quelle que soit la qualité des mesures préventives mises en œuvre - qui gardent au demeurant toute leur pertinence -, il est désormais irréaliste de considérer qu'un système d'information demeurera rigoureusement étanche aux attaques. Il convient de prendre au contraire pour axiome le fait qu'un attaquant motivé finira toujours par prendre pied au sein du système d'information. Une défense adaptée se doit par conséquent d'être étendue à l'ensemble du système d'information à protéger, dans une logique de défense en profondeur, et d'incorporer un volet consacré à la détection des attaques et à la réaction à celles-ci.

Plus fondamentalement, la prise en compte de la sécurité doit être effective à toutes les étapes du cycle de vie d'un système d'information, qui peut être schématiquement décrit selon quatre phases (*cf.* annexe 8) : phase de conception et de développement ; phase de recette et de vérification de la sécurité du système ; phase de vie opérationnelle du système avec, sur le plan de la sécurité, un double enjeu de maintien en condition de sécurité et de supervision en vue de détecter les attaques ; phase de réaction aux éventuelles attaques.

L'absence de prise en compte des enjeux de sécurité dans une de ces étapes obère fortement la capacité à garantir la sécurité du système tout au long de sa vie. Ainsi, il est illusoire de

prétendre atteindre un bon niveau de protection par un simple audit et la correction des vulnérabilités identifiées à cette occasion, si les bons choix techniques et organisationnels n'ont pas été adoptés dès la conception du système. De même, l'absence de supervision de sécurité d'un système, quel que soit son niveau de sécurité initial, ne peut que déboucher à terme sur une illusion de sécurité.

Chaque phase du cycle de vie du système fait appel à des compétences spécifiques, tant techniques que méthodologiques, et est associée à un certain nombre de bonnes pratiques. L'élaboration de ces bonnes pratiques nécessite par ailleurs, à chaque étape, une connaissance régulièrement actualisée des technologies disponibles et de l'état de la menace.

Enfin, l'enchaînement de ces différentes phases doit être considéré comme un cycle plutôt que comme un déroulement linéaire, dans la mesure où la réaction à une attaque identifiée doit naturellement entraîner une revue de la conception du système et une amélioration itérative de sa sécurité. Cet enchaînement cyclique des étapes du cycle de vie se justifie à plus forte raison dans le cas d'un développement structuré selon les méthodes dites « agiles », qui voient se succéder de nombreux cycles de développement et les étapes de sécurisation afférentes, y compris en l'absence d'attaques identifiées.

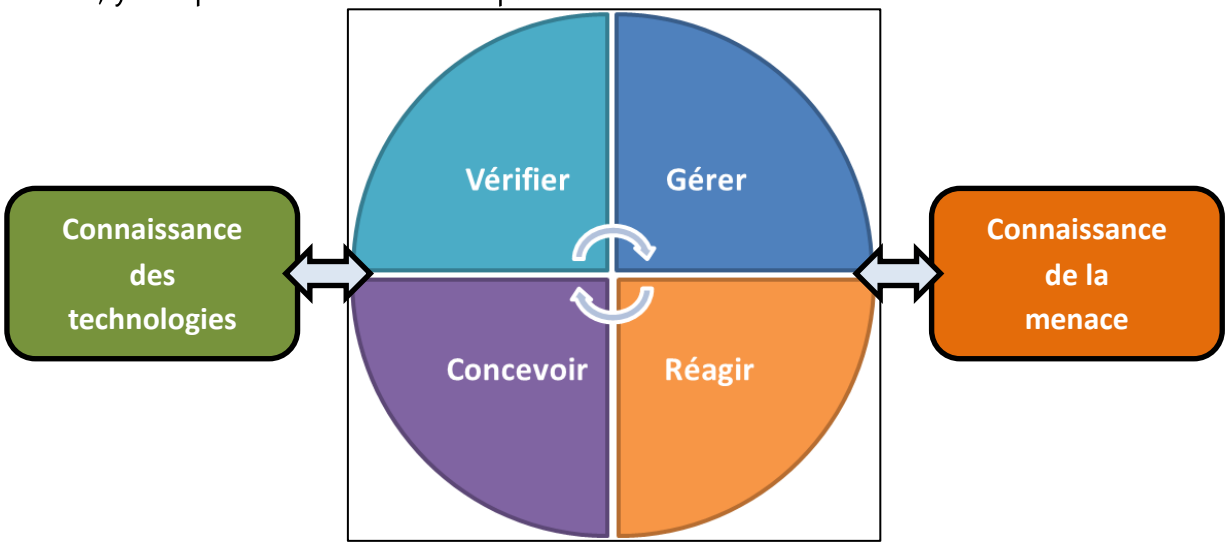


Figure n°4 : Cycle de vie de la sécurité d'un système d'information

1.4.3. Connaître les technologies et la menace

Une démarche de sécurité ne peut être efficace qu'à la condition d'être alimentée, à toutes ses phases, par une connaissance régulièrement actualisée des technologies et de la menace. L'entretien d'une telle connaissance nécessite un investissement conséquent, qui n'est pas justifié pour la majorité des entités déployant des systèmes d'information sécurisés. Ces connaissances devront donc dans la majorité des cas être recherchées auprès des administrations spécialisées, ou de prestataires de service en cybersécurité.

Sur le plan technique, l'intégration cumulative des retours d'expérience issus de la conception et de la mise en œuvre de systèmes d'information sécurisés doit en premier lieu

être réalisée. Il s'agit ensuite de posséder une connaissance approfondie des technologies disponibles et d'en comprendre les mécanismes de sécurisation, leurs apports, leurs limites et leurs vulnérabilités. Une veille active, portant aussi bien sur les nouvelles solutions mises sur le marché que sur les vulnérabilités identifiées dans les solutions existantes doit être conduite et, le cas échéant, être complétée par des actions de maquettage et de test. L'identification précoce des principales ruptures technologiques ou changements des usages doit aussi être recherchée dans une logique d'anticipation, ce qui nécessite une relation étroite avec le champ de la recherche académique.

La connaissance des menaces doit, quant à elle, intégrer une identification précise et actualisée des outils mis en œuvre par les attaquants afin d'en déduire, notamment grâce à la rétro-conception d'échantillons de codes malveillants, des marqueurs caractéristiques susceptibles d'alimenter les solutions de détection d'attaques. Elle a également pour objectif la description des principaux modes opératoires adverses, avec un double enjeu d'identification des cibles privilégiées de ces modes opératoires, et de compréhension pour chacun d'entre eux des procédés et techniques mis en œuvre à chaque étape d'une cyberattaque, depuis la phase de reconnaissance jusqu'à celle d'exploitation. La connaissance de la menace est alimentée par une capacité de veille et d'analyse d'informations disponibles en sources ouvertes, par les informations issues des moyens de supervision et de détection mis en œuvre au sein des différents systèmes d'information protégés, et par le fruit des analyses conduites en réaction aux attaques. Ces éléments peuvent être utilement complétés par des signalements et analyses comparables mis à disposition par des organismes tiers. Le développement durable de la connaissance requiert une capacité à capitaliser avec soin un vaste ensemble d'informations, dont le cycle de vie et les règles de partage avec des tiers doivent être gérés avec attention.

1.4.4. Envisager une défense active maitrisée

Pour compléter les dispositifs actuels de cybersécurité, de nouvelles techniques plus actives et agressives commencent à être mises en place de manière de plus en plus systématiques. Entre une défense purement passive et des mesures résolument offensives, on les regroupe dans la catégorie des mesures de défense active.

Les techniques dites de « pots de miel » ou « honey pots » visent ainsi à attirer les attaquants sur des cibles factices pour qu'ils dévoilent leurs outils, ce qui permettra ensuite de les repérer plus facilement. Cette technique très utilisée par les chercheurs leur permet d'observer une grande palette de logiciels malveillants.

Une autre technique, dite de « sinkholing » (*cf. glossaire*), consiste à observer les agissements d'un attaquant en détournant vers un serveur maîtrisé les flux remontant vers son infrastructure de commande-contrôle. Ce type d'opérations, souvent réalisées par les éditeurs d'antivirus, leur permet d'observer l'attaquant pendant plusieurs années et de comprendre les cibles visées et les objectifs poursuivis. Toutefois, pendant le temps de l'observation, l'attaquant poursuit ses méfaits, ce qui interroge sur l'attitude de l'industriel qui a

connaissance d'une infraction et décide seul de la laisser se dérouler pour obtenir une connaissance sur des attaquants qu'il valorisera à son profit ensuite.

Pour faire cesser une attaque, les victimes peuvent aussi être tentées de détruire l'infrastructure de l'attaquant en supprimant les serveurs qu'il utilise pour son infrastructure de commande-contrôle. Ces actions peuvent se faire par des moyens judiciaires en faisant « saisir » les moyens incriminés. Cette démarche entreprise par *MICROSOFT* avec le soutien du FBI leur a permis depuis quelques années de supprimer de nombreux « *botnet* » de plusieurs centaines de milliers de machines. Mais d'autres techniques sans base légale sont également utilisées pour rendre inopérant l'infrastructure d'un attaquant.

La victime peut aussi être tentée de contre-attaquer en utilisant les mêmes techniques que son agresseur. Cette pratique en contradiction avec le droit national et international, appelée « hack back », peut être utilisée pour récupérer les données subtilisées, détruire le système des attaquants, voire dérober les moyens dont ils disposent. Ce mode d'action, qui semble avoir déjà été mis en œuvre dans quelques cas, mène à une escalade inévitable, des dégâts collatéraux étant plus que probables et l'attaquant pouvant lui-même vouloir répliquer à nouveau.

Toutes ces techniques soulèvent le besoin de clarifier le droit international dans ce domaine pour éviter des situations inextricables ou une escalade incontrôlée.

1.5. Une régulation internationale encore trop balbutiante

Le tableau présenté précédemment d'une menace toujours plus structurée et de systèmes rendus plus vulnérables par la numérisation et leur inter-connectivité croissante s'inscrit dans un contexte international où aucun accord multilatéral n'a encore pu être trouvé pour établir une architecture et des règles de sécurité communes régissant les relations entre Etats et entre acteurs privés et publics à l'ère numérique.

1.5.1. Les négociations internationales sur la régulation du cyberespace à un tournant

Le cyberespace n'est pas totalement dépourvu de normes et de règles, dans la mesure où celles du droit international ou les grands principes qui régissent les relations entre Etats s'y appliquent. Ainsi, les négociations, sous l'égide des Nations-Unies, du « groupe des experts gouvernementaux sur la cybersécurité » (GGE), organisées dans des formats différents à cinq reprises entre 2004 et 2017, ont permis de reconnaitre, dès 2013, l'applicabilité du droit international, et notamment de la Charte des Nations-Unis, au cyberespace, puis de consolider, en 2015, un socle d'engagements volontaires de bonne conduite pour les Etats dans ce domaine. Ces « normes de comportement responsable » s'articulent autour de plusieurs grands principes ou objectifs. Afin de faciliter la coopération et réduire les risques d'incompréhensions, il est ainsi recommandé aux Etats de faire preuve de transparence sur leur organisation et leur posture nationale en matière de cybersécurité et d'adopter un

comportement coopératif vis-à-vis des pays victimes d'attaques émanant de leur propre territoire, en particulier lorsque l'attaque vise une infrastructure critique. Afin de renforcer la résilience globale de l'espace numérique, chaque Etat est également encouragé à renforcer sur le plan national sa propre cybersécurité, et notamment celle de ses systèmes les plus sensibles, comme ceux des infrastructures critiques. Un autre objectif est de lutter contre la prolifération des outils informatiques malveillants et de préserver l'intégrité de la chaîne d'approvisionnement numérique. On peut également rappeler qu'il est apparu important pour les Etats participant à ces négociations de s'engager, hors contexte d'opérations militaires, à ne pas endommager des infrastructures critiques d'un autre Etat ou à détériorer leur capacité à fournir leur service au public.

A l'occasion du dernier cycle de négociations du GGE 2016-2017, la France a fait des propositions à ses partenaires pour approfondir ce travail et préciser l'ensemble de ces normes, notamment sur l'interdiction des pratiques de *hack back* (contre-attaque cyber - *cf. glossaire*) par des acteurs privés ou encore l'imposition d'un contrôle des exportations pour les outils cyber malveillants. Ces propositions ont dans l'ensemble fait l'objet d'un consensus, mais les négociations ont échoué sur la question - dé-corrélée - des modalités d'application du droit international à la conduite des Etats dans le cyberespace.

Cet échec des négociations au sein du GGE de l'ONU est le signe d'une divergence fondamentale de perception, parmi les différents pays, de l'architecture internationale de sécurité devant régir les relations entre Etats à l'ère numérique. A court et moyen terme, cette incompatibilité signe l'arrêt des négociations à l'ONU sur le comportement responsable des Etats dans le cyberespace.

L'échec de ce dernier cycle de négociations ne remet nullement en cause les normes et principes agréés au cours des années précédentes. De plus, il ne doit pas mettre un terme aux efforts de la France et de la communauté internationale en vue de promouvoir des normes de comportement et mesures de confiance en faveur de la stabilité et de la sécurité internationale du cyberespace

Au-delà des seules relations entre Etats, un important effort de régulation reste notamment à mener autour des activités du secteur privé. L'irruption du numérique comme nouvel outil et espace de confrontation confère en effet à ce secteur, et particulièrement à certains acteurs systémiques, un rôle et des responsabilités inédites dans la préservation de la paix et de la sécurité internationale.

Sur ces différents sujets, les Etats ne seront pas en mesure de créer et d'imposer seuls des règles à tous les acteurs du cyberespace. Ces dernières années, plusieurs initiatives visant à promouvoir certaines visions de la régulation internationale du cyberespace, selon une approche holistique intégrant des acteurs du secteur privé et de la société civile ont d'ailleurs vu le jour.

Lancée en février 2017 par le ministre des affaires étrangères des Pays-Bas, la Commission globale sur la stabilité du cyberespace (*Global Commission on the stability of cyberspace*) a pour

objectif de développer des propositions originales en matière de normes internationales, dans le but d'encourager un comportement responsable des acteurs étatiques et non-étatiques dans le cyberespace. La Commission est composée de vingt-six commissaires (dont une commissaire française) représentant une large variété de régions géographiques et de parties prenantes (gouvernements, industrie, communauté technique, société civile) et choisis en fonction de leur légitimité à s'exprimer sur les différents aspects du cyberespace. Lors de la Conférence globale sur le cyberespace tenue à New Delhi en novembre 2017, cette Commission a appelé Etats et acteurs non-étatiques à s'engager à protéger le « cœur public de l'Internet ».

Par ailleurs, des entreprises privées entendent aussi peser dans ces débats. *MICROSOFT* a ainsi, dès 2014, proposé aux Etats un ensemble de normes de comportement relatives aux différents aspects de la sécurité internationale du cyberespace (lutte contre la prolifération, gestion responsable des vulnérabilités, assistance en cas de crise) avant de proposer en 2016 que ces normes soient reprises dans une « Convention de Genève du numérique ». *MICROSOFT* est également à l'origine d'un ensemble de règles de comportement à destination du secteur privé (le *TechAccord*).

1.5.2. Des fondements théoriques en construction

Dans ce monde « post-GGE » dans lequel nous vivons désormais, où la paix et la sécurité internationales de la société numérique sont encore en construction, et les rôles respectifs que doivent y jouer les Etats et les acteurs privés encore à définir, les fondements théoriques de la cyberdéfense sont encore, au sein des pays comme au sein de différentes organisations internationales, en discussion. Plusieurs grandes tendances se dégagent cependant.

La classification des menaces et de la gravité des attaques informatiques apparaît, tout d'abord, comme une nécessité partagée. Les Etats-Unis ont élaboré une grille d'appréhension des cyberattaques qui, si elle ne peut être transposée sans adaptation à l'ensemble des pays au regard des spécificités des organisations de leur cyberdéfense, constitue une référence intéressante.

Par ailleurs, des avancées technologiques remettent en cause certaines des prérogatives régaliennes. L'extraterritorialité des données appelle également la structuration de fondations théoriques nouvelles.

Enfin, la question de l'application du concept de dissuasion au cyberespace continue à faire l'objet de nombreux débats au niveau international. La France réserve, quant à elle, le terme de dissuasion au domaine nucléaire militaire. Garantie ultime de notre souveraineté, la dissuasion se fonde sur la nature unique de l'arme nucléaire. L'arme cyber ne saurait exercer l'effet de retenue ou de dissuasion très spécifique constaté et entretenu avec la dissuasion nucléaire en raison de ses effets profondément différents. Enfin, la « grammaire » de la dissuasion nucléaire est singulière et ne s'applique pas aux actions cybernétiques.

Le concept de « cyber-dissuasion » avancé par certains emporte au moins trois limites :

- tout d'abord, tout acte de dissuasion est fondé sur une rhétorique claire et crédible. Or, en matière de cyber, dévoiler publiquement ses capacités revient à compromettre leur efficacité dans la mesure où cela peut conduire l'adversaire potentiel à prendre les mesures nécessaires pour nier toute possibilité d'attaque cyber. La « cyber dissuasion » ne peut donc avoir une efficacité absolue car les armes sur lesquelles elle s'appuie peuvent rapidement s'avérer inefficace si des contre-mesures sont déployées ;
- deuxième limite, les armes cyber n'exercent pas le même effet dissuasif que les armes nucléaires, ces dernières ayant la capacité unique d'infliger des dommages absolument inacceptables, hors de proportions avec le bénéfice de l'agression. Il s'agit d'une arme d'une autre nature, sans continuité avec les moyens conventionnels et cyber. L'équation est donc forcément différente pour la menace de l'emploi d'une arme cyber ;
- la dissuasion nucléaire repose, enfin, sur un dialogue dissuasif entre Etats dotés. Elle demeure aujourd'hui une composante essentielle de la sécurité et de la stabilité internationale, notamment dans la zone euro-atlantique. La situation est différente avec les armes cyber dans la mesure où celles-ci peuvent être produites et surtout utilisées - pour les moins sophistiquées d'entre elles - assez facilement par un grand nombre d'acteurs, étatiques ou non. Par conséquent, les armes cyber ne sont pas en mesure de susciter des équilibres stratégiques pourvoyeurs de stabilité dans la zone euro-atlantique.

La vocation de dissuasion dans le cyberespace utilisée par nos partenaires britannique et américain désigne en réalité un concept différent du nôtre : il s'agit, par une combinaison de mesures défensives, de résilience et de riposte (pas nécessairement cyber) de « dissuader » (au sens américain) un adversaire. C'est la reproduction dans le domaine cyber d'un débat stratégique qui dure depuis 60 ans et qui nous a notamment déjà opposés sur les notions de « dissuasion conventionnelle » ou de « dissuasion par déni ».

Il est en revanche possible, notamment à l'OTAN, de gérer ces divergences doctrinales anciennes. Le *Cyber Defence Pledge*, la reconnaissance du cyberespace comme domaine d'opérations, la politique de protection des infrastructures cyber de l'Alliance constituent des messages qui visent à décourager l'adversaire et contribuent, à ce titre, à renforcer la posture globale de dissuasion et de défense de l'Alliance. Une forme de découragement des velléités d'agressions contre des membres de l'OTAN dans le cyberespace est donc possible et acceptable.

1.6. Les différents modèles d'organisation de cyberdéfense dans le monde

1.6.1. Dans le domaine cyber, les puissances sont peu nombreuses et bien identifiées

Une dizaine d'acteurs particulièrement puissants en matière de cyberdéfense dominent la scène internationale : la communauté dite des « *Five eyes* », qui regroupe les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle Zélande, du nom de l'alliance qui réunit

les services de renseignement technique de ces pays depuis la Seconde guerre mondiale, la Russie, la Chine, Israël, l'Allemagne et la France.

Engagé depuis le début des années 2000, l'effort français en matière de cyberdéfense s'inscrit dans une dynamique de développement capacitaire et de réflexion stratégique que l'on retrouve dans les pays anglo-américains (Etats-Unis et Royaume-Uni), en Allemagne, comme en Russie, en Chine et en Israël.

Les stratégies de cyberdéfense de ces pays reposent toutefois sur des modèles distincts (avec d'une part un modèle regroupant au sein des agences de renseignement les aspects défensifs et offensifs et, d'autre part, un modèle séparant distinctement ces deux aspects), ainsi que sur des visions du cyberespace opposées (les visions russe et chinoise apparaissant comme fondamentalement différentes de la vision occidentale).

Par ailleurs, si l'effort capacitaire est partagé, les moyens humains et financiers mobilisés par ces différents pays s'inscrivent dans des ordres de grandeur hétérogènes. De plus certains pays ont adopté ou vont adopter des politiques de protectionnisme notamment pour maitriser totalement la sécurisation de leurs réseaux.

Le cyber, une priorité stratégique partagée par les Etats-Unis, le Royaume-Uni, l'Allemagne, la Russie, la Chine et Israël

Leader incontesté dans le domaine de la cyberdéfense, les États-Unis ont pris conscience avec un temps d'avance sur les autres puissances mondiales, dès la fin des années 1990, des risques pesant sur leurs systèmes d'information et de communication et leurs infrastructures. Un décret présidentiel sur la protection de l'infrastructure critique est signé en 1998, et le *Department of Homeland Security* est créé en 2001 pour protéger les réseaux étatiques. Héritage d'une attention portée de longue date au renseignement technique, les Etats-Unis accordent une priorité stratégique à la cyberdéfense. Le président OBAMA en avait fait une priorité de son mandat et avait nommé, dès 2009, à la *Maison Blanche* un conseiller spécialement chargé du sujet. La cyberdéfense a progressivement occupé une place de premier plan dans la stratégie de défense et de sécurité nationale américaine. Figurant parmi les axes majeurs de la *National Security Strategy* de 2010, son importance a été réaffirmée par celle de 2015 et confirmée à nouveau dans celle de 2017. Le modèle de cyberdéfense américain se distingue du modèle français, fondé sur la séparation des capacités offensives et défensives. Les capacités de cyberdéfense américaines sont en effet largement concentrées au sein de la communauté du renseignement. Ce modèle, s'il a l'avantage de permettre une mutualisation des compétences techniques nationales au sein du pôle d'expertise que constitue la NSA, présente néanmoins des inconvénients. Il pose en effet la problématique de l'acceptabilité par le secteur privé des interventions de l'État en matière de sécurité des systèmes d'information, dans un contexte marqué par les révélations d'Edward SNOWDEN, qui ont mis en lumière l'ampleur des renseignements techniques qui auraient été collectés par la NSA.

Le modèle britannique est proche du modèle américain. Le Royaume-Uni a adopté une stratégie nationale en matière de sécurité de l'information dès 2003 ; cette première

stratégie mettait l'accent sur le partenariat entre les secteurs publics et privés au sein du *National Infrastructure Security Coordination Center*, afin notamment d'assurer la sécurité des réseaux et des systèmes informatisés de contrôles industriels. Le Royaume-Uni a présenté sa nouvelle *National Cyber Security Strategy* en novembre 2016. Elle constitue le nouveau cadre d'action du gouvernement britannique pour la période 2016-2021. L'objectif est que le Royaume-Uni puisse, à l'horizon 2021, être en situation d'être « *sûr et résilient face aux menaces cyber afin de se montrer prospère et confiant dans le monde numérique* ».

C'est en 2011 que le gouvernement fédéral allemand a adopté sa première stratégie nationale de cybersécurité. Sa version actualisée en 2016 traduit une vision du cyberespace très proche de celle de la France. Paris et Berlin partagent des orientations stratégiques communes sur de nombreux sujets techniques, tels que la cryptographie ou la certification des produits de sécurité, mais également politiques, comme la promotion d'une Union européenne résolue et dynamique en matière de sécurité numérique. Cette proximité fait de l'Allemagne un partenaire privilégié de la France au sein des diverses enceintes internationales traitant de ces sujets, et confère au couple franco-allemand un rôle d'impulsion majeur dans les projets européens relatifs à la sécurité des systèmes d'information.

C'est en 2006 que le *Plan de développement national pour les sciences et des technologies* du gouvernement chinois mentionne pour la première fois les enjeux de sécurité des systèmes d'information critiques. La cyberdéfense est élevée au rang de priorité absolue en 2014, avec la création du *Groupe dirigeant restreint pour la sécurité des réseaux centraux et l'informatisation*, organe stratégique rassemblant les plus grands décideurs politiques du pays. Le président XI JINPING a alors choisi d'assurer personnellement la présidence de ce *Groupe dirigeant restreint*, envoyant un signal fort au pays mais également à l'ensemble de la communauté internationale. Une place prépondérante est accordée à la cybersécurité dans le Livre blanc chinois, adopté en mai 2015. Il constitue une première reconnaissance publique de l'existence de capacités cyber-offensives et introduit une doctrine de *défense active*, assurant d'une réponse potentiellement militarisée, de nature cyber ou non, à toute action jugée contraire aux intérêts de Pékin. En décembre 2016, dans le prolongement de ce Livre blanc, la Chine publie pour la première fois une stratégie nationale de cybersécurité, qui appelle à rechercher « la paix, la sécurité, l'ouverture, la coopération, et l'ordre dans le cyberespace » et affirme son ambition de devenir une « superpuissance cyber ». Le cyberespace est considéré par les autorités chinoises à la fois comme un lieu et un moyen de développement économique et de contrôle de l'opinion. L'approche chinoise du cyberespace se distingue nettement de l'approche occidentale dans la mesure où elle confère à l'Etat une mission de « sécurité de l'information », qui s'étend bien au-delà de la « sécurité des systèmes d'information ». Cette vision, que la Chine partage avec la Russie, est héritée du fort attachement des régimes de ces pays au contrôle étatique de l'information : l'État ne doit pas uniquement assurer l'intégrité de ses réseaux mais également contrôler le contenu des informations qui y transitent. Cette approche est en opposition fondamentale avec la conception occidentale du cyberespace.

Dès son arrivée au pouvoir, Vladimir POUTINE a montré son intérêt pour le cyberespace. Il dote en 2000 la Russie de sa première doctrine de *sécurité informationnelle*, qui décrit la sécurité de l'information comme une composante essentielle de la sécurité de l'État. La doctrine russe s'est étoffée dans les années 2010 avec la publication de la doctrine militaire de la Fédération de Russie de 2010, les *Points de vue conceptuels sur les activités des Forces armées dans l'espace informationnel* de 2012. La Russie se distingue nettement de la plupart des grandes puissances occidentales dans sa conception du cyberespace. Marquée par une préoccupation de contrôle de l'information héritée de la période soviétique, la vision russe ne se limite pas aux systèmes d'information mais s'étend à l'ensemble de la sphère informationnelle. Par opposition aux doctrines cyber des Etats occidentaux, centrées sur la protection des contenants, la doctrine russe, tout comme la doctrine chinoise, s'intéresse avant tout au contenu. Cette perception s'incarne dans le concept de *défense informationnelle*, qui constitue un pilier de la doctrine russe. Moscou place ainsi les activités d'influence, en particulier dans leur dimension psychologique, au cœur de sa cyberstratégie. Les médias y sont pleinement intégrés en tant que forces de *contre-propagande* et de nombreuses agences de « *trolling* » rémunèrent des internautes pour relayer massivement des messages pro-russes sur les réseaux sociaux. L'organisation de la cyberdéfense russe repose sur des capacités dans ce domaine largement concentrées au sein de la communauté du renseignement.

Israël, enfin, est aujourd'hui en pointe en matière de cyberdéfense, grâce à un dispositif gouvernemental performant en lien étroit avec l'armée, le monde universitaire et l'industrie. La stratégie israélienne n'ait pas encore fait l'objet d'un document officiel.

Des efforts capacitaires asymétriques

L'analyse de ces organisations révèle un développement capacitaire hétérogène, sur les plans humain et financier, des pays pouvant être considérés comme les principales puissances cyber.

Le budget des Etats-Unis dans le domaine de la cyberdéfense s'est élevé à 14 milliards de dollars en 2016 et, dans son projet de budget pour l'année fiscale 2017, l'administration OBAMA avait requis des financements de près de 19 milliards de dollars. En 2016, le *Department of Homeland Security* (DHS) comptait 691 agents dans le secteur de la cybersécurité et a réalisé 818 million de dollars d'investissements dans ce domaine, soit 2 % de son budget total. Pour sa part, l'US-CERT dispose d'un budget de 98 millions de dollars pour 203 agents. Enfin, si le budget affecté à la NSA est une information classifiée, il est estimé proche de 10 milliards de dollars et ses effectifs supérieurs à 30 000 agents.

La nouvelle *National Cyber Security Strategy* du Royaume-Uni, présentée en novembre 2016, prévoit un investissement budgétaire de £1,9 milliards sur les cinq ans à venir.

Les ressources et le budget du ministère de l'intérieur allemand affectés à la cybersécurité ne sont pas connus avec précisions, Le BSI emploie quant à lui plus de 700 agents, auxquels devraient s'ajouter 100 nouvelles recrues d'ici fin 2018.

Les capacités cyber-offensives chinoises, dont le périmètre exact demeure difficile à évaluer, se concentrent principalement au sein de l'*Armée Populaire de Libération*, qui constitue le fer de lance des actions d'espionnage politique et économique visant l'étranger. Cette dernière fait actuellement l'objet d'une importante réforme, dont un des objectifs est la mutualisation des ressources d'attaque et de défense au sein de l'armée.

1.6.2. Des puissances de taille modeste capables de déployer des capacités offensives avancées

Si ces quelques pays se sont positionnés assez tôt sur le sujet, il serait très surprenant que d'autres pays n'aient pas déjà investi fortement dans des capacités offensives. En effet, la divulgation des outils américains et les outils de hacking disponibles sur des marchés plus ou moins officiels peuvent permettre à des États, même de taille modeste, de construire des capacités offensives pour peu qu'ils disposent d'une main d'œuvre compétente. Aussi, des pays comme la Corée du nord, le Pakistan et l'Iran ou bien encore le Japon, la Corée du sud et l'Inde, comme de nombreux pays européens, ont déjà des capacités, même s'il est difficile de les évaluer.

Partie 2. L'Etat, responsable de la cyberdéfense de la nation

La puissance d'un Etat dans le domaine cyber ne se mesure pas à la seule possession de capacités offensives et défensives. Elle repose fondamentalement sur l'aptitude et la volonté de celui-ci de les employer pleinement. Elle dépend de la détermination à décourager les attaques en augmentant la difficulté, le coût et le risque pour un agresseur. Elle suppose, enfin, que l'État puisse s'appuyer sur une industrie en mesure de relayer ou d'élargir son action. Il appartient aujourd'hui à la France de relever ce défi de la cyberpuissance.

La cyberdéfense de la France repose sur un modèle d'organisation et de gouvernance qui sépare les missions et capacités offensives des missions et capacités défensives (2.1.). Fondé sur la mise en place d'une chaîne défensive indépendante, ce modèle est garant du respect des libertés individuelles. Aujourd'hui, il prend toutefois insuffisamment en compte la contribution de certains acteurs à la cyberdéfense de notre pays et reflète de manière incomplète les missions de la cyberdéfense. Il mérite à ce titre d'évoluer (2.2.).

La consolidation de notre modèle de cyberdéfense permettra de mieux répondre aux attaques informatiques, voire de les prévenir. Elle devra s'accompagner de l'amélioration de la protection contre les menaces de nos systèmes d'information les plus critiques (2.3.).

La nouvelle ambition portée par cette revue stratégique suppose par ailleurs l'amélioration de la prévention et des facultés d'investigations, ainsi que le renforcement de l'efficacité de la réponse pénale à la cybercriminalité (2.4.).

Enfin, à l'heure où les capacités cyber des États évoluent considérablement, la France doit agir en acteur de référence au sein de l'Union européenne sur les questions numériques. Elle doit y déployer une stratégie d'influence promouvant son modèle et participer activement à la définition des normes régulant le cyberespace aux niveaux européen et international (2.5.).

2.1. Le modèle français de cyberdéfense

2.1.1. Aux origines du modèle français de cyberdéfense

La France a pleinement pris conscience de la nouvelle donne stratégique que constitue la cyberdéfense dès le milieu des années 2000, et a réagi de façon continue aux évolutions extrêmement rapides qui caractérisent ce secteur. La cyberdéfense constitue un enjeu stratégique majeur pour la sécurité nationale et le développement économique de notre pays. Relever le défi de la cyberdéfense, c'est être capable à la fois de créer les conditions d'une supériorité opérationnelle et de contribuer au développement économique et au rayonnement national et international des solutions françaises dans ce domaine.

Le Livre blanc sur la défense et la sécurité nationale de 2008 a permis à la France de franchir une étape décisive dans la prise en considération de la menace cyber et dans la mise en œuvre des réponses qu'elle requiert. Il a annoncé la création d'une agence nationale pour

traiter les attaques informatiques et protéger les systèmes d'information de l'État et les infrastructures critiques. Avec l'ANSSI, instituée par le décret n°2009-834 du 7 juillet 2009, rattachée au secrétaire général de la défense nationale, la France met alors en place un modèle de cyberdéfense fondé sur la séparation de ses capacités offensives et de ses capacités défensives. Un an plus tard, alors qu'une attaque de ses ministères économiques et financiers à des fins d'espionnage est révélée, la France élabore sa première stratégie de cybersécurité qu'elle publie début 2011.

En 2013, le nouveau Livre blanc sur la défense et la sécurité nationale confirme les menaces et les risques induits par l'expansion généralisée du cyberespace. Il élève la cyberdéfense au rang de priorité stratégique et affirme le principe d'une doctrine nationale de réponse aux agressions informatiques intégrant deux volets complémentaires consistant en la mise en place [20] :

- d'une posture robuste et résiliente de protection des systèmes d'information de l'État, des OIV et des industries stratégiques, couplée à une organisation opérationnelle de défense de ces systèmes, coordonnée sous l'autorité du Premier ministre ;
- d'une capacité de réponse gouvernementale globale et ajustée face à des agressions de nature et d'ampleur variées faisant en premier lieu appel à l'ensemble des moyens diplomatiques, juridiques ou policiers, sans s'interdire l'emploi gradué de moyens relevant du ministère des armées si les intérêts nationaux sont menacés.

Le Livre blanc de 2013 identifie la possibilité d'une attaque informatique majeure contre les systèmes d'information nationaux dans un scénario de guerre informatique comme une menace de première importance pour la France et ses partenaires européens. Il précise qu'une telle attaque, au regard de ses conséquences envisageables (paralysie de pans entiers de l'activité du pays, déclenchement de catastrophes technologiques ou écologiques, nombreuses victimes), pourrait « *constituer un véritable acte de guerre* ».

Tirant les conséquences de ce constat, la loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 renforce la sécurité informatique des OIV. Cette loi de programmation militaire prévoit notamment plus qu'un doublement des effectifs du ministère des armées dans le domaine cyber sur la période 2012-2019. Elle fixe ainsi un objectif de 3 200 personnes participant à la mission cyber en fin d'exercice et prévoit un triplement des crédits consacrés à cette mission, avec près de 440 millions d'euros engagés pour le développement et l'acquisition de nouvelles solutions de cybersécurité sur la période 2014-2019.

Plusieurs évènements sont venus ces dernières années accélérer et renforcer dans notre pays la prise de conscience de l'ampleur de la menace cyber. Ce fut le cas des attentats de janvier 2015 qui ont été suivis par des défigurations de sites Internet de collectivités locales qui, si elles ont été sans grandes conséquences, ont mis en lumière le volet cyber de la menace

[20] *Livre blanc sur la défense et la sécurité nationale*, 2013, pages 106-107.

terroriste. Ce fut aussi le cas de l'attaque informatique contre *TV5 Monde*, quelques mois plus tard, qui a révélé la vulnérabilité d'une chaîne de télévision participant au rayonnement international de la France. Enfin, l'attaque contre la messagerie des membres de l'équipe du mouvement politique « En Marche » en avril 2017, suivie de la publication des « MacronLeaks » à quelques heures de la fin de la période de campagne, a constitué une tentative de déstabilisation du processus électoral français.

2.1.2. Les principes du modèle français de cyberdéfense

La cyberdéfense de notre pays repose sur un modèle d'organisation et de gouvernance qui sépare les missions et capacités offensives des missions et capacités défensives - distinction au départ empirique puis consacrée par les *Livres blancs sur la défense et la sécurité nationale* de 2008 et de 2013. Ce modèle français se distingue nettement du modèle choisi par les pays anglo-saxons, dont les capacités de cyberdéfense sont concentrées au sein de la communauté du renseignement[21].

Le modèle français présente d'incontestables avantages. En distinguant les missions et les moyens dédiés à la cyberprotection de ceux dont l'objectif est le renseignement et les actions offensives, il facilite l'acceptation des interventions de l'État en matière de sécurité des systèmes d'information, tant dans l'administration que dans la sphère économique. Il est considéré comme respectueux des libertés individuelles et de la protection de la vie privée et permet le développement de relations de confiance entre des acteurs privés et les services de l'Etat chargés de la cyberprotection. C'est bien la stricte séparation des domaines d'intervention, et son statut d'agence interministérielle, qui ont permis à l'ANSSI d'être mobilisée avec efficacité et réactivité, en dehors de son champ d'action traditionnel, pour traiter plusieurs crises récentes, même si ces attaques ont, dans le même temps, souligné la nécessité de renforcer les mécanismes de coordination. Ce fut ainsi le cas, en 2015, au profit de *TV5 Monde*, victime de la première attaque informatique aux fins de sabotage perpétrée en France et, en 2017, au profit de la société *Saint-Gobain* ou pour contribuer à la sécurité des campagnes électorales. Pour ces raisons, d'autres pays, comme l'Allemagne, ont adopté un modèle quasi-similaire au modèle français.

Toutefois, s'il n'est pas compensé par une très forte coordination entre ses pôles défensif et offensif, le modèle français peut présenter, en termes d'efficacité, l'inconvénient d'une bipolarité trop fortement assumée. Nonobstant les avantages qu'il présente, notre modèle manque encore d'une confirmation de ses principes de base, d'une description précise de sa gouvernance, d'une clarification de son organisation opérationnelle, ainsi que d'une meilleure prise en compte des objectifs liés aux missions de renseignement et aux actions judiciaires. Il exige enfin, pour être plus efficace et cohérent, une plus grande fluidification des échanges au sein de la communauté de la cyberdéfense.

---

[21] C'est en particulier le cas au sein des agences de renseignement que sont la NSA aux Etats-Unis et le *Government Communications Headquarters* (GCHQ) au Royaume-Uni (*cf. supra*).

2.1.3. Le cadre juridique de la cyberdéfense française

Le cadre juridique sur lequel repose le modèle français de cyberdéfense est essentiellement polarisé sur la description et l'encadrement du volet défensif de la cyberdéfense depuis la création de l'ANSSI en 2009 par le décret n° 2009-834 du 7 juillet 2009, pris dans la continuité des préconisations du *Livre blanc sur la défense et la sécurité nationale* de 2008. La loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 (LPM 2014-2019) et portant diverses dispositions concernant la défense et la sécurité nationale a permis de préciser la définition de ce cadre juridique.

En vertu de l'article 21 de la LPM 2014-2019, le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information (article L. 2321-1 du code de la défense). Le secrétaire général de la défense et de la sécurité nationale, conformément à l'article R. 1132-3 de ce même code qui définit ses attributions, propose au Premier ministre et met en œuvre la politique du Gouvernement en matière de sécurité des systèmes d'information. Il dispose à cette fin de l'ANSSI, service à compétence nationale qui lui est rattaché, et dont les missions sont décrites par son décret de création (*cf. supra*).

L'article 22 de la LPM 2014-2019 a mis en place le dispositif approprié à la protection des activités d'importance vitale pour le fonctionnement normal de la Nation, qu'appelait de ses vœux le Livre blanc de 2013. En vertu des articles L. 1332-6-1 et suivants du code de la défense, les OIV sont désormais tenus de mettre en œuvre les règles de sécurité nécessaires à la protection de leurs systèmes d'information, de se soumettre à des contrôles destinés à s'assurer du respect de ces règles et de déclarer les incidents affectant le fonctionnement de leurs systèmes.

Cette loi a également permis de définir le cadre de la réponse de l'Etat aux attaques informatiques visant les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation. L'article L. 2321-2 du code de la défense offre ainsi aux services agissant sous l'autorité du Premier ministre les outils juridiques indispensables pour leur permettre de défendre les infrastructures d'importance vitale contre des attaques informatiques.

Au niveau interministériel, les capacités défensives de l'Etat sont pilotées par l'ANSSI. Autorité nationale de sécurité et de défense des systèmes d'information, rattachée au SGDSN, elle a été créée afin, notamment, d'assurer les trois missions suivantes :

- en tant qu'agence interministérielle au service de l'ensemble des administrations, elle coordonne les travaux interministériels en matière de sécurité des systèmes d'information ;
- elle prescrit aux administrations et aux OIV des règles de sécurité préventives, en contrôle l'application et, en cas de crise majeure, peut leur imposer des mesures réactives ;

- elle coordonne l'action gouvernementale en matière de défense des systèmes d'information et peut répondre, par des mesures techniques, aux attaques visant les administrations et les OIV, le cas échéant en neutralisant les effets des attaques.

L'ANSSI peut également apporter un soutien technique au ministère de l'intérieur et à l'autorité judiciaire en vue de caractériser les attaques, notamment en contribuant à la détermination des modes opératoires et l'identification des auteurs de cyberattaques.

Sur le périmètre des armées et conformément à l'article D. 3121-14-1 du code de la défense, le commandant de la cyberdéfense (COMCYBER) est responsable de la conduite de la défense des systèmes d'information des réseaux opérationnels du ministère des armées. Le COMCYBER, en lien avec l'ANSSI, est au cœur de la détection des attaques qui visent son périmètre et contribue, par le partage de ses informations, à une bonne compréhension de la menace.

Enfin, la DGSE et la DGSI traitent de la cyberdéfense dans le cadre général de leurs missions, décrites respectivement par les articles D. 1326-1 et suivants du code de la défense et par le décret n° 2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la DGSI. Lorsqu'une cyberattaque menace les intérêts fondamentaux de la Nation, limitativement énumérés à l'article L. 811-3 du code de la sécurité intérieure, les services spécialisés de renseignement, agissant dans le cadre de leurs missions de contre-ingérence, de contre-espionnage et de contre-terrorisme, peuvent solliciter la mise en œuvre d'une technique de renseignement pour compléter les informations dont ils disposent au plan national ou international, du fait de l'action de leurs agents ou par leurs partenaires. Les cyberattaques sont en effet un moyen d'action mobilisé de plus en plus largement par des ennemis ou des groupes hostiles, à des fins de déstabilisation, de dommages économiques et politiques ou de compromission et de manipulation d'agents. La loi sur le renseignement reconnait ainsi l'action qui incombe aux services de renseignement en matière de cyberattaques.

La mise en œuvre des techniques de renseignement aux fins d'anticiper, caractériser et attribuer se fait dans le cadre rigoureux de la loi du 24 juillet 2015 relative au renseignement, sous le contrôle a priori et a posteriori de la CNCTR.

Par ailleurs, l'article L. 2321-2 du code de la défense offre aux services agissant sous l'autorité du Premier ministre les outils juridiques indispensables pour leur permettre de défendre les infrastructures d'importance vitale contre des attaques informatiques sans risquer d'entrer dans le champ des incriminations prévues aux articles 323-1 à 323-3 du code pénal. Il est mis en œuvre dans les conditions fixées par le Premier ministre et n'est déclenché que lorsqu'une attaque informatique est de nature à affecter le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation.

Telles qu'elles ont été définies par le Premier ministre dans l'instruction classifiée du 7 mars 2016, les conditions de mises en œuvre du dispositif prévu à l'article L. 2321-2 du code de la défense prévoient une coordination de l'action des différents services concernés sous la responsabilité de l'ANSSI qui définit, organise et dirige les opérations techniques nécessaires

à la caractérisation d'une attaque informatique. Il revient au SGDSN de faire procéder, le cas échéant, aux opérations techniques nécessaires à la neutralisation des effets d'une attaque informatique, après une évaluation préalable des conséquences potentielles des opérations techniques envisagées.

Par dérogation à ces principes, lorsque l'attaque informatique vise exclusivement des capacités opérationnelles des armées ou les chaînes de commandement de la défense, l'autorité compétente est le commandement opérationnel de la cyberdéfense de l'état-major des armées, en liaison avec l'ANSSI.

La rédaction de cet article, dont le Conseil d'Etat a estimé qu'elle ne se heurtait à aucun obstacle constitutionnel[22] offre aux services compétents le cadre juridique nécessaire pour répondre aux attaques informatiques majeures. Bien que la loi ne l'exige pas, le schéma d'organisation des services dans la mise en œuvre des opérations autorisées par la loi pourrait, cependant, être conforté, à périmètre constant de responsabilités, par l'adoption d'un acte réglementaire de niveau supérieur à l'instruction.

Par conséquent, pour conforter le dispositif de réponse aux attaques informatiques, il pourrait être proposé de définir par un texte réglementaire, à périmètre constant de responsabilités, les conditions de mise en œuvre des dispositions de l'article L. 2321-2 du code de la défense. Ce texte pourrait prendre la forme d'un arrêté publié, approuvant en annexe classifiée l'instruction du 7 mars 2016, dont les dispositions doivent rester couvertes par le secret de la défense nationale.

2.1.4. Les six missions de la cyberdéfense française

Avant de détailler les évolutions nécessaires à la consolidation du modèle français de cyberdéfense, la présente revue propose une nomenclature des missions de la cyberdéfense en six catégories :

- prévention ;
- anticipation ;
- protection ;
- détection ;
- attribution ;
- réaction (remédiation, répression des infractions et actions militaires).

[22] Avis n° 387788 du 25 juillet 2013 « *l'autorisation donnée par la loi aux services de l'Etat, pour répondre à une telle attaque informatique, de détenir des matériels permettant l'intrusion dans un système d'information, et la suppression, la modification ou l'altération des données ou de son fonctionnement afin de procéder aux opérations techniques strictement nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets ne se heurtait à aucun obstacle constitutionnel* ».

Prévention

Le degré de prise de conscience des risques numériques reste très différent d'un utilisateur à un autre. Si les OIV et, prochainement, les opérateurs de services essentiels sont légalement tenus de respecter un certain nombre de règles de cybersécurité, bon nombre d'acteurs et a fortiori les particuliers restent très vulnérables et réagissent souvent seulement après avoir été victimes d'une cyberattaque. Les petites et moyennes entreprises (PME) comme les collectivités territoriales peinent à dégager les ressources nécessaires à leur cybersécurité.

Pourtant, compte tenu des menaces que représentent les cyberattaques pour l'activité des entreprises et les particuliers, l'ensemble des acteurs doivent être sensibilisés à haut niveau. Si les contraintes budgétaires et financières sont réelles pour les petites structures, il existe toutefois de bonnes pratiques d'hygiène informatique et de conception des systèmes peu coûteuses et faciles à mettre en œuvre, mettant notamment l'accent sur les risques liés au facteur humain[23].

Cette mission de prévention et de sensibilisation revêt un caractère interministériel. Conformément aux orientations de la *Stratégie nationale pour la sécurité du numérique* adoptée par le Premier ministre en 2015, elle s'appuie localement sur l'action des préfets et des services de l'Etat. Le réseau territorial de l'ANSSI, les délégués régionaux à l'intelligence économique et les services du ministère de l'intérieur compétents en matière de sécurité économique, le réseau de transition numérique participent aussi à cette mission. Les chambres de commerce et d'industrie, les chambres des métiers et plus largement tous les réseaux professionnels sont également sollicités[24].

Anticipation

En complément des actions de sensibilisation des victimes potentielles, les attaques peuvent être anticipées (prévenues, atténuées ou neutralisées dans leurs effets) par le biais d'une meilleure connaissance des groupes d'attaquants. L'ANSSI estime à une soixantaine le nombre de modes opératoires différents actuellement mis en œuvre par les groupes d'attaquants susceptibles de porter atteinte à des intérêts relevant du champ de la sécurité nationale. Ces modes opératoires d'attaque (MOA) peuvent schématiquement être classés en trois catégories :

- MOA stratégique : mode opératoire employé par des attaquants dotés de capacités très avancées (exploitations de vulnérabilités non publiques, codes ayant un niveau de furtivité et de persistance élevé, rythme opérationnel soutenu) et connus pour se livrer à large échelle à des activités de sabotage d'infrastructures critiques, de déstabilisation ou d'espionnage de nature à remettre en cause la souveraineté nationale.

[23] *Cf.* troisième partie de la présente revue.

[24] *Stratégie nationale de sécurité numérique,* 2015, p. 21-22.

- MOA actif : mode opératoire employé par des attaquants n'entrant pas dans la première catégorie mais connus pour avoir déjà atteint des cibles françaises ou soupçonnés de cibler actuellement les intérêts français (institutions, ministères régaliens, OIV).
- Autres MOA : anciens MOA appartenant aux deux premières catégories sur lesquels l'ANSSI a peu d'information, ou nouveaux MOA ayant récemment fait l'objet de rapports d'éditeurs de solution de sécurité ou des services de renseignement.

La phase d'anticipation est conduite par l'ANSSI et l'ensemble des services de renseignement sous le pilotage du C4 TECHOPS (cf. page 55).

Protection

La protection des systèmes d'information est la brique essentielle pour résister aux attaques informatiques. Qu'il s'agisse de l'Etat ou des OIV, les dispositifs de protection doivent être renforcés et pouvoir compliquer fortement la tâche des attaquants, tout en facilitant la détection par les services compétents. Cet effort, qui doit se traduire par un travail de sécurisation périmétrique et intrinsèque des systèmes, est la seule option pour obtenir à moyen terme des systèmes d'information résilients et sûrs.

Si la stratégie de renforcement de la résilience des systèmes d'information d'importance vitale, et plus globalement de l'ensemble des systèmes, conduite par l'ANSSI, est absolument nécessaire, les effets bénéfiques de cette stratégie ne s'obtiendront qu'à moyen terme. D'ici là, la France doit développer une stratégie plus assertive vis-à-vis des cybermenaces [25].

Il convient de détecter et d'attribuer les attaques informatiques visant notre pays ou nos alliés et, le cas échéant, d'en neutraliser les effets.

Détection

La détection des attaques informatiques est une mission essentielle pour lutter contre les cybermenaces. La détection d'une attaque qui peut intervenir, comme nous l'avons vu dans la première partie, plusieurs années après le début de celle-ci, est liée à l'observation des effets de l'attaque ou à l'identification d'éléments techniques liés au mode opératoire de l'attaquant. Ces éléments, qui peuvent provenir de sociétés privées, de partenaires étrangers, des services de renseignement ou de l'administration, sont centralisés à l'ANSSI. L'ANSSI doit aussi assurer la bonne coordination de différentes entités. En plus de ce travail de consolidation et de coordination, l'ANSSI a en charge la détection des attaques sur les systèmes de l'administration. Le COMCYBER, par délégation de l'ANSSI, assure cette détection sur le périmètre des armées.

Le déploiement de techniques de chiffrement dans la sphère civile, y compris pour les particuliers, complexifie fortement la tâche des outils de détection qui, sauf à déchiffrer

[25] L'annexe 10 (page 166) décrit les mesures intégrées au projet de loi de programmation militaire et leurs conséquences.

l'ensemble des flux observés, n'accèdent facilement qu'à des métadonnées. Cette généralisation de la cryptographie invite à développer de nouvelles stratégies de détection en déployant des capteurs au sein même des systèmes.

Les services de renseignement ont une place importante dans ce dispositif de détection. Ils sont susceptibles d'obtenir des renseignements démontrant une intrusion. Ils peuvent, agissant dans le cadre de leurs missions de contre-ingérence, de contre-espionnage et de contre-terrorisme, solliciter la mise en œuvre d'une technique de renseignement pour compléter les informations de détection dont ils disposent au plan national ou international, du fait de l'action de leurs agents ou par leurs partenaires.

Attribution

Après la détection d'une attaque, il est essentiel de pouvoir remonter jusqu'à l'instigateur pour pouvoir lancer des poursuites judiciaires à son encontre ou préparer une réponse adaptée. L'attribution des attaques, si elle reste bien une décision politique, se base en premier lieu sur les indices récupérés lors de la détection de l'attaque et de l'investigation qui s'en suit. Ce travail réalisé par une société privée, les services de police et de gendarmerie ou bien l'ANSSI n'est souvent pas suffisant pour obtenir des éléments factuels.

Pour compléter les premiers éléments techniques, les services spécialisés de renseignement peuvent solliciter, comme dans le cadre de leur mission de détection, la mise en œuvre d'une technique de renseignement pour parfaire l'attribution. La loi sur le renseignement reconnaît l'action qui incombe aux services de renseignement en matière de cyberattaques.

La mise en œuvre des techniques de renseignement à fin d'attribution des cyberattaques se fait dans le cadre rigoureux de la loi du 24 juillet 2015 relative au renseignement, sous le contrôle *a priori* et *a posteriori* de la CNCTR. Les renseignements nécessaires obtenus par ce biais, comme par toute autre voie, sont portés, lorsque nécessaires, à la connaissance de l'ANSSI et du COMCYBER pour l'exercice de leurs missions.

Réaction (remédiation, répression des infractions et actions militaires)

La réaction à une attaque nécessite de remettre rapidement le système attaqué en état de fonctionnement tout en s'assurant que l'attaquant ne pourra pas revenir s'installer facilement sur le système. Ce travail, aussi appelé remédiation, est conduit par le responsable du système qui peut bénéficier des conseils de l'ANSSI pour s'assurer que le nouveau système est sain et le restera. C'est au responsable du système d'assumer le compromis entre une remise en état fonctionnel rapide du système et l'assurance de disposer *in fine* d'un système sain et robuste.

Par ailleurs, une attaque informatique peut entraîner le déclenchement d'une enquête judiciaire. Si la cybercriminalité explose et nécessite une répression adaptée, la criminalité traditionnelle s'appuie également de plus en plus sur des moyens informatiques. Les techniques de chiffrement et les précautions mises en œuvre par les malfaiteurs nécessitent la mise en place de nouveaux moyens pour les enquêtes. Ces moyens cyber, permettant la

récupération d'éléments de preuves sur les équipements d'un suspect, vont se multiplier, en particulier la captation de données informatiques à distance. D'autres moyens, tels que l'enquête sous pseudonyme, devront voir leur champ d'application élargi. Ce développement doit évidemment se faire dans des conditions qui permettent de préserver le caractère non contestable sur le plan juridique de la preuve numérique et des moyens de son obtention (*cf. infra 2.4.*).

Enfin, le développement important à l'échelle mondiale du numérique présente une réelle opportunité pour l'utilisation d'actions cyber en soutien des opérations militaires. Quelques pays utilisent déjà massivement des moyens cyber pour réaliser des opérations de renseignement ou soutenir des opérations spéciales. « L'arme cyber » est un outil qui peut être particulièrement sélectif et dont les effets peuvent être réversibles. Utilisées pour garantir la supériorité dans le cyberespace, les capacités cyber permettent aussi aux armées de mener leurs opérations traditionnelles de manière plus efficace et moins coûteuse. La France a déjà investi dans ce domaine et la capacité cyber est désormais intégrée à toutes les opérations militaires.

2.2. Consolider l'organisation de la cyberdéfense

Organisé autour de ses deux pôles chargés, pour l'un, de la lutte informatique active (LIA) et, pour l'autre, de la lutte informatique défensive (LID), notre modèle de cyberdéfense présente, nous l'avons souligné, d'incontestables avantages. Il prend toutefois, ainsi que nous l'avons montré, insuffisamment en compte la contribution de certains acteurs nationaux à la cyberdéfense et reflète actuellement de manière incomplète les différentes finalités de la cyberdéfense que nous venons de décrire. C'est pourquoi la présente revue propose de clarifier l'organisation de la cyberdéfense en la formalisant autour de quatre chaînes opérationnelles (2.2.1.), et d'en renforcer les mécanismes de gouvernance et de cohérence technique (2.2.2.). Elle préconise ensuite d'optimiser la démarche capacitaire (2.2.3.) et de mettre en place un processus opérationnel de gestion des crises cyber (2.2.4).

2.2.1. Créer quatre chaînes opérationnelles pour conduire les missions de cyberdéfense

Sans remettre en cause les principes sur lesquels le modèle français est fondé, la revue stratégique de cyberdéfense propose une organisation de l'action de l'État en matière de cyberdéfense selon quatre chaînes opérationnelles, chacune concourant à une ou plusieurs des six missions de cyberdéfense précédemment exposées : chaîne « protection », chaîne « action militaire », chaîne « renseignement » et chaîne « investigation judiciaire ». Chaque chaîne opérationnelle a vocation à disposer, selon des modalités appropriées, de procédures de direction et de contrôle *ad hoc*, qui préservent la distinction entre les différentes missions de cyberdéfense.

La chaîne opérationnelle « Protection »

Sous la responsabilité du Premier ministre, la chaîne « protection » recouvre le périmètre de la lutte informatique défensive et a pour objet d'assurer la sécurité nationale en cas de cyberattaque. Des missions de prévention, d'anticipation et de protection y sont conduites.

Conformément aux textes législatifs et réglementaires encadrant la cyberdéfense en France, le SGDSN anime cette chaîne. La responsabilité de la conduite des opérations est confiée au directeur général de l'ANSSI. En lien avec l'ANSSI, le COMCYBER est responsable des opérations conduites sur le périmètre du ministère des armées.

La chaîne opérationnelle « Action militaire »

Sous l'autorité du Président de la République, chef des armées, la chaîne « action militaire » a recours à la lutte informatique et doit permettre la conduite des opérations de défense nationale.

La chaîne opérationnelle « Renseignement »

Sous l'autorité du gouvernement, la chaîne « renseignement » recouvre l'ensemble des actions entreprises dans un but de renseignement et notamment en vue d'attribution.

Aujourd'hui, les lois sur le renseignement du 24 juillet et du 30 novembre 2015 encadrent les facultés de capter des données aux fins de renseignement pour les services de renseignement. Les autorités d'emploi sont les directeurs des services concernés, sous l'autorité de leur ministre de tutelle.

Le CNRLT favorise, entre les services, le partage de renseignement d'intérêt cyber. Il peut ponctuellement s'appuyer sur l'inspection des services de renseignement pour assurer un rôle de conseil et de contrôle des capacités.

Le Premier ministre autorise les opérations à fins de renseignement menées sur le territoire national, après avis de la CNCTR, qui s'effectuent dans le respect de la loi renseignement, notamment concernant la durée de conservation des données et les finalités légales.

La chaîne opérationnelle « Investigation judiciaire »

La chaîne « investigation judiciaire » recouvre l'action des services de police et de gendarmerie et de la justice.

Selon les cadres d'enquête, les services de police et de gendarmerie travaillent sous le contrôle de l'autorité judiciaire (procureur de la République, juge des libertés et de la détention ou juge d'instruction).

Différents services sont chargés de mettre à disposition des services d'enquête, spécialisés ou non, des outils et techniques modernes d'investigation. Par exemple, la DGSI est chargée de la mise en œuvre des capacités opérationnelles de captation de données ; le service interministériel d'assistance technique (SIAT) met en œuvre des techniques d'infiltration ; l'agence nationale des techniques d'enquêtes numériques judiciaires (ANTENJ) via la

plateforme nationale des interceptions judiciaires (PNIJ) fournit un service d'interceptions judiciaires.

2.2.2. Moderniser la gouvernance de la cyberdéfense

Le comité directeur cyber

Les orientations et directives dans le domaine de la cyberdéfense sont prises en Conseil de défense et de sécurité nationale (CDSN).

Le comité de direction de la cyberdéfense (dit « comité directeur cyber ») est chargé de suivre la mise en œuvre des décisions prises en matière de développement et d'organisation générale du domaine. Il veille en particulier au bon déroulement de la montée en capacité du système dans le domaine technique (investissements en moyens humains et financiers, socle de cohérence technologique) et à la bonne coordination fonctionnelle entre les quatre chaînes opérationnelles décrites précédemment.

Le comité directeur cyber a un rôle organique et n'intervient pas dans la conduite des opérations.

Chargé de préparer et d'instruire les décisions du niveau du Président de la République, il est coprésidé par le chef de l'état-major particulier du Président de la République (CEMP), le coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT) et le directeur du cabinet du Premier ministre. Il associe l'ensemble des ministères et des services impliqués dans le domaine de la cyberdéfense.

Le secrétariat du comité directeur cyber est assuré par le secrétaire général à la défense et à la sécurité nationale (SGDSN).

Le comité de pilotage de la cyberdéfense

Les travaux du *comité directeur cyber* sont préparés par un comité de pilotage, placé sous la direction du cabinet du Premier ministre.

Le centre de coordination des crises cyber (C4)

Si aujourd'hui l'Etat est bien organisé pour faire face à une crise majeure d'origine cyber (avec la cellule interministérielle de crise - CIC), l'expérience opérationnelle récente a montré que l'organisation de la gestion des crises de moindre ampleur était perfectible. Pour les crises cyber ne nécessitant pas la mise en œuvre de plans gouvernementaux, ainsi qu'en cas de publication de vulnérabilités majeures susceptibles d'être exploitées à court terme, il paraît indispensable de mettre en place un mécanisme interministériel permanent d'analyse de la menace, de préparation et de coordination, associant l'ensemble des ministères concernés par la crise.

Il est proposé que ce mécanisme prenne la forme d'un *centre de coordination des crises cyber* (C4), appelé de leurs vœux par les ministères concourant à la mission de cyberdéfense. Chargé de la supervision de la cyberdéfense, ce C4 se structurera en trois niveaux distincts :

un C4 stratégique (C4 STRAT), un C4 technique (C4 TECH) et un C4 restreint permanent et technique (C4 TECHOPS).

❖ *Le C4 stratégique (C4 STRAT)*

Le C4 STRAT regroupera, mensuellement et autant que de besoin, l'ensemble des acteurs concernés au-delà de la seule sphère technique. Il aura pour mission d'assurer l'échange des informations et analyses relatives aux attaques informatiques et de faciliter la préparation des options de réponse de l'Etat, tant sur les aspects techniques, que diplomatiques voire judiciaires, sans préjudice des responsabilités politiques et opérationnelles des organismes et ministères de tutelle et de l'autorité judiciaire.

A ce titre, le C4 STRAT favorisera, par la confrontation des expertises de ses membres, la préparation des options de réponse portées par les ministères et acteurs concernés lors de crises dans le domaine cyber qui ne nécessitent pas l'activation de la CIC. A cette fin, il valorisera notamment les éléments techniques issus du C4 TECH et veillera à la cohérence des mesures techniques avec les acteurs non cyber de la gestion de crise.

❖ *Le C4 technique (C4 TECH)*

Le C4 technique est hébergé à l'ANSSI et présidé par le directeur général de l'ANSSI ou son représentant. Il supervise l'emploi des moyens relatifs à la résolution des crises cyber de moindre ampleur. En particulier, il a pour missions de :

- structurer le dialogue entre les représentants des différents acteurs pour établir une évaluation technique de la crise en cours ;
- veiller à la cohérence des décisions techniques des services de l'Etat ;
- veiller à la cohérence des mesures techniques avec les acteurs non cyber de la gestion de crise.

En cas de crise majeure, et quel que soit le domaine de celle-ci, le C4 TECH se place en appui de la CIC dès son activation pour fournir aux autorités un état de la situation cyber et assurer un rôle de conseil.

❖ *Le C4 restreint permanent et technique (C4 TECHOPS)*

Le C4 TECHOPS est un organe permanent, à vocation technico-opérationnelle, permettant une analyse partagée entre les services compétents, de la menace, des modes d'actions et des acteurs menaçants, ainsi que l'anticipation des réponses sur le court/moyen terme, dont les travaux sont couverts par le secret de la défense nationale.

2.3. Améliorer la protection des activités sensibles

La consolidation du modèle national de cyberdéfense proposé par la présente revue permettrait de mieux réagir, voire de prévenir les attaques informatiques. Elle doit s'accompagner de l'amélioration de la protection de nos systèmes les plus critiques contre les menaces. A cet égard, cinq champs apparaissent prioritaires : la sécurisation des systèmes

d'information de l'Etat (2.3.1.), la protection des organismes d'importance vitale (2.3.2.), la protection des activités essentielles (2.3.3.), la protection des collectivités territoriales (2.3.4.) et la protection de la vie démocratique (2.3.5).

2.3.1. La sécurisation des systèmes d'information de l'Etat

La sécurité des réseaux de l'Etat est une des priorités de la stratégie de cyberdéfense française. Au-delà des réseaux les plus sensibles, qui doivent bénéficier d'une sécurité sans compromis, l'ensemble des réseaux de l'Etat doit faire l'objet d'une attention particulière. Cela constitue la mission historique de l'ANSSI qui, depuis sa création en 2009, assure un rôle d'expertise en sécurité informatique au profit de l'ensemble des services de l'Etat et, à ce titre, apporte son soutien technique à de nombreux projets informatiques sensibles. En tant qu'autorité nationale de sécurité et de défense des systèmes d'information, l'agence déploie également des dispositifs de détection des attaques au profit des ministères, élabore les règles de sécurité informatique qui s'appliquent aux services de l'Etat et réalise des inspections de la sécurité des systèmes d'information ministériels.

Si l'on constate une meilleure prise en compte des enjeux de cybersécurité par les acteurs publics, notamment par les autorités, celle-ci reste insuffisante. Le niveau de sécurité réel des systèmes d'information de l'Etat demeure inégal et souvent trop faible, ce qui les expose à des attaques informatiques, y compris non ciblées ou menées par des attaquants aux compétences techniques limitées. Plusieurs axes d'amélioration peuvent cependant contribuer à pallier ces faiblesses : le perfectionnement de la gouvernance de la cybersécurité, l'optimisation de l'utilisation du réseau interministériel de l'Etat à des fins de cyberdéfense, le renforcement de la supervision de la cybersécurité des services de l'Etat et l'adaptation de la politique d'achat de l'Etat aux enjeux de sécurité informatique.

Perfectionner la gouvernance de la cybersécurité

Le rattachement de l'ANSSI au secrétaire général de la défense et de la sécurité nationale, qui place celle-ci au plus près du Premier ministre, facilite les processus décisionnels et lui permet d'assurer son rôle de centre d'expertise interministériel. Néanmoins, la visibilité de l'ANSSI et son pouvoir de contrôle sur les initiatives numériques de l'Etat ne suffisent pas pour lui permettre de veiller à la bonne prise en compte de la sécurité. Son expertise est souvent sollicitée à des phases trop avancées des projets informatiques ministériels, ce qui génère alors d'importants surcoûts et rend difficile l'atteinte *in fine* d'un niveau de sécurité adapté aux risques. C'est pourquoi la présente revue recommande que les projets informatiques les plus importants et les plus sensibles de l'Etat soient soumis, dès leur phase de lancement, à l'ANSSI pour avis. S'agissant des projets de nature opérationnelle du ministère des Armées, il revient au COMCYBER d'être saisi pour avis et de solliciter l'ANSSI autant que de besoin. Cette démarche devra s'articuler avec le dispositif existant d'encadrement des projets informatiques par la DINSIC.

Au sein des ministères, la gouvernance de la sécurité des systèmes d'information doit être renforcée afin que la cybersécurité soit mieux prise en compte dans les projets informatiques

de l'Etat. En premier lieu, les directions des systèmes d'information (DSI) ministérielles sont insuffisamment formées et peu responsabilisées dans ce domaine. Leurs processus de travail prévoient rarement un volet relatif à la sécurité des systèmes d'information et le risque cyber est par conséquent souvent mal pris en compte dans de nombreux projets numériques ministériels. C'est pourquoi la revue recommande une responsabilisation des DSI ministérielles quant à la prise en compte de la cybersécurité dans les projets informatiques qu'elles conduisent, et le renforcement de leur formation à la sécurité des systèmes d'information.

En ce qui concerne les besoins en sécurité associés aux projets informatiques *métier*, on observe que le dialogue entre les directions métier et les DSI ministérielles est perfectible. Si la responsabilité de la sécurité du socle informatique commun à l'ensemble d'un ministère - comprenant par exemple la bureautique ou la messagerie électronique - relève de la DSI du ministère, il appartient en revanche aux directions *métier* elles-mêmes de fixer les besoins en sécurité des outils et applications numériques développées au profit de leur métier, parfois sans une implication significative de la DSI. Elles seules disposent des connaissances nécessaires pour qualifier les impacts d'une éventuelle attaque informatique sur les données et processus propres à leur activité et peuvent donc évaluer le risque et leurs besoins en cybersécurité. Pour cela, elles doivent être en mesure de s'appuyer sur du personnel disposant de compétences *métier* et formé à la cybersécurité. Cette mission doit être assurée par des référents en sécurité, issus des pôles d'expertise métier et formés à la sécurité numérique. La responsabilisation des directeurs d'administration quant à la sécurité des systèmes d'information *métier* apparaît ainsi indispensable, de même que la nomination et la formation de référents en sécurité numérique au sein des directions *métier* des ministères.

Optimiser l'utilisation du réseau interministériel de l'Etat (RIE) à des fins de cyberdéfense

Le réseau interministériel de l'Etat (RIE) est le réseau unifié de communications électroniques reliant les administrations de l'Etat. Sa gestion et son exploitation opérationnelle sont confiées à un service à compétence nationale créé en 2012 et placé au sein des services du Premier ministre. Ses missions sont de fluidifier les échanges interministériels et d'optimiser les coûts liés aux infrastructures informatiques de l'Etat, mais également de renforcer la sécurité du système d'information de l'Etat. Le réseau interministériel de l'Etat s'appuie notamment sur une plateforme unifiée d'accès à Internet qui offre des services de sécurité centralisés. Ces fonctions de sécurité permettent une réaction efficace en cas d'attaque informatique, par exemple par la mise en œuvre de mesures de blocage du trafic malveillant.

Cette plateforme commune d'accès à Internet est néanmoins insuffisamment utilisée par certains ministères, et par ailleurs souvent utilisée sans ses fonctions de sécurité, ce qui réduit les capacités de cyberdéfense de l'Etat. Son utilisation généralisée à tous les ministères permettrait en outre à l'ANSSI de renforcer significativement son service de détection des attaques informatiques. Au-delà des aspects relatifs à la sécurisation du réseau lui-même, il convient donc d'optimiser l'utilisation du RIE pour améliorer les capacités de cyberdéfense

étatiques. Cela implique d'inciter les ministères à rallier la plateforme d'accès à Internet du RIE et à utiliser pleinement les services qu'elle offre. De manière plus générale, il convient d'inciter les ministères à recourir de manière quasi-systématique aux services de sécurité offerts par le RIE.

Par ailleurs, l'exploitation des métadonnées du réseau interministériel de l'Etat pourrait être renforcée, le service à compétence nationale chargé de gérer ce réseau ne disposant pas des ressources et des compétences nécessaires pour assurer leur collecte et leur exploitation à des fins de cybersécurité. Or, ces données sont susceptibles de renforcer la capacité nationale de détection des attaques, notamment en permettant de rechercher *a posteriori* des traces de compromission dans le système d'information de l'Etat. Confier à l'ANSSI la détection des attaques sur ce réseau constituerait une réponse adaptée à cette situation, à charge pour l'ANSSI d'informer les ministères des découvertes d'attaques pour décision de l'autorité qualifiée SSI (AQSSI) et action éventuelle.

Renforcer la supervision de la cybersécurité des services de l'Etat

L'ANSSI opère depuis sa création un service interministériel de supervision de la sécurité, qui s'appuie notamment sur des sondes de détection d'attaques informatiques, positionnées sur les réseaux des ministères et sur le RIE. Le modèle actuel se heurte néanmoins à plusieurs limites.

En premier lieu, plusieurs administrations ne font toujours pas l'objet d'une supervision de sécurité, ce qui limite de fait la capacité nationale de détection des attaques. Cette situation s'explique par un investissement insuffisant des équipes de certains ministères dans le soutien qu'elles doivent apporter au déploiement de sondes de détection. Il convient néanmoins de noter que le raccordement progressif des ministères au RIE devrait permettre d'étendre le dispositif national de détection à des acteurs aujourd'hui non couverts.

En outre, ce dispositif de supervision de sécurité n'est pas applicable aux services étatiques hébergés par des prestataires externes, ces entreprises privées n'entrant pas dans le domaine de compétence de l'ANSSI. La tendance à l'externalisation des applications *métier* est donc susceptible, à droit constant, de remettre en question la capacité nationale de détection des attaques informatiques. C'est pourquoi, la présente revue recommande d'imposer la couverture complète des services informatiques utilisés par l'Etat par un dispositif de supervision de la sécurité, y compris dans les cas où ces services sont externalisés.

Adapter la politique d'achat de l'Etat aux enjeux de sécurité informatique

Le recours à des produits et à des services de cybersécurité labellisés par l'ANSSI constitue un levier important pour assurer la sécurité des réseaux de l'Etat. Cependant, sa mise en œuvre se heurte à plusieurs obstacles, dont l'incompatibilité des cadres d'achat ministériels et interministériels avec l'acquisition de telles solutions et l'insuffisance des budgets ministériels dans ce domaine. Par ailleurs, l'acquisition par l'Etat de solutions de sécurité est encore morcelée et, par conséquent, sous-optimale d'un point de vue économique.

Plusieurs approches mises en œuvre ponctuellement ces dernières années ont démontré leur capacité à lever certains de ces obstacles, tout en engendrant des effets bénéfiques pour les fournisseurs industriels des solutions concernées. Ainsi, l'inscription de certaines solutions labellisées par l'ANSSI dans les cadres existants d'acquisition de solutions informatiques a fortement facilité leur mise en œuvre par les administrations, et l'acquisition par l'ANSSI, en 2015, d'une licence globale libératoire pour les solutions logicielles labellisées de la société *Prim'X* a également été couronnée de succès, permettant le déploiement de plus de 600 000 logiciels de chiffrement robuste au sein de l'administration.

Un travail d'inventaire des besoins des administrations en solutions sécurisées et d'élaboration d'un cadre interministériel d'acquisition de telles solutions, y compris selon des logiques de licences libératoires, dans un double objectif d'optimisation de la dépense publique et de facilitation du déploiement de ces solutions, pourrait être confié à la *direction des achats de l'Etat*, avec le soutien de l'ANSSI.

Au-delà de l'acquisition de solutions spécialisées en matière de sécurité, les démarches plus générales d'achat de solutions informatiques par l'Etat devraient également faire l'objet d'une attention particulière à la sécurité, afin de garantir *a minima* le respect de bonnes pratiques élémentaires de sécurité informatique par tout nouvel outil numérique acquis par l'Etat.

Le principe d'avis de l'ANSSI sur les projets informatiques de l'Etat ne suffit pas à atteindre cet objectif, dans la mesure où une part significative de la commande publique en matière numérique ne relève pas de projets informatiques majeurs, mais d'acquisitions courantes ou de projets d'autre nature - comme, par exemple, la mise en place d'un système de vidéosurveillance dans le cadre d'un projet immobilier. C'est pourquoi la revue recommande d'élaborer des clauses contractuelles types regroupant les bonnes pratiques de sécurité applicables dans l'acquisition d'une solution informatique et d'inciter fortement les ministères à systématiser l'inclusion de ces clauses dans leurs marchés publics comportant un volet numérique.

2.3.2. La protection des opérateurs d'importance vitale (OIV)

Piliers de la résilience de l'Etat, les infrastructures critiques comprennent les entités publiques et privées qui fournissent des biens ou des services indispensables à la Nation ou peuvent présenter un danger grave pour la population. Si la définition d'une infrastructure critique varie selon les pays, elle recouvre généralement *a minima* l'approvisionnement en énergie, les communications électroniques, les systèmes de transport, les services financiers, la santé publique, la gestion de l'eau et les services publics indispensables. La France a ainsi défini en 2006 douze « secteurs d'activité d'importance vitale » et identifié plus de 200 « opérateurs d'importance vitale » (OIV) publics et privés. Ces derniers constituent le noyau dur des infrastructures critiques françaises. Le dispositif de sécurité des activités d'importance vitale, inséré dans le code de la défense, constitue le cadre législatif et réglementaire permettant d'associer les OIV au système national de protection contre le terrorisme, le

sabotage et les actes de malveillance. Il formalise le dialogue permanent entre l'Etat et ces opérateurs afin d'assurer leur sécurité.

Depuis sa création, l'ANSSI a progressivement renforcé son rôle auprès des OIV. Jusqu'en 2013, à l'exception du secteur des communications électroniques, les missions de l'ANSSI se limitaient à la diffusion de conseils techniques par l'élaboration de guides et de recommandations ou la réalisation d'audits de sécurité, uniquement à leur demande. Face à une menace informatique grandissante et à un risque de sabotage informatique de plus en plus élevé, le niveau de sécurité de ces acteurs demeurait insuffisant, les exposant, et à travers eux la Nation, à un risque cyber majeur. La France a donc choisi en 2013 d'imposer, par voie législative, des exigences en matière de sécurité informatique aux OIV, devenant ainsi un des premiers pays à légiférer dans le domaine de la cybersécurité des infrastructures critiques. Les dispositions cyber de la loi de programmation militaire de 2013[26] ont confié de nouvelles missions à l'ANSSI en la matière : elles prévoient que ces opérateurs appliquent les mesures de sécurité informatique fixées par l'ANSSI et lui notifient les incidents de sécurité affectant leurs systèmes d'information. Ces mesures, qui ont fait l'objet de concertations avec les opérateurs, sont aujourd'hui fixées par arrêtés du Premier ministre et revêtent donc un caractère contraignant. L'ANSSI accompagne les OIV sur le plan technique dans la mise en œuvre des textes d'application. En parallèle de cette démarche, la DGSI par le biais de son réseau territorial mène un travail indispensable en matière de sécurité intérieure et de protection économique couvrant, notamment, les OIV.

Ce nouveau dispositif constitue une étape majeure dans le renforcement de la cybersécurité des infrastructures critiques. Il a d'ores et déjà permis de recenser les systèmes d'information les plus sensibles de la Nation, de sensibiliser les dirigeants d'OIV au risque cyber et a conduit à d'importants investissements en cybersécurité. Néanmoins, le niveau de maturité reste inégal entre les différents secteurs d'activité, et de nombreux opérateurs ne disposent pas à ce jour des ressources suffisantes et de l'organisation adéquate pour piloter efficacement la sécurité de leurs systèmes d'information. Certaines règles élémentaires de sécurité informatique ne sont parfois pas appliquées aux systèmes critiques, dont certains présentent encore des failles exploitables par des attaquants de faible niveau. En outre, le socle de règles fixé par le dispositif actuel ne permet pas de prendre en compte de façon optimale les particularités de certains systèmes *métier*. Il importe en parallèle de la préparation de ces nouvelles règles de faire un bilan financier des mesures déjà mise en place afin d'en évaluer le rapport coût-efficacité.

Il convient donc de faire évoluer le modèle pour l'adapter davantage aux contraintes des secteurs et à l'évolution de la cybermenace, dans cinq directions : l'adaptation des règles de sécurité informatique aux métiers ; le renforcement de la cybersécurité des opérateurs « supercritiques » ; l'extension du dispositif réglementaire au traitement des incidents ; la

[26] Articles L. 1332-6-1 à L. 1332-6-7 du code de la défense.

prise en compte des particularités des entreprises de services numériques ; et le développement de l'offre privée d'assistance technique en cybersécurité.

La mise en œuvre des propositions faites dans cette partie de la revue sera assujettie à une étude d'impact détaillée, qui devra confirmer leur faisabilité économique (coût pour les acteurs économiques et pour l'Etat), technique, juridique et conclure à l'absence de risque pour les processus métier des entreprises.

Adapter les règles de sécurité informatique aux métiers

Afin d'être en mesure d'établir des règles de sécurité adaptées aux différents métiers, il a été décidé de les inscrire dans des arrêtés sectoriels. Toutefois, les exigences fixées par ces textes d'application sont aujourd'hui très proches d'un secteur à l'autre. En effet, les travaux préliminaires conduits avec les opérateurs ont révélé un niveau de maturité en cybersécurité très hétérogène, y compris au sein d'un même secteur. Ce constat a conduit l'ANSSI, en accord avec les ministères concernés et les OIV, à adopter une stratégie en deux étapes : imposer dans un premier temps à tous les opérateurs un socle commun de règles de sécurité élémentaires puis, dans un second temps, les adapter plus finement aux métiers et, le cas échéant, renforcer leur niveau d'exigence. Les arrêtés publiés à ce jour concrétisent cette première étape, dont l'objectif est de faire franchir à l'ensemble des opérateurs un premier seuil en matière de sécurité numérique.

L'application de ce socle de règles permettra de protéger les systèmes d'information les plus critiques contre la grande majorité des cyberattaques, en particulier contre les campagnes d'attaques indiscriminées telles que celles menées par rançongiciels au printemps 2017. Néanmoins, il ne permet pas de sécuriser selon l'état de l'art l'ensemble des systèmes d'information *métier*, dont certaines spécificités ne peuvent être prises en compte par un corpus de règles génériques. A titre d'exemple, il ne couvre pas de façon optimale la sécurité des systèmes d'information des opérateurs d'infrastructures numériques (points d'échange Internet, fournisseurs de services DNS, etc.), pour lesquels il est nécessaire d'élaborer des règles spécifiques, permettant notamment de prendre en compte leur forte interconnexion avec les réseaux publics. Ce modèle générique ne convient également pas aux particularités des systèmes industriels et embarqués.

Au regard des impacts sur la Nation qu'est susceptible d'avoir une attaque à l'encontre de tels systèmes et du niveau de sophistication croissant des attaques informatiques ciblant les infrastructures critiques, il est désormais nécessaire d'initier des travaux d'adaptation fine des règles aux métiers. Des travaux visant à adapter des règles de sécurité applicables aux OIV aux spécificités *métier* de chaque secteur pourraient ainsi être engagés, sous le pilotage de l'ANSSI et en lien étroit avec les acteurs publics et privés concernés.

Renforcer la cybersécurité des opérateurs « supercritiques »

En raison de leur rôle de fournisseur de services auprès d'autres OIV, les secteurs des communications électroniques et de l'approvisionnement en énergie électrique peuvent être qualifiés de « supercritiques ». Une attaque informatique à l'encontre d'un de ces acteurs

est en effet susceptible d'avoir des répercussions sur l'ensemble des activités d'importance vitale, et donc des effets potentiellement catastrophiques sur la résilience de l'ensemble de la Nation.

Par ailleurs, le potentiel rapprochement entre des groupes terroristes et des acteurs possédant de fortes capacités techniques qu'ils seraient prêts à monétiser laisse entrevoir la possibilité d'actes de sabotage informatique perpétrés à des fins terroristes. Le secteur des transports, qui constituerait alors une cible privilégiée, pourrait à l'avenir être qualifié de « supercritique » et nécessiter des mesures de sécurité renforcées.

Développer l'offre privée d'assistance technique en cybersécurité

Si l'ANSSI a un rôle important à jouer auprès des OIV, en particulier en matière de soutien technique et d'appui au traitement des incidents graves, elle ne peut seule assurer la mise en place de ce dispositif et doit être en mesure de s'appuyer sur un large écosystème de prestataires de services de cybersécurité à la fois compétents techniquement et de confiance. La qualification par l'ANSSI de prestataires de détection des incidents, d'audit de sécurité et de réponse aux incidents, prévue par le cadre réglementaire et en cours de mise en œuvre, répond en grande partie à cette nécessité.

Cependant, ce dispositif de qualification ne satisfait pas aujourd'hui le besoin des opérateurs de disposer de prestataires labellisés en mesure de les accompagner au quotidien dans la prise en compte de la cybersécurité dans leurs projets informatiques. L'absence de définition claire des missions d'assistance technique en matière de cybersécurité constitue un obstacle certain au développement d'un tel écosystème. Un nouveau référentiel relatif au métier d'assistance technique en cybersécurité, et l'extension de la labellisation par l'ANSSI à ce domaine, pourraient se révéler très utiles. Une réflexion pourrait par ailleurs être conduite sur la mise en place d'une mesure financière incitative visant à valoriser la labellisation par l'ANSSI et la prise en compte de la sécurité.

2.3.3. La protection des activités essentielles

Au-delà des OIV, qui constituent les piliers de la résilience de la Nation, d'autres acteurs fournissent des services essentiels au fonctionnement quotidien de l'économie et de la société. A ce titre, ils entrent également dans la catégorie des infrastructures critiques.

Malgré une prise de conscience qui se renforce, beaucoup de ces acteurs demeurent très vulnérables à des attaques informatiques susceptibles de paralyser durablement leur activité. Les récentes vagues mondiales de cyberattaques ont montré l'extrême fragilité et le manque de préparation d'entités essentielles à la vie quotidienne de la Nation. La propagation en mai 2017 du rançongiciel *WannaCry* a par exemple rendu durablement indisponibles de nombreux services de différentes natures dans le monde[27]. Malgré l'existence de

[27] Ont été affectés par *WannaCry* des usines de production, dont les usines RENAULT en France, des distributeurs automatiques de billets, des hôpitaux, des panneaux d'affichage en gare, etc. Au Royaume-Uni, plus de 20 % des

recommandations, de guides et de campagnes de sensibilisation, le niveau de cybersécurité de ces acteurs progresse trop lentement au regard de la menace. L'absence de bonnes pratiques de sécurité informatique, souvent liée à un manque de moyens humains et financiers accordés à la cybersécurité, les expose à des attaques informatiques susceptibles d'affecter fortement leurs activités.

Il est donc nécessaire d'imposer un socle minimal d'exigences en matière de cybersécurité à ces acteurs sensibles pour lesquels une cyberattaque est susceptible d'avoir des conséquences majeures sur la vie quotidienne de la Nation.

Transposer la « directive NIS »

La directive (UE) 2016/1148 du 6 juillet 2016, dite « directive NIS », qui concerne des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne, a notamment pour objet le renforcement du niveau de sécurité informatique des opérateurs fournissant des services essentiels au fonctionnement de l'économie et de la société. Première initiative législative globale de l'Union européenne dans le champ de la cybersécurité, cette directive s'inscrit dans le cadre d'une stratégie européenne visant à renforcer la cyber-résilience au niveau européen. Elle cherche plus particulièrement à augmenter les capacités nationales en matière de cyberdéfense et à accroître la coordination en cas d'incidents affectant plusieurs Etats membres.

La directive NIS fixe une liste minimale d'activités critiques devant être soumises à ces nouvelles obligations, Elle permet également de de protéger, un champ d'activités s qui, si elles étaient atteintes par une cyberattaque, pourraient entraîner des répercussions majeures sur la vie de la Nation. Un tel dispositif, , générerait en outre un effet d'entraînement sur l'écosystème numérique par l'atteinte d'une masse critique d'entreprises ayant recours à des solutions sécurisées. Les acteurs en charge de la santé, des prestations sociales ou bien encore de la conservation du patrimoine numérique national ont vocation par exemple être intégrés dans la transposition de cette directive pour en particulier être en mesure de répondre à une attaque criminelle systémique qui viserait à les paralyser massivement et qui malheureusement ne manquera pas d'arriver.

Définir un socle commun de règles de sécurité proportionnées

S'il serait disproportionné d'imposer à ces fournisseurs de services essentiels des règles aussi exigeantes que celles qui s'appliquent aux OIV, il est nécessaire que l'Etat fixe un socle commun de règles élémentaires de sécurité proportionnées permettant de protéger ces acteurs. En effet, si la paralysie d'un seul de ces opérateurs aurait des impacts moindres que l'arrêt d'une infrastructure critique, une cyberattaque massive affectant un nombre significatif de ces acteurs serait susceptible d'avoir un impact grave sur la vie de la Nation. L'application de règles élémentaires de sécurité informatique permettra de protéger ces acteurs contre la

---

organismes régionaux de gestion de santé ont été touchés, ce qui a conduit les hôpitaux affectés à reporter certains actes médicaux.

majorité des menaces, en particulier contre les vagues d'attaques massives et indiscriminées, telles que les rançongiciels, qui se sont propagées au printemps 2017.

Promouvoir une harmonisation européenne progressive

Si la sécurité des OIV est une prérogative souveraine des Etats, la sécurisation des entreprises essentielles pour l'économie et pour la société s'inscrit dans le cadre des compétences de l'Union européenne. L'article 114 du *Traité sur le fonctionnement de l'Union européenne* prévoit en effet que l'Union européenne est habilitée à adopter des mesures destinées à établir ou assurer le fonctionnement du marché intérieur. Le rôle primordial que jouent les systèmes d'information en soutien de ce fonctionnement justifie la mise en œuvre à l'échelle européenne de dispositifs de cybersécurité communs.

Par ailleurs, une grande part de ces acteurs est constituée d'entreprises multinationales qui fournissent des services essentiels à plusieurs Etats membres, et dont les réseaux et systèmes d'information sont déployés dans plusieurs pays. Cette situation justifie la recherche au niveau européen d'une harmonisation des règles de cybersécurité s'appliquant à ces opérateurs dans les différents Etats membres de l'Union.

Cette harmonisation doit cependant être progressive et tenir compte des différents niveaux de maturité de chaque pays en la matière. Le renforcement des capacités de chaque Etat membre doit ainsi constituer une priorité, et la France doit veiller à ce que le processus d'harmonisation ne se réalise pas au détriment du niveau des exigences de sécurité, afin de ne pas affaiblir la sécurité des acteurs français.

Renforcer le rôle des opérateurs de communications électroniques

Les opérateurs de communications électroniques qui, au travers de leurs réseaux, connectent les systèmes d'information de leurs clients au réseau mondial, et voient passer par leurs réseaux l'ensemble des flux, ont un rôle clé à jouer dans la cyberdéfense des opérateurs essentiels à l'économie et à la société.

Les cyberattaques visant les systèmes de leurs clients peuvent en effet être détectées, bloquées, analysées et traitées au niveau des réseaux des opérateurs de communications électroniques. En outre, ces acteurs sont en mesure d'identifier et d'alerter les détenteurs de systèmes d'informations vulnérables - par exemple à partir de données techniques fournies par l'ANSSI, ce qui peut permettre de limiter drastiquement les effets d'une vague d'attaques informatiques. Les opérateurs de communications électroniques doivent donc être des partenaires majeurs de l'Etat dans la lutte contre la cybermenace.

Dans cette perspective, l'ANSSI a tissé de nombreux liens de partenariat avec ces opérateurs pour améliorer le niveau de cybersécurité de leurs réseaux, notamment au travers de conseils techniques et d'audits. Toutefois, compte tenu du développement de la cybermenace, un renforcement de la coopération de l'Etat avec les opérateurs de communications électroniques afin de renforcer l'utilisation de leurs réseaux à des fins de détection et de blocage des attaques, de prévention des incidents et d'alerte des victimes, éventuellement

encadré par un nouveau cadre législatif, permettrait d'améliorer sensiblement la cybersécurité de l'ensemble des acteurs.

2.3.4. La protection des collectivités territoriales

Les collectivités territoriales s'administrent librement. L'État ne peut décider de la gouvernance de leurs systèmes d'information, et encore moins en imposer la supervision par ses services. Du fait de cette autonomie, alliée à la diversité de leurs tailles et de leurs physionomies, les collectivités s'organisent et se gèrent de manières très diverses. Leur niveau de maturité et de sensibilité aux enjeux de sécurité du numérique est donc très variable, selon les contextes économiques, culturels et, *a fortiori*, numériques.

Elles restent cependant particulièrement vulnérables face à la menace cyber.

Compte tenu du poids des collectivités territoriales dans la sphère publique, du nombre de leurs administrés, de leurs responsabilités en matière de traitement des données personnelles et sensibles ou de la prééminence de leur rôle économique, pour ce qui concerne les régions, leur cybersécurité appelle un appui, même indirect, des services de l'État. Les travaux conduits dans le programme de développement concerté de l'administration territoriale DcANT devront donc poursuivre la prise en compte des enjeux de cybersécurité et proposer des pistes pour les aider.

Encourager la mutualisation des ressources des collectivités territoriales

Les collectivités territoriales se sont déjà engagées dans la mutualisation de leurs moyens.

Qu'il s'agisse d'établissements publics de coopération intercommunale (EPCI), de syndicats mixtes ou, plus généralement, de toutes les formes d'intercommunalité, les structures qui endossent la fonction de DSI, par exemple au profit de chaque commune d'un département, ont démontré l'efficacité de la démarche. Là où existent de telles entités, les actions de sensibilisation et d'accompagnement sont plus simples à mettre en place et mieux acceptées par les adhérents. Néanmoins, l'ensemble du territoire n'est pas couvert par ces structures dédiées et l'expérience montre que les compétences sont relativement rares et mal réparties.

Plus récemment, plusieurs élus ont annoncé leur intention de mettre rapidement en place et de financer eux-mêmes des structures dédiées qui doivent assurer, notamment à l'échelon de la région, les fonctions de sensibilisation et de formation, voire de supervision des systèmes, et de réponse aux incidents. Certains envisagent même de jouer le rôle de centres de certification.

Ces initiatives permettront le regroupement des compétences en matière de sécurité des systèmes d'information et auront vocation à accompagner les collectivités territoriales dans la mise en place de leurs projets numériques, en toute sécurité et dans une relation de confiance. De tels regroupements de compétences pourront en outre servir d'observatoire concernant la maturité de protection numérique et la sensibilisation, sur la base d'indicateurs régionaux précis et partagés. Ils pourront être immédiatement identifiés comme le point de référence régional en matière de sécurité du numérique.

Les initiatives visant le développement d'activités de certification de produits ou services de sécurité au sein de ces coordinations régionales doivent cependant être découragées, dans la mesure où elles ne seraient pas cohérentes avec la démarche d'harmonisation européenne de la certification défendue par la France, et entraineraient de fait une fragmentation contreproductive de ce dispositif.

À cette dernière exception près, les services de l'État doivent accompagner ce mouvement, notamment afin que les règles de sécurité appliquées ou promues soient celles préconisées par l'ANSSI, au lieu d'être façonnées par la seule offre des prestataires.

Il est donc recommandé de soutenir la création, par les collectivités territoriales elles-mêmes, d'une coordination des ressources en cybersécurité,.

Favoriser la communication en matière de sécurité numérique avec les collectivités territoriales

Les systèmes d'information des collectivités territoriales sont les cibles d'attaques numériques nombreuses et très diverses. La réponse à ces attaques, et plus généralement aux incidents de sécurité, est très souvent rendue délicate par l'absence, au moins dans les plus petites collectivités, de points de contacts pour leurs interlocuteurs dans la sécurité numérique, notamment les services de l'État. En outre, même si ces points de contact peuvent être clairement identifiés, il est rare qu'ils puissent communiquer efficacement avec les structures spécialisées, faute de maitriser un langage commun. La remontée des incidents de sécurité qui affectent les collectivités ne peut donc, en l'état, s'opérer de manière fluide.

Par ailleurs, même si elles sont conduites par des acteurs de proximité, les actions de sensibilisation menées au profit des plus petites collectivités, et notamment de la majorité des communes, perdent une grande partie de leur efficacité en l'absence d'un relais interne apte à maitriser les enjeux de la cybersécurité.

Il est donc recommandé d'inciter et d'aider chaque collectivité territoriale, notamment les plus petites, à désigner et à former un « référent » en sécurité numérique, interlocuteur privilégié des acteurs de la cybersécurité et relais des actions de sensibilisation et de formation.

Favoriser le développement d'une offre adaptée de produits et de services

Toutes les collectivités mettent en place des services aux administrés qui leur imposent de se tourner vers des solutions clés en main externalisées, notamment de *cloud computing*, sans se préoccuper du niveau de sécurité ou de la confiance que l'on peut leur accorder. Quand la sécurité numérique est prise en compte, elle n'est que rarement intégrée dès les prémices des opérations de transformation numérique. Dans les faits, notamment en l'absence de référentiels *ad hoc*, peu de collectivités territoriales disposent de la capacité de rédiger elles-mêmes des cahiers des charges précis ou de choisir les entreprises spécialisées susceptibles de répondre à des besoins et à des exigences réglementaires très spécifiques. Les formations organisées par les collectivités territoriales au profit de leurs agents sont généralement

dispensées par des opérateurs privés, sur la base de modules existants destinés aux entreprises.

L'expérience montre que, même si l'adéquation entre l'offre des produits et services qualifiés par l'ANSSI et le besoin des collectivités territoriales n'a jamais été formellement analysée, elle semble améliorable. Il est donc recommandé d'améliorer l'intégration des besoins et des contraintes spécifiques aux collectivités territoriales dans les référentiels de l'ANSSI et dans ses catalogues de produits et services qualifiés, en menant un travail d'inventaire de ces besoins et d'analyse du marché industriel associé. Cette démarche doit être accompagnée par la mise en place d'instances de dialogue adaptées, par exemple avec certains acteurs intercommunaux, afin de favoriser dans la durée la communication de ces besoins à l'ANSSI.

2.4. Renforcer la lutte contre la cybercriminalité

Comme le précisait déjà en 2014 le propos liminaire du rapport « Protéger les internautes : rapport sur la cybercriminalité[28] », il n'existe pas, à ce jour, de définition juridique de la cybercriminalité. La première recommandation de ce rapport consistait d'ailleurs en la formulation d'une définition très englobante du terme : « *La cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet* ». Le préambule de la Convention de Budapest de 2001 (cf encadré ci-après), s'il ne définit pas ce qu'est la cybercriminalité, évoque quant à lui trois types d'activités que la convention entend couvrir : les atteintes à l'intégrité, la disponibilité ou à la confidentialité d'un système d'information ; l'utilisation des réseaux électroniques et de l'information électronique pour commettre des infractions pénales ; les atteintes aux données.

Le texte de la Convention de Budapest permet d'esquisser à grands traits une approche opérationnelle de ce que représente la lutte contre la cybercriminalité. Ainsi, des mesures de cyberdéfense sont mises en œuvre et des poursuites judiciaires éventuellement déclenchées lorsqu'un acte porte atteinte à la disponibilité, à l'intégrité ou à la confidentialité d'un système d'information et s'il met en jeu la défense ou la sécurité nationale (acte de guerre, espionnage, sabotage), la vie des populations (terrorisme), le fonctionnement de l'économie (déni de service, compromissions massives ou diffusion large de rançongiciels) ou de la société (entrave à la vie démocratique, vol massif de données à caractère personnel ou de santé). Lorsqu'en revanche l'acte n'a pas une des conséquences évoquées ci-dessus, ou lorsque le système d'information n'est utilisé que comme vecteur (phishing, ventes sur Internet de produits illégaux, diffusion sur Internet de contenus illicites, etc.), il n'entraine pas la mise en œuvre de mesures de cyberdéfense.

[28] www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

Les outils statistiques classiques ne permettent pas de dresser aisément un état des lieux précis en matière de cybercriminalité, ces crimes entrant dans différentes catégories d'infractions de droit commun sans référence explicite à l'utilisation des techniques informatiques utilisées. Complémentaires des résultats statistiques attendus de la plate-forme de lutte contre les actes de cybermalveillance[29] mise en place en 2017, les travaux engagés au sein du ministère de l'intérieur par le *Service statistique ministériel de la sécurité intérieure* (SSMSI) doivent donc se poursuivre pour améliorer la connaissance de la cybercriminalité. Il est établi néanmoins que, dans un contexte de numérisation accrue de la société, la multiplication et la sophistication grandissante des moyens dont disposent les cybercriminels (réseaux d'anonymisation tels que le réseau *Tor*, outils d'attaque disponibles sur Internet, ...) compliquent l'accès à la preuve numérique et créent les conditions d'une explosion de la cybercriminalité.

Comme le souligne le rapport publié en 2016 par EUROPOL[30], on observe cinq tendances en matière de cybercriminalité :

- le développement des rançongiciels, qui constituent aujourd'hui la première menace parmi les logiciels malveillants ;
- l'intérêt porté par certains groupes criminels aux technologies de paiement sans contact ;
- l'essor des attaques par déni de service, notamment grâce à des « botnets » d'objets connectés ;
- l'utilisation des crypto-monnaies, en particulier du *bitcoin*, comme moyen privilégié pour les échanges financiers entre criminels ;
- l'utilisation des technologies de chiffrement pour protéger les communications entre délinquants ou stocker les informations.

Ces évolutions constituent un défi important pour les services d'enquête et un défi majeur pour les acteurs judiciaires qui doivent faire face à un contentieux protéiforme exigeant parfois une véritable spécialisation.

L'analyse conduite dans le cadre de la présente revue a par ailleurs permis de mettre en lumière un mouvement de convergence entre cyberdéfense et lutte contre la cybercriminalité. Les attaques informatiques susceptibles de porter atteinte aux intérêts fondamentaux de la Nation et, plus particulièrement, aux systèmes d'information des opérateurs d'importance vitale (espionnage, vol ou modification de données, entrave,

[29] www.cybermalveillance.gouv.fr

[30] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

sabotage, etc.) constituent d'ailleurs des infractions qu'il est prévu de punir depuis la loi GODFRAIN de 1988[31].

La Convention de Budapest

La convention de Budapest sur la cybercriminalité a été élaborée sous l'égide du Conseil de l'Europe. Signé le 23 novembre 2001 à Budapest – d'où son appellation commune de « Convention de Budapest » - cette convention est le premier - et à ce jour le seul - texte international traitant exclusivement de lutte contre la cybercriminalité.

Fin 2017, la convention avait été ratifiée par 56 États (quatre États l'ont signée mais pas ratifiée), dont certains ne sont pas membres du Conseil de l'Europe comme l'Australie, les Etats-Unis, Israël, le Japon, le Maroc ou le Sénégal. Le seul membre du Conseil de l'Europe à n'avoir pas signé la convention est la Fédération de Russie.

L'objectif de la convention est de favoriser l'harmonisation des législations nationales visant les infractions pénales commises via internet et d'autres réseaux informatiques. Le texte traite à la fois d'infractions informatiques (accès illégal, interceptions illégales, atteintes à l'intégrité des données ou des systèmes, sécurité des réseaux) et d'infractions se rapportant aux contenus (pornographie enfantine, atteinte aux droits d'auteur).

La convention contient également une série de pouvoirs de procédures, tels que la perquisition de réseaux informatiques (conservation de preuves, injonction de produire, ...) et l'interception. La convention vise également à faciliter la coopération internationale des forces de l'ordre et des appareils judiciaires des États parties.

2.4.1. Evaluer plus finement l'étendue des actes de cybercriminalité

La lutte contre la cybercriminalité s'appuie en premier lieu sur une perception la plus juste possible des actes délictueux commis dans l'espace numérique. Quatre sources permettent aujourd'hui au pouvoir judiciaire de prendre connaissance des incidents et infractions cyber :

- le citoyen, qu'il soit simple internaute signalant des actes de cyberdélinquance[32] ou victime ;
- les services de police et de gendarmerie effectuant des opérations de recherche proactive auprès de sources ouvertes ;

[31] Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique.

[32] L'internaute confronté à des contenus ou à des comportements illicites sur Internet a la possibilité d'envoyer un signalement sur la plateforme PHAROS de la Direction centrale de la police judiciaire. Celle-ci reçoit près de 200 000 signalements par an qui concernent principalement des escroqueries et des contenus pédopornographiques, d'incitation à la haine ou faisant l'apologie du terrorisme.

- des partenaires de confiance, agrégateurs ou relais d'information ;
- les opérateurs de réseaux et les prestataires de services de communication électronique.

L'évaluation de l'étendue des actes de cybercriminalité est aujourd'hui altérée par deux facteurs. Tout d'abord, lorsque celle-ci émane d'un éditeur de solution de sécurité informatique, dont la viabilité économique est étroitement liée au niveau de la menace, il est légitime de s'interroger sur son objectivité. Ensuite, la police et la gendarmerie ne sont pas en mesure de recenser la totalité des faits de cybercriminalité car les infractions constatées ne couvrent qu'une partie des cybermalveillances, certaines d'entre n'étant pas détectées et toutes les victimes ne se faisant pas connaître[33].

Une meilleure évaluation de l'ampleur de la cybercriminalité devrait cependant devenir accessible dans les prochains mois grâce aux projets *PERCEV@L* de la gendarmerie nationale et *THESEE* de la police nationale. Le projet *PERCEV@L* prévoit, dans un premier temps, un processus de signalement en ligne des infractions liées aux cartes de paiement[34], suivi à terme d'un projet d'extension à la plainte en ligne. Le projet *THESEE* concerne, quant à lui, cinq modes opératoires d'escroqueries sur Internet (piratage de boîte mail, *Romance Scam* et escroquerie à la petite annonce, chantage à la *webcam*, fraude liée aux faux sites de vente et *Ransomwares*). Il a pour objet de permettre le dépôt de plainte en ligne, d'améliorer la qualité des procédures et de développer la capacité d'analyse des phénomènes.

La plateforme gouvernementale « cybermalveillance.gouv.fr » (cf encadré), dont ce n'est pas l'objet principal, joue également pour le ministère de l'intérieur et l'ANSSI un rôle de capteur des risques numériques permettant d'affiner la connaissance globale de la cybercriminalité.

La plateforme gouvernementale « cybermalveillance.gouv.fr »

La plateforme gouvernementale « cybermalveillance.gouv.fr » assume aujourd'hui un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de la population française. Elle accompagne les particuliers, les entreprises et les collectivités territoriales qui pensent être victimes d'un acte de cybermalveillance pour l'établissement d'un diagnostic précis de leur situation, la mise en relation avec les spécialistes et organismes compétents proches de chez eux (1 123 prestataires référencés fin 2017) et la mise à disposition d'outils et de publications dispensant de nombreux conseils pratiques.

[33] A cet égard, il est régulièrement observé une absence de signalement ou de dépôt de plainte par les entreprises qui craignent que cette démarche se traduise par une publicité inutile sur leur vulnérabilité et une atteinte à leur image.

[34] Un peu plus de 4,5 millions de transactions frauduleuses par cartes bancaires en France en 2016 pour un montant global de 400 M€ selon l'*Observatoire de la sécurité des moyens de paiement.*

Ce dispositif national d'assistance, animé par le groupement d'intérêt public (GIP) *Action contre la cybermalveillance* (ACYMA) et porté par une démarche interministérielle associant l'ANSSI, le ministère de l'intérieur et le secrétariat d'Etat chargé du numérique est accessible depuis octobre 2017 pour toutes les régions de France. L'expérimentation du dispositif a permis, entre mai et octobre 2017, plus de 700 mises en relation entre prestataires en cybersécurité et victimes[35].

La plateforme constitue aussi un levier contribuant à référencer et fédérer plus largement l'ensemble des outils et campagnes de sensibilisation touchant au cyber vis-à-vis du grand public sous une même signalétique.

La plateforme constitue également pour le ministère de l'Intérieur et l'ANSSI l'opportunité d'affiner la connaissance de la menace visant les systèmes d'information, par un observatoire des risques numériques.

2.4.2. Renforcer l'efficacité de la réponse judiciaire pour améliorer la lutte contre la cybercriminalité

Dans un contexte d'effritement de la frontière entre cyberdéfense et lutte contre la cybercriminalité, d'une part, et de transposition au numérique de la criminalité traditionnelle, d'autre part, le renforcement de l'efficacité de la réponse pénale constitue une priorité.

Au-delà de l'adaptation nécessaire des techniques de recueil de la preuve pénale à ce nouveau contexte, ce sont les conditions de préservation de la donnée numérique qu'il faut repenser aujourd'hui. La conservation des données et leur accès est en effet le premier enjeu pour les services de police judiciaire.

Adapter la politique pénale en matière de lutte contre la cybercriminalité

La démocratisation des techniques d'anonymisation et de chiffrement, le développement de marchés parallèles sur les *Darknets* et les évolutions technologiques rendent plus difficile l'identification des cybercriminels et obligent à repenser la manière de diligenter les enquêtes, notamment au vu du principe du procès équitable.

Une réflexion pourrait d'abord être conduite sur la pertinence d'enquêter de manière plus systématique, y compris en l'absence de plainte, lorsque les informations recueillies laissent entrevoir l'existence probable d'infractions pénales.

Ensuite, il apparaît utile d'engager une évaluation des voies et moyens susceptibles de diminuer le sentiment d'impunité qui anime un certain nombre de cybercriminels. Arrêter et condamner ceux d'entre eux qui bénéficient d'une notoriété établie et cibler les plateformes

[35] 83 % des incidents de cybermalveillance ont été déclarés comme des virus, mais 44 % d'entre eux correspondaient en fait à des attaques par *Ransomware*.

criminelles les plus populaires pourraient ainsi constituer des axes d'effort. A cet égard, les récentes opérations menées contre les sites de vente de produits stupéfiants *Alphabay*[36] et *Hansa* par EUROPOL et les autorités américaines et néerlandaises font figure d'exemple à suivre.

La France pourrait aussi amplifier ses efforts à l'international en jouant notamment un rôle moteur dans les équipes communes d'enquête (ECE) au niveau d'EUROJUST. L'exemple de l'ECE mobilisée dans l'affaire *NotPetya* doit être salué et reproduit.

Pour réaliser cette adaptation de la politique pénale en matière de lutte contre la cybercriminalité, un renforcement des ressources humaines (magistrats et enquêteurs spécialisés) apparaît indispensable. Des moyens accrus en matériel sont également nécessaires tant au niveau des services d'enquête spécialisés qu'au niveau des unités de traitement de la preuve numérique. Un effort devrait être porté sur la mise en place d'outils de veille adaptés aux différentes sources ouvertes, de capacités de déchiffrement renforcées et d'outils de captation à distance des données. Au-delà de cet aspect matériel, un cadre juridique adapté fait encore parfois défaut, comme par exemple en matière de conservation des données collectées en source ouverte en dehors d'un cadre purement judiciaire.

Améliorer la réponse judiciaire

La voie judiciaire doit être pleinement mise à contribution dans la mobilisation générale des services de l'Etat face à la cybercriminalité. A ce titre, un renforcement des moyens actuellement déployés au sein de la chaine judiciaire apparait nécessaire.

La création en 2014 de la section du parquet de Paris spécialisée en cybercriminalité[37], ainsi que la centralisation en 2016, au niveau du tribunal de grande instance (TGI) de Paris, de la compétence en matière d'atteintes aux systèmes informatisés de données vont dans le sens d'une meilleure coordination de la réponse judiciaire à la cybercriminalité. Pour autant, un renforcement des effectifs du Parquet et du TGI de Paris apparait nécessaire, tout comme ceux des TGI de Nanterre et de Pontoise qui seront vraisemblablement impactés par les projets *THESEE* et *PERCEV@L*.

Rapprocher les acteurs de la lutte contre la cybercriminalité et ceux de la cyberdéfense

L'adaptation de la politique pénale aux enjeux de la cybercriminalité doit aller de pair avec un effort de formation cyber au profit des procureurs, des juges et des enquêteurs impliqués. Il apparaît notamment indispensable de mieux sensibiliser, dans le cadre de leur formation initiale et continue, les magistrats et enquêteurs aux besoins de la chaîne cyber. De façon réciproque, une meilleure information des personnels de cette chaîne aux enjeux de la lutte

[36] Supermarché en ligne de drogue et d'armes dans le *Darkweb* qui a, selon EUROPOL, brassé depuis 2014 pour plus d'un milliard de dollars de transactions délictueuses.

[37] Cette section est armée par deux magistrats et un assistant spécialisé.

contre les cybercriminels et aux interactions à entretenir avec les acteurs judiciaires est également nécessaire.

Plus globalement, il apparait nécessaire de développer les échanges entre les acteurs judiciaires et les spécialistes du domaine cyber. Une réflexion pourrait ainsi être lancée sur la mise en place d'un cadre juridique autorisant le partage réciproque de certaines informations collectées par les autorités judiciaires ou les services spécialisés en cyberdéfense.

La présente revue recommande ainsi de permettre un transfert des éléments techniques récupérés dans les enquêtes judiciaires vers l'ANSSI dans une logique de capitalisation de données techniques sur les menaces, et depuis l'ANSSI vers les services opérationnels pour faciliter les actes techniques d'investigation et la compréhension de la menace.

Rendre les interventions territoriales plus efficaces

Dans le cadre de l'intelligence économique, une coordination entre les différents services de l'Etat concernés est aujourd'hui réalisée au niveau déconcentré sous l'égide des préfets de région. Les *Comités régionaux d'intelligence économique et territoriale* (CRIET) répartissent ainsi les actions de sensibilisation aux risques - parmi lesquelles les actions de sensibilisation au risque cyber - menées au profit des acteurs économiques. Une meilleure planification des interventions conduites dans les domaines de la lutte contre la cybercriminalité et de la cybersécurité permettrait aux CRIET de gagner en efficacité.

Ce point rejoignant le besoin déjà identifié de regrouper les compétences pour sécuriser les systèmes des acteurs territoriaux, la revue recommande que soit étudiée la création d'entités régionales de cyberdéfense.

2.4.3. Développer un réseau international de collaboration entre magistrats et enquêteurs

La cybercriminalité ne reconnaissant pas les frontières entre les Etats, il ne suffit pas que la France seule soit bien préparée pour y faire face. Des données utiles à l'orientation des enquêtes sont en effet détenues par des acteurs étrangers. Dès lors, la France doit s'efforcer de perfectionner avec ses partenaires les mécanismes d'entraide judiciaire en matière de lutte contre la cybercriminalité et poursuivre les échanges d'expérience et de technologies dans ce domaine.

Dans cette logique, il apparait essentiel d'encourager un dialogue effectif et constructif, notamment avec les grands opérateurs américains de l'Internet[38], et d'entretenir un réseau international de collaborations policières et judiciaires.

Le groupe de contact permanent, qui réunit les enquêteurs et la chancellerie avec les grands acteurs de l'Internet apporte une première réponse à cette exigence en permettant un dialogue technico-opérationnel. En matière de coopération policière et judiciaire, des

[38] Le dialogue n'exclut pas lorsque cela s'avère nécessaire, d'envisager des contraintes législatives - européenne ou nationale.

contacts bilatéraux, notamment avec les pays sources de cybercriminalité, et des échanges avec les services compétents des différents Etats au sein des instances européennes ou internationales (EUROPOL, EUROJUST, INTERPOL) existent et démontrent régulièrement leur intérêt. Mais, outre le partage d'informations, l'objectif est aussi la définition d'approches et de solutions partagées, sinon communes. C'est le cas par exemple des travaux européens menés dans le domaine de la disponibilité et de l'accès à la preuve numérique. L'accès à la preuve numérique représente aujourd'hui un défi qui doit être relevé grâce à une meilleure coopération avec les grands opérateurs de l'internet mais aussi avec les autorités nationales concernées. Les décisions prises en matière de définition de la localisation des données seront déterminantes à cet égard.

Les contacts avec les entreprises du net au niveau national ou dans un cadre international (Union européenne, G7, ONU) doivent permettre d'amener les entreprises à mieux prendre en compte nos besoins en matière de retrait des contenus à caractère illicite et en particulier les contenus d'apologie du terrorisme. Nos partenaires du secteur doivent aussi être mobilisés concernant l'utilisation de nouvelles technologies pour le financement du terrorisme.

Le caractère résolument technique et transfrontalier de la cybercriminalité implique une mobilisation et un effort constant afin de donner aux acteurs de la chaîne pénale tous les moyens utiles au développement des enquêtes, à l'identification et à l'interpellation des auteurs, fussent-ils en dehors du territoire national. L'accès transfrontalier à la preuve numérique - très souvent détenu par des opérateurs étrangers - est ainsi un enjeu essentiel pour le bon développement des enquêtes pénales. Cet accès doit être amélioré afin de permettre l'obtention en quelques heures des données techniques et en quelques jours des données de contenus (contre respectivement plusieurs jours et parfois plusieurs mois actuellement).

Enfin, la France doit poursuivre la promotion de la coopération internationale en matière de lutte contre la cybercriminalité en apportant un soutien démonstratif et entrainant à la Convention dite de Budapest. Dans cette perspective, la présente revue recommande de moderniser la transposition de la Convention de Budapest en ce qui concerne les mesures de coopération, notamment pour les rendre possibles lorsqu'aucune enquête judiciaire n'est ouverte en France. En particulier, la transposition en droit français des articles 29 et 30 de la convention, relatifs aux gels des données numériques, n'est pas adéquate ; les demandes de gel n'entrant pas dans le cadre judiciaire (le gel des données n'est pas encadré en droit français), elles ne peuvent faire l'objet de réquisitions telles que prévues par le texte français. Elle recommande, d'autre part, l'identification des dispositions de la Convention de Budapest susceptibles d'être portées en droit international, au-delà des objectifs de politique pénale poursuivi par la convention. La France est opposée à la négociation d'un nouvel instrument juridique international.

2.5. L'action internationale de la France dans le domaine cyber

A l'heure où les capacités cyber des États varient considérablement, la France doit se positionner comme un acteur de référence, chef de file au sein de l'Union européenne. Cette stratégie d'influence doit conduire à promouvoir le modèle français et à participer activement à la définition des normes cyber au niveau européen et international. Cette stratégie doit être menée au sein de l'Union européenne, de l'Alliance atlantique, à l'Organisation des Nations Unies et dans les diverses instances multilatérales qui leurs sont rattachées mais aussi au travers de coopérations bilatérales privilégiées. Cette démarche d'influence suppose en contrepartie d'accepter de porter assistance à un allié proche victime d'une cyberattaque d'ampleur. Cet appui doit notamment pouvoir être offert à nos partenaires européens sans que la France ne se substitue aux prérogatives et aux responsabilités des Etats secourus. Par ses positions publiques, la France peut exprimer sa volonté de contribuer à la stabilité stratégique d'un cyberespace de paix et de prospérité.

La présente revue préconise tout d'abord de renforcer notre dialogue et les coopérations avec nos alliés et partenaires pour prévenir les crises cyber (2.5.1). Elle présente ensuite plusieurs propositions visant à mieux garantir la sécurité et l'autonomie stratégique européenne dans l'espace numérique (2.5.2.). Elle propose l'adoption d'un schéma de classement des attaques informatiques et d'une doctrine d'action (2.5.3.). Elle analyse, enfin, les conditions d'une meilleure régulation du cyberespace (2.5.4.).

2.5.1. Renforcer le dialogue et les coopérations avec nos alliés et partenaires pour prévenir les crises cyber

Le renforcement de la protection, de la résilience et de la coopération de l'ensemble des acteurs du cyberespace participe de manière directe au renforcement de notre sécurité nationale. La France doit aujourd'hui accroître ses efforts à l'international et continuer à développer ses dialogues bilatéraux sur ces questions en vue de consolider la stabilité du cyberespace et la résilience de l'ensemble des Etats face aux crises cyber.

La France doit nouer des relations stratégiques bilatérales et développer les canaux d'un dialogue franc et ouvert avec les principaux acteurs du cyberespace. Ces échanges offrent aussi bien l'opportunité de suivre et d'organiser au niveau stratégique les travaux d'intérêt commun que d'améliorer la compréhension de l'organisation et de la stratégie de ces pays, de préciser les positions françaises sur les grands sujets cyber et de partager des informations sur d'éventuels incidents.

Ces contacts, et de manière plus large, nos relations stratégiques bilatérales dans le domaine cyber, répondent à trois impératifs :

- la franchise du dialogue, y compris s'agissant de la menace émanant, le cas échéant, de notre interlocuteur ;
- la mise en place de canaux d'échange dédiés, qui permettront notamment le contrôle de l'escalade en cas de crise ;

- l'acceptation mutuelle de limites à ne pas franchir sur le plan bilatéral, comme, par exemple, s'interdire certaines pratiques identifiées comme néfastes par les deux interlocuteurs.

La France conduit déjà, sous la coordination du ministère de l'Europe et des affaires étrangères, un certain nombre de dialogues bilatéraux sur les questions de cybersécurité (avec les Etats-Unis, la Chine, l'Inde, le Brésil et le Japon notamment). Ces échanges doivent bien évidemment être poursuivis et, si nécessaire, approfondis.

S'agissant de nos coopérations structurelles, techniques et opérationnelles, elles sont des instruments stratégiques concourant de manière directe et indirecte à consolider notre sécurité nationale et notre influence. Ces coopérations sont un atout à plusieurs titres. Elles permettent tout d'abord d'élever le niveau général de la sécurité du cyberespace et d'en renforcer la stabilité via l'amélioration des capacités et de la résilience de pays alliés et partenaires, ainsi que des organisations internationales auxquelles nous appartenons. Elles contribuent également à améliorer notre capacité à faire face à une crise cyber de dimension internationale qui toucherait la France ou l'un de nos partenaires. Elles sont enfin un vecteur efficace pour promouvoir l'offre et l'expertise française en matière de cybersécurité, pour faire connaître notre organisation nationale et pour nous maintenir à l'état de l'art en se confrontant à nos pairs et en apprenant d'eux. Ces coopérations participent ainsi à la diffusion de notre vision politico-diplomatique et juridique concernant la régulation et le comportement responsables des acteurs dans le cyberespace.

Dans le domaine cyber, les priorités géographiques de la France dépendent en grande partie du type de coopération envisagée (opérationnelle, technique, structurel, etc.) et de l'acteur institutionnel qui sera amené à la mettre en œuvre (ANSSI, ministère de l'intérieur, ministère des armées, ministère de l'Europe et des affaires étrangères, etc.). Bien entendu, nos partenaires européens et occidentaux, avec qui les échanges et les coopérations sont aujourd'hui approfondis et réguliers, demeurent des associés privilégiés. Certaines zones sont par ailleurs prioritaires comme l'Afrique subsaharienne, notamment les pays francophones, l'Afrique du Nord, ainsi que certains pays du Moyen-Orient et d'Asie du Sud et de l'Est.

Il est important que les coopérations entretenues par les différentes entités gouvernementales soient coordonnées et cohérentes avec leurs périmètres de responsabilité respectifs. En outre, les différentes actions menées doivent être complémentaires afin de pouvoir proposer à certains de nos partenaires une offre française de coopération globale.

Outre le travail réalisé avec nos partenaires et alliés étatiques, la France doit contribuer à renforcer la cybersécurité des organisations internationales dont elle est membre, notamment celles qui ont à traiter d'informations essentielles à notre autonomie stratégique, au premier rang desquelles l'Union européenne et l'OTAN.

Ces actions de coopération, en particulier lorsqu'elles sont opérationnelles, nécessitent de mobiliser des ressources publiques rares et limitées au regard des besoins humains, techniques et financiers. Pour dépasser cet obstacle, plusieurs pistes peuvent dès à présent

être explorées, notamment la mobilisation des réservistes, la sollicitation d'acteurs de confiance non étatiques (opérateurs, universités, secteur privé, etc.) et, enfin, le fait de privilégier la « formation de formateurs ».

L'école nationale à vocation régionale sur les enjeux cyber de Dakar

La France supportera, en partenariat avec le Sénégal, l'ouverture à Dakar, d'ici la fin de l'année 2018, d'une école nationale à vocation régionale (ENVR) sur les enjeux cyber. Ce projet sera bâti en relation étroite avec notre partenaire sénégalais, ainsi qu'avec les pays de la région, afin de définir ensemble les besoins spécifiques de l'Afrique de l'Ouest dans ce domaine. Elle sera une école d'un nouveau genre. Son champ d'expertise pourrait être très large, allant de la gouvernance et de la régulation internationale du numérique, jusqu'à des aspects plus pratiques, voire opérationnels, couvrant les besoins des décideurs publics et privés. La souplesse d'organisation de ses cours devrait permettre de répondre aux besoins de formations, tant longues que courtes, dans un secteur où les connaissances évoluent très rapidement. S'appuyant sur l'expérience de la *Direction de la coopération de sécurité et de défense* (DCSD) du ministère de l'Europe et des affaires étrangères en matière de création d'écoles régionales dont la qualité d'enseignement est reconnue, cette école devra enfin pouvoir délivrer un enseignement labellisé qui conduira à combiner, dans le tour de table initial, des partenaires régaliens, universitaires voire privés.

2.5.2. Garantir la sécurité et l'autonomie stratégique européenne dans l'espace numérique

Au sein de l'Union européenne, la France cherche à promouvoir le meilleur équilibre entre autonomie stratégique européenne pour la sécurité du numérique et maintien de ses prérogatives souveraines en la matière, dans une logique de subsidiarité et de respect des compétences des Etats en matière de sécurité nationale.

L'objectif d'autonomie stratégique européenne est le gage de notre capacité collective d'initiative et d'action. Alors que la cohésion de l'Union européenne est fragilisée et que des interrogations ont été soulevées sur la crédibilité des alliances, la prise de conscience d'intérêts de sécurité partagés progresse, tout comme l'ambition de disposer de moyens d'action plus autonomes.

Cet objectif s'applique pleinement aux enjeux de sécurité au sein de l'Europe numérique et se décline en trois axes.

Le premier axe est technologique et sera détaillé dans la troisième partie de cette revue. La politique industrielle de l'Union européenne est un vecteur important pour soutenir des capacités de recherche et développement de pointe afin de favoriser le déploiement de technologies et de services numériques de sécurité de confiance, dont la fiabilité doit pouvoir

être évaluée. L'intégration de la sécurité dans l'ensemble des composantes numériques permettra également de donner un avantage concurrentiel aux offres européennes.

Le deuxième axe est réglementaire. Par sa politique extérieure, l'Union européenne doit chercher à maintenir sa capacité à définir des réglementations qui prennent en compte les exigences de compétitivité et les potentialités du numérique mais qui restent protectrices des citoyens, des entreprises, des Etats-membres, conformément à nos valeurs communes (droit à la vie privée et protection des données à caractère personnel, protection des infrastructures critiques).

Le troisième axe, enfin, est capacitaire. L'Union européenne a un rôle essentiel pour la promotion et le soutien du développement de capacités de cyberdéfense des entités publiques et privées au sein des Etats membres, en s'appuyant sur des savoir-faire européens. Cette nécessité concerne aussi les institutions européennes elles-mêmes (Commission, Parlement, etc.) qui ont à se protéger contre d'éventuelles attaques.

Dans ce contexte, la France doit continuer à défendre le renforcement de la cyber-résilience de l'espace européen (mise en œuvre de la directive NIS, coopération pour le traitement des crises cyber de grande ampleur, cybersécurité des institutions et agences de l'Union européenne, etc.) et à promouvoir une politique industrielle européenne en la matière (partenariat public-privé pour la cybersécurité, nouveaux investissements dans les technologies numériques d'avenir, dites « de rupture », etc.). Il est par ailleurs essentiel d'œuvrer à une meilleure prise en compte de la cyberdéfense au sein de la politique de sécurité et de défense commune (projets de l'agence européenne de défense, cursus communs de formation, procédures et moyens pour intégrer le fait cyber aux opérations de l'Union européenne, etc.). La France doit, enfin, mettre en œuvre des moyens de réponse diplomatique aux crises cyber à l'échelle européenne.

Au-delà de ces différentes dimensions, il apparaît aujourd'hui nécessaire de renforcer la coopération opérationnelle entre les 28 Etats membres de l'Union européenne. En effet, si les exercices *CyberEurope*, organisés par l'ENISA (l'agence européenne chargée de la sécurité des réseaux et de l'information) depuis 2010, ont permis aux Etats membres de tester leur collaboration en cas de crises cyber, la coopération opérationnelle en cas d'incidents reste en revanche embryonnaire. Elle se structure toutefois progressivement depuis le lancement du réseau européen des *Computer Security Incident Response Teams* (CSIRTs) en 2017.

De nombreux Etats membres, qui connaissent des difficultés pour développer leurs propres capacités, souhaitent que l'Union européenne joue un rôle accru en appui aux Etats victimes de cyberattaques. La Commission européenne, de même que l'ENISA et certaines agences sectorielles qui pourraient être amenées à intervenir dans ce domaine, sont particulièrement réceptives à ces attentes.

Ce contexte pourrait conduire à un renforcement des obligations des Etats membres en matière de partage d'informations et à l'établissement d'une capacité opérationnelle supranationale au sein de l'Union européenne.

Ces propositions doivent continuer à faire l'objet d'une vigilance particulière, compte tenu des enjeux de souveraineté associés. La France, à ce stade et compte tenu des principes de souveraineté et de subsidiarité, considère que dans ce domaine les échanges opérationnels doivent se faire sur la base de coopérations volontaires et souhaite éviter l'émergence d'une capacité européenne autonome, redondante et compétente pour intervenir au sein des Etats membres en matière de réponse à incident. Elle promeut cependant l'approfondissement de la coopération volontaire entre les Etats membres, notamment à travers le réseau européen des CSIRTs. La France doit s'associer pleinement et apporter son soutien à toutes les initiatives qui pourraient contribuer à répondre à ce besoin croissant de coopération face à des attaques d'ampleur européenne, dans le respect de la compétence des Etats.

Cette démarche doit s'appuyer sur quatre principes :

- le maintien d'une posture claire sur la répartition des compétences et la préservation de la souveraineté nationale en matière opérationnelle ;
- le renforcement des capacités cyber des Etats ;
- le développement de la coopération opérationnelle au sein de l'Union européenne ;
- la promotion d'un modèle adapté d'assistance aux Etats en cas d'incident, qui soutienne notamment un secteur privé européen de confiance fournissant des services de cybersécurité mobilisables en cas de crise.

Une déclinaison de cette démarche en actions opérationnelles est proposée en annexe 9.

2.5.3. Définir une doctrine d'action

La présente revue préconise l'établissement d'une doctrine d'action. Des options de réponses à une attaque cyber doivent être préparées en avance afin de permettre aux autorités de réagir dans le tempo de la crise. S'interroger sur la pertinence de l'adoption d'une doctrine d'action nécessite toutefois au préalable de renforcer notre capacité de discrimination des incidents et agressions au regard de nos intérêts nationaux.

Adopter un schéma de classement des attaques informatiques

Aujourd'hui, en effet, il n'existe pas de schéma de classement des incidents et attaques qui soit utilisable au niveau national et encore moins de façon reconnue par tous au niveau international.

Or, pour prendre une décision politique, les autorités doivent pouvoir s'appuyer sur un schéma de classement des attaques informatiques qui ne doit, en aucune façon, devenir l'élément déclencheur d'une réponse automatique. Afin de pouvoir réagir de manière appropriée à un incident cyber, tout Etat doit en effet d'abord analyser et caractériser cet événement. Les effets des attaques informatiques sont complexes, variés et ne peuvent faire l'objet d'un recensement exhaustif. Pour permettre une réponse adaptée et proportionnée, il est nécessaire de s'appuyer sur une compréhension rapide de l'attaque, complétée par la conduite d'analyses plus approfondies sur le mode opératoire et les techniques employées.

Les États-Unis ont rendu public un tel schéma de classement mais ce dernier n'est pas directement transposable.

<table>
<tr><th>Echelle de gravité</th><th>Equivalence avec l'échelle CISS USA</th><th>Caractérisation de l'impact</th><th>Caractérisation comme agression armée au sens de l'article 51 de la Charte des Nations-Unies</th></tr>
<tr><td>Niveau 5 - Situation d'urgence extrême</td><td>Level 5 Emergency (Black)</td><td>Impact extrême</td><td>Probablement possible : à examiner au cas par cas.</td></tr>
<tr><td>Niveau 4 - Crise majeure</td><td>Level 4 Severe (Red)</td><td>Impact majeur</td><td rowspan="6">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.).</td></tr>
<tr><td>Niveau 3 - Crise</td><td>Level 3 High (Orange)</td><td>Impact fort et étendu</td></tr>
<tr><td>Niveau 2 - Incident grave</td><td>Level 2 Medium (Yellow)</td><td>Impact fort et circonscrit</td></tr>
<tr><td>Niveau 1B - Incident</td><td rowspan="2">Level 1 Low (Green)</td><td>Impact significatif et circonscrit</td></tr>
<tr><td>Niveau 1A - Evénement significatif</td><td>Impact faible</td></tr>
<tr><td>Niveau 0 - Evénement</td><td>Level 0 Baseline (White)</td><td>Impact négligeable</td></tr>
</table>

Schéma national de classement des attaques informatiques

Ce schéma de classement, compatible avec le schéma américain, intègre les normes juridiques nationales (code pénal, code de la défense, etc.) et internationales (règlement général sur la protection des données, Charte des Nations Unies, droit international humanitaire, etc.). Il présente quatre avantages : il permet de partager une vision commune et synthétique, d'accélérer la compréhension de la situation engendrée par l'attaque informatique, de faciliter la prise de décision s'agissant des réponses potentielles à y apporter et, au-delà de son usage à l'échelle nationale, de favoriser la collaboration internationale en cas d'incident.

Il est fondé essentiellement sur les effets induits par l'incident. Parmi les éléments qu'il revient de prendre en compte, on peut notamment mentionner les effets néfastes constatés, directs et indirects, produits par l'attaque, les effets néfastes prévisibles d'une attaque non

terminée, d'une menace ou d'une attaque imminente, et l'urgence à apporter une réponse, et, enfin, les aspects techniques, notamment le caractère innovant des vecteurs d'attaque.

Afin de caractériser plus précisément la gravité de tout incident, au moins cinq critères complémentaires aux effets induits doivent pris en compte, à savoir un critère d'intentionnalité (l'intention derrière l'attaque), un critère de dangerosité (la nature des cibles), un critère d'attribution (la nature de l'attaquant), un critère de massivité ou de volumétrie (la relation de l'incident avec d'autres incidents) et un critère de récurrence (la répétition d'une attaque).

Enfin, la gravité de l'incident doit être appréhendée en fonction de l'atteinte portée à quatre réalités :

- les intérêts fondamentaux de la Nation, sa souveraineté et à sa démocratie (atteinte aux Institutions et à la démocratie, atteinte à la continuité de l'action de l'Etat et de l'action gouvernementale, atteinte à l'intégrité du territoire national, atteinte à la sécurité des forces armées, atteinte aux capacités de dissuasion nucléaire, atteinte au secret de la défense nationale, atteinte à la capacité de tenir les engagements internationaux) ;
- la sécurité intérieure et civile ;
- la population et l'environnement (atteinte à la santé de la population, atteinte à la vie quotidienne, atteinte aux infrastructures civiles essentielles - réseaux de distribution d'eau, d'électricité, etc. -, atteinte aux besoins élémentaires de la population, atteinte à la confiance de la population dans la capacité des pouvoirs publics, atteinte à l'environnement) ;
- l'économie.

Ce schéma constituera à la fois un outil d'aide à la décision pour les autorités, un élément fondamental d'une doctrine d'action pour la France, et un support favorisant la coopération internationale. Un tel schéma ne permettra cependant jamais, à lui seul, de régler les questions d'évaluation et de caractérisation d'une attaque cyber, qui précèdent une attribution relevant *in fine* d'une décision de nature politique à prendre au cas par cas.

Définir des options de réponse aux incidents cyber

La France, comme chaque Etat, dispose d'un large panel de réponses possibles, de nature militaire ou non, à un incident ou une attaque informatique. Ces options, qui sont parfois cumulables, peuvent répondre à des logiques, bases juridiques et objectifs différents. Certaines pourront être menées de concert avec nos partenaires, d'autres resteront purement nationales. Dans tous les cas, elles ne pourront être prises que sur la base d'une décision entièrement souveraine, fondée sur une évaluation nationale et indépendante de la menace ou de l'attaque à laquelle elle a pour objet de répondre.

Ces mesures sont de plusieurs ordres en fonction de la gravité de l'événement et de sa caractérisation juridique. La France doit tout d'abord s'efforcer d'avoir recours à des

mécanismes de coopération internationale et de règlement pacifique des différends. La France dispose d'une vision claire, spécifique et précise de l'application du droit international dans le cyberespace, présentée dans l'encadré ci-dessous.

L'application du droit international dans le cyberespace

Ainsi que le groupe des experts gouvernementaux de l'ONU (GGE) a pu le conclure dans son rapport publié en 2013, les principes et règles de droit international s'appliquent aux comportements des Etats dans le cyberespace. Si le cyberespace présente des spécificités propres (anonymat, rôle des acteurs privés), le droit international offre toutefois les moyens nécessaires pour encadrer de manière responsable le comportement des Etats dans cet environnement. A cet égard, le défaut d'attribution ne saurait constituer un obstacle définitif à l'application du droit international existant, d'autant que ce dernier offre des moyens d'action neutres quant à celle-ci. Le principe de souveraineté s'applique au cyberespace. A ce titre, la France réaffirme qu'elle exerce sa souveraineté sur les systèmes d'information, les personnes et les activités cyber sur son territoire, dans les limites de ses obligations découlant du droit international. Le champ des mesures que la France pourrait adopter pour réagir à une attaque informatique dont elle serait victime est fonction de la gravité de celle-ci. Plus la cyberattaque sera grave, plus le champ des mesures sera large. Une attaque informatique majeure visant la France, eu égard aux graves dommages qu'elle causerait, pourrait constituer une « agression armée », au sens de l'article 51 de la Charte des Nations Unies, et justifier ainsi l'invocation de la légitime défense. La caractérisation d'une attaque informatique en tant qu'« agression armée », au sens de l'article 51 de la Charte des Nations Unies, relèvera d'une décision politique au cas par cas. Cette décision pourra prendre en compte, notamment, les paramètres suivants :

- Une agression armée, est un usage de la force défini comme tel en raison de sa gravité et de ses effets. Il s'agit d'un emploi de la force armée par un Etat contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un autre Etat.
- L'Etat victime pourrait ainsi qualifier une attaque informatique d'agression armée, en raison de pertes en vies humaines substantielles ou de dommages physiques aux biens considérables. Dans une telle hypothèse, l'Etat serait victime d'une attaque informatique causant des dégâts et/ou des victimes similaires à ceux qui résulteraient de l'utilisation d'armes classiques.
- Une seconde hypothèse pourrait être celle d'une attaque informatique visant un Etat, qui semblerait constituer la première étape d'une intervention militaire massive plus classique.
- Il ne peut par ailleurs être exclu qu'une série d'attaques, dont chacune prise isolément n'équivaudrait pas à une agression armée, puisse être qualifiée comme telle, l'accumulation des attaques atteignant un seuil de gravité suffisant pour permettre la qualification d'agression armée.

En dessous du seuil de l'agression armée, qui représente la forme la plus grave d'usage de la force, et au-dessus de celui à partir duquel un cyber-incident est considéré comme un fait internationalement illicite, il convient de distinguer différents seuils de gravité :

- Certaines attaques pourraient ainsi ne pas atteindre le seuil de l'emploi de la force interdit à l'article 2, paragraphe 4 de la Charte des Nations Unies. Ces attaques pourraient tout de même être contraires au principe de non-intervention, ainsi qu'à d'autres règles spécifiques du droit international et ouvrir ainsi la voie à un engagement de la responsabilité internationale de l'Etat responsable de l'attaque et à la possibilité pour l'Etat victime de prendre des contre-mesures pacifiques où d'autres moyens de rétorsion en réponse et, dans certains cas, de saisir le Conseil de Sécurité ;
- En cas d'attaques atteignant le seuil de l'emploi de la force au sens de l'article 2, paragraphe 4 de la Charte, mais n'atteignant pas le seuil d'une agression au sens de l'article 51 de la Charte, les options de réponse de l'Etat victime doivent demeurer pacifiques, conformément à la théorie des contre-mesures. En fonction de la gravité du préjudice, l'Etat victime est toutefois fondé à sanctionner d'autant plus gravement l'Etat commanditaire.

L'adoption de contre-mesures est licite si les conditions suivantes sont réunies :

- L'action de l'Etat victime est conduite en réponse à un fait internationalement illicite initial (y compris un usage de la force), et a pour unique but la cessation de celui-ci ;
- L'action de l'Etat victime est nécessaire et proportionnée à cet objectif, et doit rester pacifique (en dessous du seuil du recours à la force).

La violation d'une obligation internationale par un autre Etat, créant dès lors un fait internationalement illicite, pourrait se manifester :

- par « action » : dans les cas où l'Etat dans lequel est située l'infrastructure d'où émane l'attaque est lui-même le commanditaire. L'Etat commanditaire engage à ce titre sa responsabilité internationale et s'expose à des contre-mesures. De même, une cyberattaque émanant d'acteurs non-étatiques pourra engager la responsabilité internationale d'un Etat si l'Etat exerce une forme de contrôle sur les auteurs de l'attaque ;
- par « omission » : en vertu de l'obligation de diligence raisonnable, qui est un principe de droit international coutumier, tout Etat a l' « obligation de ne pas laisser sciemment utiliser son territoire aux fins d'actes contraires aux droits d'autres Etats ». Un Etat qui n'aurait pas rempli cette obligation (de moyens) pourrait ainsi, dans certain cas engager sa responsabilité et être l'objet de contre-mesures par l'Etat victime, même s'il n'est pas le commanditaire. Pour faire jouer cette hypothèse, il convient néanmoins de notifier au préalable à l'Etat que ses infrastructures sont utilisées à des fins malveillantes (critère de connaissance) et de s'assurer que l'Etat n'a pas rempli son obligation (de moyens) de faire cesser l'attaque. Une telle situation pourrait par exemple

se caractériser par le silence complet d'un Etat saisi d'une requête d'assistance, où le refus de coopérer en vue de résoudre l'incident ou de mettre un terme à l'attaque.

Compte-tenu des spécificités du vecteur cyber (une attaque peut se préparer clandestinement et être mise en œuvre très rapidement ; les dégâts peuvent être considérables sur tous les plans, humains, financiers, organisationnels), la France ne peut exclure de recourir, dans des circonstances exceptionnelles, à la légitime défense contre une agression armée non encore déclenchée mais sur le point de l'être, de façon imminente et certaine, pourvu que l'impact potentiel de cette agression soit suffisamment grave. Dans le cadre d'un conflit armé, la planification et la conduite d'opérations cyber pouvant être considérées comme des « attaques » au sens du *jus in bello* (ou droit international humanitaire) seront soumises à celui-ci. Les grands principes de ce droit sont la nécessité, la proportionnalité, la distinction et l'humanité. Au-delà des grands principes généraux, il revient de trancher les questions opérationnelles qui se posent au cas par cas, sur le fondement de faits précis et avérés. Dans cette analyse, les éléments suivants devront en particulier être pris en compte :

- Les armes cyber doivent pouvoir être utilisées de manière discriminante : les concepteurs de l'arme cyber doivent veiller à ce que celle-ci puisse être dirigée vers une ou plusieurs cibles explicitement désignées, tout en veillant à minimiser les effets négatifs sur d'autres entités que la cible désignée. C'est une condition au respect des principes de proportionnalité et de distinction ;
- La population civile et les biens de caractère civil ne doivent pas être l'objet d'attaques, sauf si les civils participent directement aux hostilités, et que les biens de caractère civil ont perdu leur protection en devenant des objectifs militaires ;

La neutralité des Etat non parties aux conflits doit être respectée : si le simple transit d'une attaque cyber par les infrastructures d'un Etat non partie au conflit armé semble pouvoir être toléré en droit international humanitaire, en revanche l'utilisation des infrastructures de cet Etat comme infrastructure d'attaque est contraire au droit international.

Si la situation le nécessitait, il serait alors possible de prendre des mesures de rétorsion, de recourir à des mécanismes exceptionnels d'autoprotection et/ou d'adopter des contre-mesures pacifiques. Les cas les plus graves pourraient nécessiter une réponse constitutive d'un recours à la force. Les principales options de réponse aux incidents cyber sont présentées en annexe 8.

2.5.4. Réguler le cyberespace

La France doit être à l'initiative pour promouvoir la stabilité stratégique du cyberespace et sa vision de l'application du droit international existant dans ce domaine (droit applicable au temps de paix et droits des conflits armés). Cette démarche est à compléter par l'identification et la promotion de nouvelles normes de comportement responsable des Etats dans le cyberespace. Il s'agit donc de s'accorder sur des options de régulation ou de normes

internationales informelles permettant de préserver nos valeurs et nos intérêts en décourageant les actions informatiques offensives les plus déstabilisatrices.

La France doit défendre sa vision d'un espace numérique sûr, libre et ouvert au sein des différentes enceintes et organisations internationales auxquelles elle participe ainsi qu'auprès de ses partenaires étatiques mais aussi dans de nouveaux formats qui restent à définir, incluant, le cas échéant, le secteur privé.

Nous présentons tout d'abord les règles et normes applicables aux Etats et les évolutions envisageables pour ces dernières, avant de nous intéresser aux règles et normes afférentes à la responsabilité des acteurs privés dans la sécurité du cyberespace.

Les règles et normes applicables aux Etats

Les différents cycles de négociation conduits dans le cadre du Groupe gouvernemental d'experts (GGE) de l'Organisation des Nations Unies (ONU) sur la cybersécurité ont permis des avancées sensibles en matière de régulation internationale.

La France a également eu l'occasion, avec plusieurs de ses partenaires, d'affirmer sa position en faveur de la reconnaissance claire et univoque de la licéité des moyens de réponse à une cyber-attaque, qu'ils impliquent un recours à la force (légitime défense) ou non (contre-mesures, mesures de rétorsion, etc.), et de l'applicabilité du droit international humanitaire aux opérations cyber conduites dans le cadre de conflits armés.

L'échec du cycle de négociations 2016-2017 du GGE ne mettra pas un terme aux efforts de la France pour promouvoir au niveau international des normes de comportement et mesures de confiance en faveur de la stabilité et de la sécurité du cyberespace.

Si les négociations ont achoppé sur la question de l'applicabilité du droit international au cyberespace, la France était malgré tout parvenue à susciter un consensus de l'ensemble des experts sur plusieurs de ses propositions de principes pour une régulation du cyberespace. Un accord avait notamment été trouvé concernant le contrôle des exportations d'outils et techniques cybernétiques offensifs ou l'interdiction faite aux acteurs non-étatiques, dont les entreprises privées, de conduire des activités offensives dans le cyberespace pour eux-mêmes et pour le compte d'autres acteurs non-étatiques. La proposition de réaliser un suivi de la mise en œuvre des normes de comportement et des mesures de confiance déjà agréées avait également suscité un large intérêt auprès des représentants du GGE.

Ainsi, la France continuera à œuvrer à l'universalisation de certaines normes applicables dans le cyberespace en vue d'en renforcer la sécurité. Cette démarche s'articule autour de trois principes : la prévention, la coopération, la stabilité.

- *Afin de renforcer la résilience dans et de l'espace numérique : le principe de prévention*

L'incertitude intrinsèquement liée à l'attribution d'une cyberattaque doit encourager les Etats à faire porter leurs efforts sur des mesures préventives, permettant de réduire leur vulnérabilité.

Les trois piliers défensifs sur lesquels repose le modèle français en matière de cybersécurité (un cadre réglementaire national pour la protection des infrastructures critiques ; un haut niveau d'exigence en matière de sécurité des systèmes et des données ; une séparation organique entre activités de renseignement et de cybersécurité) mériteraient, au regard de leur effet stabilisateur, d'être diffusés au niveau international. Les Etats choisissant d'adopter ce modèle seraient ainsi en particulier amenés à mettre en place une organisation institutionnelle permettant de gérer de façon responsable les vulnérabilités découvertes.

De plus, ces Etats devraient s'engager à limiter la prolifération d'armes cyber par le contrôle de l'exportation d'outils et techniques cyber offensifs (tout en prenant en compte les intérêts légitimes des entreprises de cybersécurité et du monde académique) et à encadrer les pratiques déstabilisatrices des acteurs privés (ces Etats ne devraient pas autoriser, à l'intérieur de leur juridiction, l'usage par des acteurs non-étatiques, notamment du secteur privé, de techniques et outils cyber pouvant avoir des conséquences défavorables sur une tierce partie).

- *Afin de mettre en œuvre et faire respecter les normes déjà agréées : le principe de coopération*

Améliorer la coopération de la communauté internationale dans le cyberespace est un moyen efficace d'en renforcer la stabilité par une connaissance mutuelle, voire une confiance, approfondie entre les acteurs et par l'établissement de mécanismes de gestion commune des crises, de communication et de désescalade.

Dans cette optique, la France doit en particulier œuvrer à parvenir à un accord, au niveau international, sur les obligations qui pèsent sur un Etat dont les infrastructures seraient utilisées à des fins malveillantes. L'objectif est d'appliquer, dans le domaine cyber, le principe de *due diligence* qui prévoit que tout Etat a l'obligation « de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres Etats ». Ce principe de « *cyberdiligence* » pourrait notamment permettre de renforcer la coopération opérationnelle volontaire entre les Etats, essentielle en vue de protéger certaines infrastructures critiques et de répondre à des cyberattaques majeures, notamment lorsque celles-ci transitent via un Etat tiers.

La France proposera à ses partenaires d'étudier la faisabilité d'un mécanisme coopératif de suivi de la mise en œuvre des recommandations agréées lors des sessions du GGE de 2013 et de 2015, voire dans d'autres cadres comme le G7. Ce dispositif intergouvernemental pourrait notamment reposer sur des pratiques de revue par les pairs, menée sur une base volontaire, formulant des recommandations adressées aux Etats. Un annuaire des points de contact identifiés aiderait en outre à établir des canaux de communication facilitant la prévention et la résolution des crises.

- *Pour assurer le droit aux Etats de se défendre de manière légale et appropriée : le principe de stabilité*

Sur la base de la reconnaissance par le GGE en 2013 et en 2015 de l'application du droit international existant dans le cyberespace, la France doit continuer à promouvoir le principe de l'existence de certains droits permettant aux Etats victimes de cyberattaques de prendre les mesures appropriées en vue de préserver la paix et la sécurité internationale.

Le premier de ces droits permettrait à un Etat victime de saisir le Conseil de sécurité des Nations Unies, dans le cas où la situation serait assez grave pour être considérée comme une menace contre la paix et la sécurité internationale. Entre autres options, le Conseil de sécurité pourrait alors adopter des mesures coercitives sur le fondement du chapitre VII de la Charte des Nations Unies.

Le deuxième de ces droits est de pouvoir répondre aux attaques cyber. Si les Etats doivent chercher à régler leurs différends par la coopération et la négociation, cela n'exclut pas la possibilité pour un Etat victime d'une cyberattaque ayant atteint une infrastructure critique de prendre les mesures techniques nécessaires et proportionnées afin de neutraliser les effets de cette attaque, dans le respect de ses obligations en matière de droit international.

Le troisième droit est, enfin, la possibilité de considérer une attaque cyber comme une agression armée, en particulier si elle était menée contre une infrastructure critique, entraînant la paralysie ou la destruction de fonctions et activités économiques vitales, ou si elle portait atteinte à la population.

Les règles et normes concernant la responsabilité des acteurs privés dans la sécurité du cyberespace

L'essor du numérique comme nouvel outil et espace de confrontation confère au secteur privé, notamment à un certain nombre d'acteurs systémiques (.), un rôle critique et une responsabilité inédite dans la préservation de la paix et de la sécurité internationale.

Le cyberespace est en grande partie constitué de produits commerciaux grand public, pouvant servir de support à des attaques de grande envergure qui en exploitent les défauts de fabrication (faille du logiciel *Windows* pour les attaques *WannaCry* et *Petya*). Il est donc nécessaire de fixer au niveau international des normes visant à s'assurer que les produits ayant un caractère systémique ne puissent être détournés de leur usage initial pour conduire des attaques informatiques. Le problème se pose de façon accrue avec la multiplication des objets connectés pouvant servir de vecteurs d'attaque.

Les « armes cyber » (logiciels intrusifs ou destructifs) sont, par ailleurs, pour partie produites par des entreprises privées sur un marché qui est très difficile à réguler en raison de la double finalité offensive et défensive inhérente à ces produits. Les logiciels d'intrusion sont désormais intégrés à la liste des biens à double usage de l'Arrangement de Wassenaar, un régime multilatéral de contrôle des armes conventionnelles et des biens et technologies à double usage que la France applique. Il est nécessaire de poursuivre les efforts de régulation dans ce sens, y compris en posant la question de l'inscription de certains outils cyber sur la liste des matériels de guerre. Cet aspect sera approfondi dans la troisième partie de cette revue en prenant en compte la viabilité d'une offre nationale ou européenne.

Enfin, des services de « mercenariat » se développent et proposent des prestations offensives de contre-attaque cyber, selon une logique de légitime défense privée (*Hack-back*). Afin de permettre aux Etats de conserver le monopole de la violence légitime dans le cyberespace, il est nécessaire de fixer des règles claires aux entreprises en matière de cyberdéfense « active ».

Dans ce contexte, la régulation interétatique n'est pas en mesure d'apporter seule une solution efficace et durable aux défis de la sécurité du monde numérique. Le renforcement de la stabilité et de la sécurité internationale du cyberespace nécessite donc la définition de nouvelles formes de régulation prenant en compte le rôle du secteur privé.

Trois axes prioritaires pour une meilleure régulation des activités du secteur privé nécessitent d'être abordés : l'encadrement de l'action offensive du secteur privé dans le cyberespace, le contrôle des exportations d'outils, logiciels et techniques cyber, et la responsabilité des entreprises dans la conception et la maintenance des produits numériques.

- *Encadrer l'action offensive du secteur privé dans le cyberespace*

La multiplication des attaques et les difficultés rencontrées pour en poursuivre les auteurs incitent le secteur privé à développer des capacités de cyberdéfense. Cette dynamique peut conduire à promouvoir le *Hack back*, c'est-à-dire l'autorisation pour un acteur privé de mener des actions cyber offensives en réponse à une attaque dont il serait victime.

Dans le même temps, certains Etats envisagent de confier à des entreprises privées un certain nombre d'actions cyber offensives dans le cadre de leur politique militaire, à l'instar de ce qui existe avec les sociétés militaires privées pour des capacités traditionnelles.

L'utilisation de capacités offensives par le secteur privé fait peser un risque d'instabilité systémique dans le cyberespace. La conduite de telles attaques informatiques contre des acteurs localisés sur le territoire d'un autre Etat, voire directement contre un Etat, entraînerait un risque d'escalade dangereux et remettrait en cause le monopole de l'usage international de la force par les Etats. De plus, la question de l'attribution se pose de la même manière pour le secteur privé que pour les Etats. En effet, ces sociétés possédant souvent de multiples emprises à l'international, elles pourraient être amenées à conduire la riposte depuis le territoire d'un pays tiers, différent de celui ayant subi l'agression. Cela en complexifierait l'attribution.

Face au risque de multiplication d'actions offensives dans le cyberespace, la France propose, d'une part, de promouvoir la prévention de l'utilisation de capacités cyber offensives par les acteurs non-étatiques et, d'autre part, de soutenir l'interdiction, pour les acteurs non-étatiques, de conduire des activités offensives dans le cyberespace pour eux-mêmes ou pour le compte d'autres acteurs non-étatiques, sauf dans des cas très précis et à condition que les actions techniques envisageables dans ce contexte soient strictement encadrées.

Afin d'être réalistes, de telles règles sont à définir précisément sur le plan technique afin de tracer une ligne claire, contrôlable et acceptable par tous. La question d'une potentielle

exception à l'interdiction générale de recours à des actions cyber offensives par des entreprises privées en cas de légitime défense devra être posée au niveau international.

- *La responsabilité de sécurité des entreprises pour la conception et la maintenance des produits numériques*

De nombreuses attaques informatiques sont rendues possibles par l'absence de mise à jour de sécurité de produits informatiques largement répandus. Cette situation soulève la question de la responsabilité des entreprises en matière de maintien en conditions de sécurité. Ce risque prend une dimension systémique lorsque les produits concernés sont massivement utilisés.

Il semble donc pertinent de poser au niveau international un principe de responsabilité de sécurité des acteurs privés systémiques dans la conception, l'intégration, le déploiement et la maintenance de leurs produits et services numériques. Cette responsabilisation pourrait se traduire par une obligation pour les entreprises systémiques de garantir la sécurité à long terme de leurs produits numériques, notamment en fournissant des correctifs appropriés en cas de vulnérabilité. Le niveau de responsabilité doit être fixé en fonction du rôle et de la taille de l'acteur concerné et pourrait se présenter comme une obligation de moyens plus que de résultats.

La responsabilité première incombe au producteur qui se doit de garantir une sécurité évolutive correspondant à l'usage de son produit pendant toute la durée de vie de celui-ci, conformément aux bonnes pratiques de développement de sécurité informatique. Cela vise à la fois à garantir un niveau de sécurité pour le produit lui-même mais également un niveau minimal de sécurité vis-à-vis des systèmes auxquels ce produit est connecté. Le recours à la certification de sécurité, notamment dans le cadre du schéma de certification européen en cours de définition, doit être fortement encouragé et même rendu obligatoire pour les composants critiques dans les secteurs sensibles.

Compte tenu de l'évolution rapide de l'état de l'art en matière de sécurité numérique, il est de la responsabilité du producteur de mettre en place les dispositifs nécessaires pour maintenir de manière continue la sécurité de ses produits (veille, équipes dédiées de revues de la sécurité, formation des équipes de développement, organisation de *bug bounty*...). Les correctifs doivent par ailleurs être accessibles, le plus largement possible, même en l'absence de contrat de maintenance, et dans un délai raisonnable une fois la vulnérabilité portée à la connaissance de l'industriel.

La responsabilité du producteur doit s'étendre au-delà de la date de fin de commercialisation du produit et pendant une période suffisamment longue pour couvrir la vie des produits concernés. En cas de cessation définitive de la maintenance, il est nécessaire que le producteur mette à disposition les informations techniques nécessaires (code, documentation) pour que ses clients puissent prendre eux-mêmes en charge le maintien en condition de sécurité.

Les producteurs doivent également être en mesure de fournir à leurs clients une assistance en cas d'attaque, notamment afin de faciliter le rétablissement du fonctionnement des produits concernés. Cette responsabilité concerne en particulier l'appui aux autorités publiques en cas d'atteinte à un système critique. Il s'agirait a minima de communiquer l'expertise et les informations techniques nécessaires ainsi que de mettre à disposition des systèmes permettant la reconstruction et la mise à jour du produit.

Par ailleurs, il convient également de définir la responsabilité des distributeurs et intégrateurs. La diffusion de produits dans des versions obsolètes ou non actualisables doit être proscrite, ainsi que la diffusion de produits connus pour leur niveau de sécurité insuffisant. En effet, l'intégration ou l'achat par des clients de tels produits représente un risque non seulement pour leurs systèmes mais également pour l'ensemble de l'espace numérique.

Dans cette optique, la France doit mobiliser le secteur privé pour diffuser des bonnes pratiques et des codes de conduites ainsi que pour contribuer à une prise en compte de ces enjeux dans les clauses contractuelles. Cependant, pour les produits les plus sensibles, des initiatives règlementaires, en particulier au niveau européen, pourraient être envisagées.

Les formats de négociation

L'échec des négociations au sein du GGE de l'ONU souligne l'absence de vision commune, partagée par les principales puissances cyber, quant à l'architecture internationale de sécurité qui doit régir les relations entre Etats à l'ère numérique. Toutefois, cet échec ne signifie nullement la fin des efforts diplomatiques menés en vue de réguler ce domaine. La France doit continuer à prendre une part active à ces débats, quel que soit le cadre de négociation retenu : l'ONU, le G20, le G7 ou encore des organisations régionales telles que l'Organisation pour la sécurité et la coopération en Europe (OSCE).

L'échec de la dernière session du GGE invite à repenser le traitement des enjeux de cybersécurité au sein de l'Organisation des Nations Unies.

Le G7, dont la France assurera la présidence en 2019, a déjà publié, en mars 2017, la Déclaration de Lucques sur le comportement responsable des Etats dans le cyberespace. Ce texte, négocié d'abord dans le cadre du Groupe Cyber Ise-Shima, reprend les normes de comportement agréées en 2015 par le GGE, tout en réaffirmant et en approfondissant la reconnaissance de l'applicabilité pleine et entière du droit international au cyberespace.

Le G20 semble constituer, quant à lui, un forum adapté à un sujet combinant enjeux de souveraineté, régulation internationale et acteurs privés. En 2015, les Etats membres du G20 se sont ainsi mis d'accord pour interdire l'utilisation de moyens cyber à des fins d'espionnage économique.

Les travaux menés au sein de l'OSCE doivent être approfondis. La France poursuit son action en faveur de la mise en œuvre des 16 mesures de confiance appliquées au cyberespace, adoptées en 2013 et 2016. Elle continuera à encourager ses partenaires à se doter de

procédures interministérielles qui puissent être mobilisées afin d'assurer la bonne communication entre Etats en temps de crise. De tels mécanismes pourraient utilement être reproduits dans d'autres enceintes régionales (Union africaine, Organisation des Etats américains, Forum régional de l'ASEAN, etc.).

A ces formats intergouvernementaux s'ajoutent les enceintes dites « track 2 », qui rassemblent Etats et représentants de la société civile, du monde privé ou de la recherche tels que la *Commission globale pour la stabilité du cyberespace*, le *Global Forum on Cyber Expertise*, le *Sino-European Cyber Dialogue*, etc. Ces forums constituent également des cadres de débat importants.

La présente revue préconise la création d'un nouveau *think tank* national (ou européen) dédié aux questions de cyberdéfense, au sein duquel, les idées de la France pourraient trouver un relais.

Elle recommande également le lancement d'une initiative française dans le cadre du G20 en vue de réguler les activités du secteur privé ayant un impact sur la sécurité internationale du cyberespace, autour de trois axes :

- l'encadrement des actions offensives du secteur privé dans le cyberespace ;
- le contrôle des exportations de certains outils, logiciels et techniques cyber ;
- la responsabilité de sécurité des entreprises systémiques pour la conception et la maintenance des produits numériques.

***

Les positions de la France doivent permettre d'afficher sa volonté de construire la stabilité stratégique dans le cyberespace, afin qu'il soit en paix, prospère et respectueux des libertés et dans lequel elle entend bien assurer toutes ses fonctions régaliennes et affirmer sa souveraineté.

Le modèle français, basé sur la mise en place d'une chaîne défensive indépendante, doit être promu auprès de nos partenaires, notamment via la conduite de dialogues stratégiques dédiés spécifiquement aux questions cyber, et dans différentes enceintes européennes et internationales. La France doit développer ces dialogues bilatéraux en priorité avec quelques pays clés, avec l'objectif de négocier des cadres d'accord politique permettant d'éviter les actions les plus déstabilisatrices ou dangereuses (Russie, Chine, Etats-Unis, Royaume-Uni, etc.).

La France doit aussi être moteur pour que l'Europe devienne un espace propice au développement numérique et garantissant aux citoyens un cyberespace de confiance, sûr et protecteur des libertés individuelles. La France doit porter une vision ambitieuse du rôle de

l'Union européenne en matière de cybersécurité tout en réaffirmant la responsabilité des États membres et la préservation de leur souveraineté en matière de réponse opérationnelle.

La France doit continuer à s'engager pleinement dans les travaux consacrés aux enjeux cyber dans le cadre de l'Alliance atlantique, et y contribuer de manière proactive en vue du Sommet de Bruxelles (juillet 2018). Elle s'attachera ainsi à poursuivre le renforcement des capacités de défense de l'OTAN et des Alliés, notamment via le *Cyberdefense Pledge*, et veillera à une intégration des effets cyber offensifs dans les opérations et missions de l'Alliance conforme à ses intérêts. Une communication publique susceptible de contribuer à notre propre politique de découragement des attaques informatiques tout en s'opposant à toutes velléités d'attribution collective sera développée.

La France doit porter dans les instances européennes et internationales une stratégie de promotion de comportements responsables des acteurs systémiques étatiques et non étatiques et de développement de mesures de confiance dans le cyberespace ainsi que sa vision de l'application du droit international existant, y compris du droit international humanitaire, dans ce domaine. Cette posture est d'autant plus essentielle dans le contexte international actuel d'échec des dernières négociations conduites dans le cadre du groupe des experts gouvernementaux (GGE). Dès lors, la France doit être à l'initiative pour défendre ses intérêts dans le cyberespace, mettre en avant son modèle et les idées qu'elle porte en matière de régulation internationale du cyberespace.

Enfin, le développement d'un cyberespace serein et sûr suppose de lutter efficacement contre les criminels qui y sévissent, y compris lorsque les attaques sont lancées depuis l'étranger. La France doit donc poursuivre la promotion de la coopération internationale en matière de lutte contre la cybercriminalité en apportant notamment son soutien à la Convention dite de Budapest. La France doit s'efforcer de perfectionner avec ses partenaires étrangers les mécanismes d'entraide judiciaire en matière de lutte contre la cybercriminalité et poursuivre les échanges d'expérience et de technologies dans ce domaine.

Partie 3. L'État, garant de la cybersécurité de la société

La cyberdéfense de la France, au-delà de celle de l'État lui-même et des opérateurs d'importance vitale, passe par une élévation du niveau global de cybersécurité dans la société. Pour être efficace, il s'agit bien d'envisager, dans une logique de souveraineté numérique, une défense cyber dans la profondeur de notre pays intégrant celle des citoyens, des entreprises et des collectivités territoriales.

C'est pourquoi, cette troisième partie de la revue stratégique de cyberdéfense propose des avancées ambitieuses s'agissant tant de la régulation que de l'économie de la cybersécurité. L'action publique doit se doubler de celle des agents économiques, qui restent les premiers responsables de leur sécurité informatique. Le rôle de l'État est de fournir un effort accru en matière de formation et de gestion des compétences dans le domaine de la cybersécurité.

3.1. La souveraineté numérique, composante essentielle de la souveraineté nationale

La souveraineté numérique peut être entendue comme la capacité de la France d'une part, d'agir de manière souveraine dans l'espace numérique, en y conservant une capacité autonome d'appréciation, de décision et d'action et d'autre part, de préserver les composantes les plus traditionnelles de sa souveraineté vis-à-vis de menaces nouvelles tirant partie de la numérisation croissante de la société. La souveraineté numérique ne représente donc pas la volonté de tout faire en national ce qui serait synonyme de replis sur soi mais bien de conserver une autonomie et une liberté de choix.

Les réflexions conduites dans le cadre de la présente revue convergent vers la nécessité pour notre pays d'exercer pleinement sa souveraineté numérique. Il est proposé à cette fin de structurer une politique industrielle en matière numérique, reposant sur la maitrise de technologies clés (par exemple le chiffrement de flux IP, les sondes de détection d'attaque, les radios professionnelles mobiles).

Les enjeux de l'informatique en nuage (Cloud) et de l'intelligence artificielle sont également au cœur de toute stratégie de souveraineté numérique.

3.1.1. <u>Les activités souveraines</u>

La maîtrise de certaines technologies et services est indispensable à l'exercice de notre souveraineté numérique. Cette maîtrise s'appuie largement sur la qualification par l'Etat d'une offre de confiance de technologies et de services numériques. Par ailleurs, une stratégie industrielle basée sur « l'open source », sous réserve qu'elle s'inscrive dans une démarche commerciale réfléchie, peut permettre aux industriels français ou européens de gagner des parts de marché où ils sont aujourd'hui absents et par là même de permettre à la France et à l'Union européenne de reconquérir de la souveraineté.

Identifier les besoins nécessaires à la protection de la souveraineté numérique

L'identification des besoins nécessaires à la protection des intérêts de souveraineté constitue une étape préalable à la détermination des technologies et services numériques dont la disponibilité, voire la détention, sont essentielles pour notre pays. Ces besoins découlent de la nécessité d'assurer les missions régaliennes de l'État et les activités critiques des OIV d'une part et, d'autre part, de protéger les valeurs, le patrimoine et les intérêts économiques de la nation.

Pour chacune de ces familles de besoins, une analyse doit être conduite afin de faire émerger les technologies clés qui supportent ces besoins. Par la suite, les choix stratégiques permettant de répondre à ces besoins doivent être identifiés, comme les architectures de solutions retenues[39]. Enfin, s'il n'existe pas de solution pertinente ou si des évolutions technologiques sont susceptibles de faire évoluer ces choix stratégiques[40], il convient alors d'identifier les pistes concrètes qui pourraient permettre de proposer des solutions adaptées.

Évaluer le besoin, proposer des solutions et des architectures de solutions, arrêter une stratégie notamment pour détenir, contrôler ou faire émerger des technologies clés, tels doivent être les objectifs d'une politique publique de la cybersécurité. La conduite de cette politique requiert d'y dédier des ressources spécifiques, en charge d'une veille technologique et de proposer des choix. Il pourrait s'agir d'une petite équipe interministérielle (positionnée auprès de la direction générale des entreprises ou de l'ANSSI) mobilisant pour ces travaux et ses études l'ensemble des administrations compétentes (ministère de l'économie et des finances, ministère des armées, ministère de l'intérieur, secrétariat d'État au numérique, ANSSI, *France Stratégie*, etc.) ainsi que le secteur industriel. Elle pourrait utilement s'appuyer sur les structures mises en place dans le cadre du *Comité de la filière industrielle de sécurité* (CoFIS) pour une identification régulière et actualisée des technologies critiques et des technologies de rupture.

Qualifier une offre de confiance

La sécurité de nos approvisionnements exige que la demande puisse être satisfaite par à une offre de confiance et suffisamment diversifiée. Certains usages ou certaines fonctions supposent un contrôle minimal de l'État des produits employés (homologation, certifications, accès aux codes sources,...). Enfin, La satisfaction de certains besoins appelle le développement par un industriel de confiance de produits spécifiques selon les spécifications d'un cahier des charges précis. Ce produit doit rester totalement libre d'emploi et d'usage exclusif et pouvoir faire l'objet d'une évaluation régulière quant à la tenue de son niveau de

[39] Cette description des architectures et des technologies clés doit comprendre une analyse du degré de contrôle nécessaire sur les technologies utilisées, sur la base des critères définis. Le terme technologie est à prendre dans un sens très inclusif : pour assurer la confidentialité, si on utilise de la cryptographie, celle-ci peut se décliner en produits (chiffreurs IP) ou en option dans une offre de communication (messagerie, web,...).

[40] Cette présentation doit être faite à court et à moyen termes et préciser les horizons temporels retenus.

sécurité[41].

Pour qualifier une offre, l'Etat doit être en mesure d'identifier les industriels et les produits qui sont à la fois éligibles et disponibles (cf. encadré ci-après) pour nos besoins de sécurité et de souveraineté. Ensuite, un certain nombre de critères doivent être satisfaits, dont cinq revêtent une importance particulière :

- la maîtrise par l'entreprise de ses développements et de ses processus industriels[42] ;
- le degré de transparence accepté par l'industriel sur la fabrication de ses produits (mise à disposition du code source par exemple) ;
- l'autonomie de décision dont jouit l'industriel (pour fixer, par exemple, les *roadmaps* de ses produits, ses architectures, etc.) qui ne doit pas être soumise aux possibles interférences de tiers indésirables ;
- l'acceptation par l'industriel de contrôles. Les locaux dans lesquels sont développés ses produits doivent en particulier être accessibles (localisés en Europe) et ses processus de production pouvoir être soumis à audit ;
- le respect par l'industriel de règles de protection du secret (processus d'habilitation des personnes et des installations, mise en place de règles de sécurité et de zones à régime restrictif, etc.)[43].

La nationalité (française ou européenne) est en soi un critère à prendre en considération pour reconnaître la qualité d'industriel de confiance. Il n'est cependant pas toujours opposable, ni pertinent.

Le respect de ces différents critères doit pouvoir être régulièrement évalué, de même que certaines évolutions relatives à l'évolution capitalistique de l'entreprise ou de ses choix stratégiques.

Etablir un état des lieux de l'offre existante de technologies et services numériques essentiels au maintien de la souveraineté nationale

Pour chacun des technologies clés, l'établissement de l'état des lieux de l'offre existante se fait sur la base du schéma de questionnement suivant :

[41] Le niveau de sécurité doit être apprécié au regard des risques potentiels, qu'ils soient endogènes et liés aux performances des produits (défaillances/discontinuité du service, défaut de performance), ou exogènes et liés aux différentes formes d'attaques (visant à accéder aux informations, à modifier les informations, à prendre le contrôle de systèmes).

[42] Une éventuelle sous-traitance ne doit être réalisée que sur des parties non critiques des produits (analyse de risque à l'appui) ou via des industriels eux-mêmes de confiance.

[43] On notera que la localisation des centres de décision, des unités chargées de la recherche et du développement a un impact direct sur plusieurs de ces critères.

Une offre de confiance est-elle nécessaire ?

a) Si oui, dispose-t-on d'une telle offre ? Est-elle pérenne et susceptible de s'adapter aux besoins ?

Si oui, par quelles méthodes, à quelles conditions et à quel coût ? Quelles sont les exigences pour l'offre (maintien de la disponibilité d'une offre *Open source*, intensité concurrentielle et maintien de plusieurs offres concurrentes, positionnement adéquat dans la chaine de valeur, substituabilité du produit ou du service etc.).

b) Dans le cas contraire, une offre alternative de confiance est-elle susceptible d'émerger ? Dans quelles conditions et à quel coût ?

Cette étape doit intégrer toutes les dimensions technologiques (en principe dans la feuille de route des industriels concernés) et économiques (y compris la dimension marché « souverain », national ou exportation[44]). Elle doit également détailler les diverses actions publiques possibles ainsi que leur ampleur (au moins en ordre de grandeur) à mettre en regard de la taille du marché. L'action peut être financière (soutien public en capitaux ou en subvention pour l'industriel ou ses sous-traitants, politique d'achat, etc.), règlementaire (contrôle des investissements étrangers) ou prendre la forme d'une aide à l'approvisionnement de certains composants.

3.1.2. Trois technologies, parmi d'autres, dont la maitrise est essentielle à notre souveraineté numérique

Parmi les technologies clés dont la maîtrise est nécessaire à l'exercice de notre souveraineté numérique, la revue a choisi d'en mettre trois en évidence. Le choix s'est effectué sur le caractère indispensable de ces technologies : le chiffrement des communications, la détection d'attaques informatiques et les radios mobiles professionnelles. Les questions de l'informatique en nuage (*cloud*) et de l'intelligence artificielle sont par ailleurs également lourdes d'enjeu.

Le chiffrement des communications

Avec la convergence de tous les protocoles de communication numérique vers la technologie IP, le chiffrement des communications s'est progressivement concentré autour des chiffreurs dédiés à cette technologie (dénommés « chiffreurs IP »), qu'il s'agisse d'équipements matériels ou de pur logiciel.

Les matériels ou logiciels développés par plusieurs industriels sont par ailleurs non interopérables et aucun des fournisseurs n'est en mesure de répondre à l'ensemble des besoins, ce qui se traduit par un marché très morcelé et de faible envergure qui repose quasi exclusivement sur la commande publique. Pour éviter une obsolescence et une perte de

[44] Même les produits de sécurité sensibles sont exportés.

compétitivité des produits vis-à-vis de leurs concurrents étrangers, notamment pour les marchés UE ou OTAN, mais aussi pour certains besoins de nos entreprises, il convient de redynamiser notre offre nationale. L'ANSSI a entrepris en ce sens, par le biais d'une spécification générique, de rendre les produits interopérables, ce qui devrait permettre à terme d'avoir une couverture complète du besoin et de relancer un domaine figé par les coûts d'investissements du côté des fournisseurs et les coûts de migration du côté des clients. Pour le succès de cette démarche, il est indispensable que les clients étatiques, mais aussi les grands comptes industriels, exigent l'interopérabilité dans leurs appels d'offre.

La détection d'attaques informatiques

La capacité à superviser à grande échelle les systèmes d'information des infrastructures de l'État et des OIV pour y détecter des attaques informatiques constitue un enjeu crucial, qui suppose des fournisseurs de produits et des prestataires d'une totale confiance. L'efficacité des solutions de détection d'attaques dépend de l'intégration de composants logiciels ou matériels à des emplacements stratégiques d'un système d'information, ce qui accentue la nécessité de maîtriser ces composants et d'avoir toutes les garanties sur ceux qui les fabriquent ou les mettent en œuvre.

Le marché des outils de détection d'attaque (sondes et agents, voir tableau) est largement dominé par des acteurs industriels étrangers qui ne répondent pas nécessairement aux critères de confiance indispensables. Des travaux ont cependant été engagés pour faire émerger en 2018 des solutions de confiance pour la France en matière d'analyse de flux réseau ou d'agents locaux aux postes informatiques. Elles sont complétées par des développements étatiques spécifiques, réservés à la supervision des administrations. Toutes ces solutions (industrielles et étatiques) sont tributaires, sur le plan technologique, de composants tiers critiques pour l'analyse, dont la confiance ou la pérennité ne sont pas totalement acquises, qu'il s'agisse de fournitures industrielles ou de logiciels libres.

Il n'existe par ailleurs pas d'éditeur national de premier rang dans le domaine des technologies fondamentales permettant le traitement de grands volumes d'information. Des implémentations alternatives existent cependant sous la forme de logiciels libres ou gratuits et sont intégrables par des acteurs de confiance ou par les équipes étatiques. La pérennité de ces implémentations n'est pas nécessairement garantie et constitue un enjeu important.

La situation est analogue dans les domaines de la détection d'attaques et de l'analyse de codes malveillants, où les solutions existantes reposent majoritairement sur des acteurs étrangers ou des logiciels libres. On constate néanmoins l'émergence d'offres nationales, dont la robustesse reste à confirmer ou qui s'adressent à des marchés spécifiques. L'expertise associée à ces activités, détenue par des équipes spécialisées au sein de l'État, est par ailleurs en train de se structurer au sein d'un tissu de prestataires de services privés, *via* la qualification par l'ANSSI de *Prestataires de détection d'incidents de sécurité* (PDIS).

La constitution et la disponibilité de bases actualisées et de confiance de marqueurs d'attaques demeurent un point de fragilité. Aucun industriel national ne fournissant de telles

bases, les solutions souveraines de détection restent entièrement tributaires de bases publiques. L'ANSSI dispose d'une capacité autonome d'élaboration de marqueurs, dont la mise à disposition auprès d'acteurs privés de confiance est en cours d'organisation. Toutefois, la capacité des seules équipes étatiques à changer d'échelle et à couvrir l'ensemble des besoins en marqueurs reste d'autant plus problématique que l'extension en cours du champ de la détection vers les postes clients, les serveurs et le cloud, augmente la charge de travail.

Plus généralement, le manque d'acteurs nationaux ou européens dans le domaine de la *Threat intelligence* réduit notre capacité à disposer d'informations massives sur les cybermenaces. Cette situation risque d'obérer à terme les capacités nationales de recherche de nouvelles solutions algorithmiques de détection. Ce décrochage risque d'être accentué par le développement de nouvelles méthodes de détection basées sur l'intelligence artificielle. Or, des réponses à cette véritable rupture technologique bientôt attendue sont fortement liées à l'accès à de tels jeux de données. L'émergence d'un acteur industriel de référence, national ou européen, dans le domaine de la *Threat intelligence* et de l'élaboration de marqueurs, est pour ces raisons éminemment souhaitable et devra être recherchée.

Les composantes essentielles à une solution complète de détection

Une solution complète de détection conjugue plusieurs moyens et capacités :

- des capteurs permettant d'observer l'activité d'un système d'information en temps-réel, par le biais des flux réseaux (sondes) ou du fonctionnement des postes informatiques (agents) que ce soit sur des postes isolés ou des architectures de *cloud*;
- des capacités de collecte, d'indexation, de traitement et de stockage de grands volumes de données, issues des capteurs ou de la collecte de journaux de fonctionnement par exemple ;
- des méthodes et algorithmes permettant de distinguer les activités normales des activités malveillantes, à partir des informations issues des capteurs. Cette discrimination peut s'opérer par la reconnaissance de signatures caractéristiques d'attaques et d'anomalies « comportementales » ;
- des bases de marqueurs, y compris les signatures d'attaques classifiées en raison de leur sensibilité, et plus généralement une connaissance des principaux modes opératoires adverses ;
- une capacité d'analyse des attaques détectées, permettant la levée de doute et l'enrichissement de la base de signature.

Ces composantes dépendent à leur tour de technologies clés (analyse à haut débit de paquets réseau ou de fichiers, traitement *Big data*, outils de rétroconception ou de « détonation » sécurisée de code malveillant, etc.), de la capacité d'intégration de ces technologies, et d'expertises spécifiques.

Les radios mobiles professionnelles

En vingt-cinq ans d'existence, les réseaux de radios professionnelles mobiles ont démontré leur utilité pour les forces de sécurité et les unités de secours. Les besoins ont cependant évolué et les réseaux actuels sont à la fois saturés et techniquement limités.

L'organisation des forces et la concentration de moyens sur des surfaces géographiques restreintes rendent plus manifestes encore les limitations techniques des réseaux actuels (nombre de conférences de groupe, capacité d'inscription des terminaux sur zone...) qui, combinées avec les attentes des utilisateurs génèrent des frustrations. Les performances des terminaux qui leur sont confiés - dont l'ergonomie est plus proche des téléphones mobiles des années 1990 que des smartphones actuels - les conduisent de plus en plus à utiliser comme moyen de communication leurs smartphones professionnels ou privés. Les forces de sécurité ou les services de secours se plaignent également d'une couverture insuffisante, tant en extérieur qu'à l'intérieur des bâtiments[45]. Les responsables opérationnels reprochent l'absence de fonctions désormais perçues comme essentielles : flux vidéo, accès au système d'information, accès aux réseaux publics de téléphonie...

Pour les raisons opérationnelles évoquées plus haut et dans une logique de protection de la confidentialité des communications, une nouvelle génération de radios professionnelles mobiles devrait être développée au profit des forces de sécurité et des unités de secours. Il s'agirait de fournir une offre de réseau favorisant l'interopérabilité et la coordination des forces et des moyens engagés sur le terrain, notamment en situation de crise opérationnelle, sans régressions fonctionnelles par rapport aux moyens actuels (en particulier par rapport aux services commerciaux de téléphonie mobile)[46].

Afin de sortir des limites des technologies actuelles, la future solution devrait s'appuyer sur des équipements standards et le plus possible sur des réseaux d'opérateurs existants, limitant ainsi les coûts et l'effort de formation pour les agents. Elle devrait également être en mesure d'évoluer dans le temps (en particulier pour assurer le passage à la 5G). Une ouverture au service opérationnel avec une couverture limitée en 2022 et sur l'ensemble de la plaque parisienne dans la perspective des Jeux Olympiques en 2024, apparaît techniquement envisageable.

Du fait de la convergence observée entre ce domaine et celui de la sécurité de la mobilité (téléphonie, messageries, réseaux sociaux,...), la présente revue recommande de mener une analyse globale pour voir comment mutualiser une infrastructure et des produits permettant de répondre à ces deux besoins. A l'image du RIE, la DINSIC pourrait mettre à disposition

[45] La problématique n'étant pas tant celle de l'absence de couverture que le différentiel qui existe avec les réseaux commerciaux de téléphonie mobile.

[46] Parmi les enjeux de non régression figure notamment le sujet du mode direct (communication directe, hors infrastructure, entre deux terminaux).

des administrations des services de mobilité permettant en particulier un accès sécurisé et résilient aux données du RIE.

3.1.3. Tirer tout le potentiel des techniques d'intelligence artificielle au profit de la cybersécurité

Les enjeux de souveraineté autour de l'intelligence artificielle (IA) sont considérables et poussent toutes les grandes puissances à investir massivement dans la recherche et les développements industriels. A la suite à de la publication de plusieurs rapports sur le sujet (notamment le rapport « *France Intelligence Artificielle* » et le rapport « *Pour une intelligence artificielle maîtrisée, utile et démystifiée* » de l'Office parlementaire d'évaluation des choix scientifiques et techniques (OPECST de mars 2017[47]), une mission a été confiée le 8 septembre 2017 par le Gouvernement au député Cédric VILLANI, afin d'affiner, d'approfondir et de prioriser le travail déjà conduit sur l'intelligence artificielle. Les conclusions de cette mission pourront ensuite être déclinées dans une feuille de route concrète posant les bases d'une action française et européenne dans la durée[48]. Dans l'attente de celles-ci, seuls les liens entre cyberdéfense et intelligence artificielle sont analysés dans cette partie de la revue.

Le premier enjeu déjà identifié dans les paragraphes de la présente revue consacrés à la mémoire (cf. partie I) et dans le rapport *France Intelligence Artificielle* de mars 2017 est celui de la cybersécurité des systèmes d'intelligence artificielle. Elon MUSK, après qu'un véhicule électrique de sa marque *TESLA* se fut fait piraté par des chercheurs de la société *TENCENT*, soulignait à cet égard, en juillet 2017 devant les autorités américaines[49], que l'avenir des véhicules autonomes était conditionné par la cybersécurité. Que ce soit en phases d'apprentissage, qui peuvent impliquer la prise en compte de données sensibles en termes de sécurité, ou pendant les phases d'utilisation, les systèmes d'IA doivent être protégés afin d'empêcher un attaquant de voler des informations précieuses ou d'en prendre le contrôle. Pour des raisons d'efficacité et de coût, la cybersécurité des systèmes d'IA doit être pensée *ab initio* et être intégrée au développement de ceux-ci dès le stade de conception.

Au-delà de la question de la cybersécurité des systèmes d'IA, l'application des techniques

---

[47] Rapport de synthèse France Intelligence Artificielle, mars 2017 : www.economie.gouv.fr /France-IA-intelligence-artificielle.

Rapport *Pour une intelligence artificielle maîtrisée, utile et démystifiée*, Claude de Ganay, Dominique Gillot, OPECST, mars 2017 :

http://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_rapport_Intelligence_artificielle_synthese_4pages.pdf.

[48] L'objectif assigné à la mission consiste à étudier les actions nécessaires pour permettre à la France et à l'Europe d'être à la pointe de l'économie de l'intelligence artificielle, décrire les meilleures pratiques internationales d'application de ces technologies au service de la transformation et de l'amélioration des politiques publiques, identifier les applications prioritaires à déployer à l'intérieur de la sphère publique et ouvrir le champ à une réflexion nationale sur les impacts de l'intelligence artificielle, en considérant ses effets sur le travail les questions éthiques qu'elle soulève (http://www.villani2017.eu/blog/mission-villani-sur-l-intelligence-artificielle).

[49] Discours d'Elon MUSK, le 15 juillet 2017, devant la *National Governor Association*.

d'intelligence artificielle au domaine de la cyberdéfense offre des perspectives prometteuses. Le domaine informatique se prête en effet aisément à de la simulation ou à de l'automatisation facilitant grandement les expérimentations et l'apprentissage par renforcement à partir des données disponibles et étiquetées (bases de logiciels malveillants, base de vulnérabilités, base de données réseaux, ...). Les techniques d'intelligence artificielle ont ainsi déjà été utilisées pour détecter une attaque parmi des flux réseaux ou un logiciel malveillant mais aussi pour récupérer le code PIN d'un smartphone, la clef d'une carte à puce ou bien encore réaliser des opérations de *phishing*, par le biais de *tweets* adaptés aux habitudes d'une cible[50]. La DARPA, l'agence de recherche du *Pentagone*, a lancé en 2016 un challenge cyber pour tester la capacité de systèmes d'IA à détecter des failles au sein de logiciels et à les corriger. Si les performances du logiciel *Mayhem*, vainqueur de cette compétition, n'égalent pas les compétences des spécialistes de recherche de vulnérabilités présents à la conférence *DEF CON 2016*[51], il est vraisemblable que les machines dépassent les meilleurs experts mondiaux d'ici peu de temps.

La maitrise des systèmes d'intelligence artificielle appliquée à la cyberdéfense est donc un enjeu majeur pour la France car, utilisées en appui des experts étatiques, ces machines en augmenteront considérablement l'efficacité. Or, si la recherche française en matière d'IA est à la pointe dans de nombreux domaines, elle n'est malheureusement que peu mobilisée sur les objectifs liés à la cybersécurité. En lien avec notre industrie, il conviendrait donc d'initier un effort pour corriger cette situation, notamment dans les domaines de la détection d'attaque, de la recherche de vulnérabilité, de l'analyse et de la catégorisation de logiciels malveillants.

Au-delà des actions classiques de soutien à la recherche, l'accès à des jeux de données de qualité, actualisées et catégorisées, constitue un déterminant majeur de la recherche en matière d'intelligence artificielle. Dans son application à la cyberdéfense, force est de constater que les jeux de données publiquement accessibles concernant des attaques informatiques et des codes malveillants sont de taille réduite et de qualité médiocre. Si certains acteurs privés (éditeurs d'antivirus ou de solutions de détection en particulier) disposent de corpus de données de grande qualité, ceux-ci ne sont généralement pas partagés, et les acteurs concernés sont en majorité non européens. La consolidation des jeux de données publics, et l'accès par les chercheurs, sous des conditions à déterminer, aux jeux de données détenus par les acteurs privés et l'État, constituent à ce titre des enjeux capitaux.

[50] https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter.pdf

[51] https://www.computerworld.com/article/3105044/security/mayhem-supercomputer-takes-on-humans-at-def-con.html

3.1.4. Pour l'informatique en nuage, inventer une stratégie de régulation et de protection des données

La protection des données, véritable carburant de l'économie numérique, ne peut s'envisager qu'au niveau européen. Il sera notamment nécessaire de trouver un juste équilibre entre la bonne protection des données et leur libre circulation sur le territoire européen, qui est de nature à favoriser la pleine émergence d'un marché unique du numérique européen. Les États devront pouvoir conserver l'accès aux données, notamment les plus sensibles, qu'ils devront pouvoir continuer à réguler. Cette démarche ne pourra cependant être réellement pertinente qu'avec la mise en place d'une stratégie pour favoriser le développement des offres d'informatique en nuage de confiance.

Pour le seul hébergement de leurs données ou pour l'accueil d'applications complètes, les organismes tendent à déplacer une part croissante de leurs systèmes d'information vers des plateformes de *cloud* opérées par des prestataires tiers. L'externalisation vers un *cloud* est susceptible d'offrir des gains avérés au client, tant en termes de coût que de fiabilité et de flexibilité. Elle apporte par ailleurs une réponse séduisante à la complexité croissante de l'informatique et à la difficulté, pour de nombreuses organisations, de disposer de l'ensemble des compétences nécessaires.

Le développement du *cloud* est aujourd'hui accéléré par la stratégie adoptée par la majorité des éditeurs de logiciels, qui vise à les faire évoluer d'un modèle de commercialisation de produit (logiciel installé chez le client) à celle d'une prestation de service (accès du client au logiciel hébergé dans le *cloud* de l'éditeur). Cette évolution tend à se généraliser, y compris pour des logiciels hautement spécialisés et particulièrement critiques, tels ceux qui assurent le routage centralisé des flux réseau des opérateurs de communications électroniques.

Pour certains organismes ne disposant pas de compétences internes suffisantes (PME par exemple), le recours au *cloud* peut s'avérer bénéfique à leur sécurité informatique. Il peut en effet apporter une certaine résistance aux attaques informatiques non ciblées et de niveau technique modéré. Le recours au *cloud* est néanmoins porteur de risques nouveaux et la forte domination du marché du *cloud* par un nombre réduit d'acteurs étrangers, essentiellement américains et dans une moindre mesure chinois (mais dont la taille et le nombre ne cessent de croître), confère à ces risques une dimension de souveraineté nationale.

Sur le plan juridique d'abord, le recours au *cloud* pose la question du droit applicable aux données et applications hébergées, dès lors que l'hébergement est effectué hors du territoire national ou européen, ou que la nationalité du prestataire le soumet à des contraintes juridiques dont la portée peut comporter un caractère extraterritorial. Outre la problématique d'accès illégitime aux données qui pourrait en découler, il convient d'envisager également la possibilité pour des utilisateurs de *cloud* de se soustraire à certaines dispositions contraignantes du droit national, notamment en matière de cybersécurité.

Sur le plan technique ensuite, le recours au *cloud* peut offrir au prestataire la maîtrise complète des données et logiciels que lui confient ses clients. Un prestataire malveillant

pourrait ainsi, à son initiative ou à la demande d'un État, porter atteinte à la confidentialité des données (espionnage), mais aussi à leur disponibilité (sabotage). Le prestataire pourrait également être lui-même victime d'une attaque informatique, avec les mêmes conséquences. Ce risque est particulièrement prégnant lorsque les systèmes hébergés dans le *cloud* pourraient en cas de dysfonctionnement provoquer la déstabilisation d'un acteur économique, voire d'un État.

Sur le plan économique enfin, l'externalisation vers le *cloud* peut conduire à un risque de dépendance technologique accrue envers le prestataire. Ainsi, la commercialisation des logiciels sous la forme de service[52] dans le *cloud* transforme le client, jusqu'alors propriétaire du logiciel, en simple locataire, tributaire de la tarification imposée par son prestataire, et ce souvent sans recours par manque de solutions alternatives ou de réversibilité.

Les offres de *cloud* dites « souveraines », mises en place par des opérateurs nationaux financés par l'État, auraient pu apporter une réponse au problème stratégique de localisation du *cloud* et de confiance envers son opérateur. Cependant, ces offres peinent à établir leur viabilité économique. En revanche, il convient de noter que d'autres opérateurs nationaux de *cloud* parviennent à demeurer compétitifs et maîtres de leur solution technologique, que ce soit sur le marché général de l'hébergement ou sur un marché de niches.

Au cours des dernières années, plusieurs grands fournisseurs de *cloud* extra-européens ont par ailleurs établi des partenariats avec des opérateurs européens, permettant aux seconds de commercialiser les solutions des premiers en en assurant l'hébergement. L'accord conclu entre *DEUTSCHE TELEKOM* (*DT*) et *MICROSOFT* en constitue le cas le plus emblématique. Etabli à l'instigation du gouvernement allemand pour répondre à des préoccupations de sécurité, cet accord permet à *DT* d'héberger les solutions logicielles *cloud* de *MICROSOFT* dans ses propres centres de données et de les commercialiser, notamment au profit des administrations allemandes. En France, *OVH* se positionne également comme hébergeur de certaines solutions *MICROSOFT*.

Face à ces constats, la présente revue propose de mettre en œuvre les quatre séries de mesures ci-après.

1. Etablir, en lien avec les travaux conduits au titre du programme *Action Publique 2022*, une politique globale de recours au *cloud* par l'État, en combinant le recours aux solutions de *cloud* sous maîtrise de l'administration et celui aux prestataires de *cloud* bénéficiant d'une qualification par l'ANSSI (*SecNumCloud*).

2. Encourager en parallèle le développement de solutions de chiffrement pour le *cloud*. Les techniques de chiffrement actuelles ne répondent qu'à des cas d'usage du *cloud* très simples, principalement liés au stockage, mais présentent néanmoins un intérêt indéniable, par exemple pour des dispositifs de sauvegarde externalisés. Par ailleurs, le développement

[52] Par exemple, le remplacement du logiciel *Microsoft Office* par le service *cloud Office 365*.

de moyens de chiffrement extensibles à d'autres usages, notamment les techniques de chiffrement dites « homomorphes », qui permettent le traitement dans le *cloud* de données chiffrées, et non plus leur seul stockage, devrait rester un axe prospectif prioritaire.

3. Soutenir l'autonomie stratégique européenne sur le sujet, tant en investissant dans les technologies de rupture du domaine susceptibles de faire émerger les champions de demain, qu'en veillant par des mesures fiscales à rétablir l'équité entre les acteurs européens et certains de leurs concurrents qui échappent largement à l'impôt ou qui ne sont pas soumis à la même règlementation.

4. Etablir un cadre de confiance global pour permettre aux entreprises, aux collectivités et aux particuliers d'évaluer les risques d'utilisation et orienter le marché par le développement de la qualification *SecNumCloud*, y compris au niveau européen.

3.1.5. Réguler la production et l'exportation des armements et des activités offensives cyber

L'émergence des enjeux de cybersécurité et la volonté d'un nombre croissant de pays de disposer de capacités cyber offensives conduisent de nombreux industriels à développer de tels moyens. Dans le même temps, le caractère immatériel de ces technologies rend les contrôles difficiles, lorsque ceux-ci existent. Limiter la prolifération des technologies offensives, notamment en maintenant le principe d'une applicabilité du contrôle des armes et des technologies à double usage au domaine cyber représente donc un enjeu clé pour la stabilité du cyberespace.

En 2013, la catégorie des « logiciels d'intrusion » a été intégrée à la liste des biens à double usage de l'Arrangement de Wassenaar. Trois nouvelles entrées de contrôle ont été incluses dans cet accord international : les systèmes (*hardware*), les logiciels (*software*) et les technologies permettant le développement et l'usage des logiciels d'intrusion. Cette évolution a permis de poser les premiers jalons d'une régulation du commerce mondial des outils offensifs cyber. La modification de la liste de Wassenaar a été intégrée en 2014 à la liste des biens à double usage de l'Union européenne. La mise en œuvre de ce contrôle permet aux autorités nationales de s'assurer des conditions d'utilisation finale des capacités exportées et ainsi de refuser les opérations qui pourraient être considérées comme risquées. Certains pays participant à l'Arrangement de Wassenaar, comme les Etats-Unis, n'ont quant à eux pas encore transposé ni mis en œuvre ces nouveaux contrôles et plaident pour un assouplissement de ces règles.

Il importe aujourd'hui de consolider cette évolution en œuvrant à l'approfondissement du régime de contrôle des exportations dans le domaine cyber. Deux options peuvent être envisagées afin de poursuivre le travail engagé jusqu'ici. La première est la promotion d'une norme universelle de comportement par laquelle les Etats s'engageraient à contrôler les exportations des outils et techniques offensifs cyber selon des modalités à définir. La mise en œuvre de cette norme devrait être adaptée à la capacité des autorités nationales compétentes à exercer un contrôle efficace et harmonisé et respecter les intérêts légitimes des entreprises

de cybersécurité et du monde de la recherche. La seconde option est de considérer l'opportunité d'inscrire certains logiciels à la liste des matériels de guerre, dès lors qu'ils ne sont pas uniquement conçus pour s'introduire ponctuellement dans un système mais pour y perdurer ou endommager leur cible, constituant ainsi une véritable « arme numérique ».

Pour mettre en œuvre ces mécanismes de régulation il est indispensable d'essayer de catégoriser ces outils. Les outils sont des logiciels ou des ensembles de logiciels qui peuvent trouver des applications multiples que ce soit pour éprouver la sécurité d'un système dans un but défensif, pour mener des activités d'intrusions à des fins de renseignement, d'entrave ou encore dans un but purement lucratif pour dérober de l'argent ou des données qui pourront ensuite être monnayées. Un outil d'intrusion pour extraire du renseignement peut aussi très facilement être enrichi de quelques lignes de code pour devenir un instrument de destruction très efficace. Dans ces conditions, il est difficile de distinguer, parmi ces outils, ceux qui peuvent être qualifiés d'armes numériques et, à ce titre, être contrôlés comme le sont, pour leur fabrication et leur commercialisation, les armes de guerre.

Il est cependant possible de classer les logiciels de cyberdéfense en quatre catégories permettant de fixer des règles relatives à leur production, leur emploi et leur exportation :

1. La première catégorie regroupe les « outils d'intrusion de sécurité ». Ces logiciels qui permettent de pénétrer discrètement un système et d'en exfiltrer ou modifier une information sont commercialisés afin de tester la robustesse d'un système d'information. Ce type d'outils n'a pas vocation à intégrer des codes exploitant des vulnérabilités *zero-day* ni des charges capables de détruire un système. Conçus pour des opérations relativement limitées, ces outils ne comportent pas de fonctionnalités très évoluées. Ce type de produit rentre néanmoins dans la classe des biens à double usage, dans la mesure où, légèrement modifié, il peut être transformé en un logiciel destructif. Il demeure cependant un outil manuel d'intrusion ponctuelle.

2. Les « outils de captation de données », qui permettent de récupérer massivement des données individuelles, par exemple issues de smartphones ou d'ordinateurs personnels et de les traiter de manière quasiment automatique constituent une deuxième catégorie. Ces outils peuvent comporter des fonctions d'exploitation de *zero-day* et de pilotage. Ils peuvent être installés sur un temps long mais ne sont pas destinés à pénétrer des systèmes d'information complexes. Ces outils, déployés dans un cadre légal, sont utiles à la police et à la justice. La captation de données à la source permet en effet de surmonter certains obstacles auxquelles se heurtent les interceptions légales effectuées par les opérateurs, notamment en cas de chiffrement des applications utilisées pour communiquer. La dangerosité de tels outils suppose un étroit contrôle de leur diffusion.

3. La troisième catégorie correspond à des « armes informatiques ciblées ». Ces outils, aux fonctionnalités avancées, permettent de prendre le contrôle sur un temps long de systèmes variés mais ciblés, en permettant une exploitation du renseignement ou une destruction du système au moment souhaité. Leurs finalités combinent celles des deux

premières catégories, ce qui en termes d'emploi et d'effet ne peut être obtenu par une simple superposition des outils des deux premières catégories. Beaucoup plus sophistiqués, leur création suppose des développements *ad hoc*. Ils correspondent à des outils utilisés par les groupes d'attaquants les plus avancés.

4. La dernière catégorie est constituée des « armes informatiques massives », permettant de prendre le contrôle ou de détruire un nombre important d'équipements. Il peut s'agir de logiciels malveillants pouvant se répliquer et se propager de manière autonome sans ciblage précis. Ces outils sont particulièrement nocifs de par les risques de dommages collatéraux non maîtrisés qu'ils génèrent.

La plupart des logiciels et produits, ressortissant de ces quatre catégories sont contrôlés comme des biens à double usage dans notre législation[53] ou règlementés comme des outils pouvant porter atteinte à la vie privée (articles R226-1 à R226-12 du code pénal). L'article 323-3-1 du code pénal interdit en outre la détention ou la mise à disposition d'outils permettant de s'introduire dans un système de traitement automatisé de données hors motif de recherche ou de sécurité informatique.

Moins par son caractère rigoureux que du fait de sa complexité, cette réglementation n'a pas incité les entreprises françaises à investir dans le développement d'armes informatiques, voire d'outils d'intrusion ou encore de captation de données. Pourtant, des pays comme les États-Unis, Israël ou l'Inde se sont dotés d'une industrie dans ce domaine qui se lance aujourd'hui à la conquête du marché mondial. Certains produits vendus par des entreprises étrangères, bien que n'étant pas qualifiées « de confiance », présentent un intérêt certain pour les services de renseignement, de police ou de justice. Ces logiciels permettent en effet d'assurer la captation de données avec des mises à jour régulières qui les adaptent aux évolutions des terminaux commercialisés. Les pays européens ne sont d'ailleurs pas en reste. Des entreprises anglaises, italiennes ou allemandes ont ainsi créé des outils de captation performants, quoique pas toujours suffisamment durcis[54]. Cette situation européenne doit être d'autant plus soulignée que la plupart des pays membres de l'Union européenne, dont la France, sont engagés dans la lutte contre le terrorisme et les grands trafics et ont, à ce titre, autorisé dans leur législation la mise en place de systèmes de captation électronique aux fins d'espionnage des réseaux criminels et djihadistes. Le marché européen apparait aujourd'hui comme suffisant pour viabiliser les industriels qui fabriquent ce type de produits et créer une concurrence entre acteurs, tout en évitant que ces produits soient détournés à des fins malveillantes. Des mesures visant à protéger ces industriels vis-à-vis de prises de contrôle par

[53] Décret n°2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage modifié par le décret n°2010-292 du 18 mars 2010

[54] Ainsi, les deux leaders européens (l'italien *HACKING TEAM* et le germano-anglais *GAMMA*) ont subi récemment des intrusions informatiques démontrant le faible niveau de sécurité de leurs systèmes. Les attaquants leur ont dérobé l'ensemble de leurs données et les ont publiées sur internet, révélant à la fois l'identité de leurs clients et leur savoir-faire.

des capitaux étrangers sont aussi indispensables.

Alors que le besoin n'est pas discutable, nous sommes confrontés au double risque d'utiliser des produits de captation insuffisamment sécurisés, ou qui ne sont pas jugés de confiance. Ainsi, lorsque les outils développés par la société italienne *HACKING TEAM* ont été rendus publics à la suite d'un vol de leur code source, il est apparu que la société avait caché un piège dans tous les outils de captation de données de leurs clients. Il apparait donc aujourd'hui nécessaire d'harmoniser la fabrication, l'importation et l'exportation de ces outils, sauf à prendre le risque de livrer ce marché particulièrement sensible à des fournisseurs non européens.

La France pourrait promouvoir, notamment au sein de l'Union européenne, une approche de réglementation en matière de production et d'exportation de logiciels de cyberdéfense s'articulant autour des quatre catégories de produits introduites plus haut :

- le traitement des outils de première catégorie en tant que biens à double usage pose question dans la mesure où d'autres Etats n'appliquent pas ce contrôle. L'adopter unilatéralement reviendrait à pénaliser nos industriels vis-à-vis d'autres acteurs. Ces outils pourraient ainsi être fabriqués en toute liberté en Europe, en respectant un code déontologique, et utilisés par le secteur privé dans une logique restreinte aux tests de sécurité. Leur exportation hors de l'Union européenne devrait s'accompagner de règles d'utilisation et pouvoir être contrôlée *a posteriori* ;
- les outils de deuxième catégorie pourraient être fabriqués par des industriels soumis à des obligations de transparence et de contrôle, pour des usages exclusivement sous responsabilité gouvernementale. L'importation et l'exportation de ces produits hors de l'Union européenne pourraient être interdites, ou *a minima* strictement encadrées ;
- les outils de troisième catégorie pourraient être développés uniquement sous responsabilité étatique et utilisés uniquement par l'Etat ;
- la fabrication et l'utilisation des armes de quatrième catégorie seraient prohibées.

3.2. La régulation de la cybersécurité

Garant de la cybersécurité de la société, l'Etat intervient dans ce domaine comme prescripteur, réformateur et pourvoyeur de solutions de sécurité. Aux côtés du Parlement qui édicte la loi, le gouvernement joue un rôle normatif dans le domaine de la cybersécurité.

Chargé d'animer et de coordonner les politiques publiques concourant à la stratégie de sécurité nationale, le SGDSN, qui relève du Premier ministre, est ainsi un opérateur de sécurité en matière cyber. C'est lui qui propose au Premier ministre et met en œuvre la politique gouvernementale en matière de sécurité des systèmes d'information. Il dispose à cette fin de l'ANSSI, qui lui est rattachée.

En collaboration avec les administrations compétentes, l'ANSSI instruit et prépare les

décisions gouvernementales relatives à la sécurité du numérique et à celle des données sensibles. Elle participe également à la construction et à la maintenance des réseaux et des terminaux sécurisés pour les services de l'État. L'agence accompagne ainsi les cabinets du Président de la République, du Premier ministre et des membres du Gouvernement dans la sécurisation de leurs systèmes d'information. Au titre de son rôle normatif, elle est chargée de la définition de normes de sécurité, de la délivrance de visas de sécurité et de la qualification de prestataires de service.

Des réflexions menées dans le cadre de la présente revue, s'est dégagée la nécessité d'améliorer le cadre actuel de certification afin de contribuer à l'amélioration de la sécurité des produits.

3.2.1. Le rôle normatif de l'ANSSI

La définition des normes de sécurité

Créée pour doter l'Etat d'une administration faisant autorité sur les questions de cybersécurité, l'ANSSI s'est construite autour d'une expertise scientifique et technique à l'état de l'art, enrichie encore par l'expérience acquise au fil du traitement de cyberattaques au plus haut niveau de sophistication. Forte de sa mission et de ses compétences, l'ANSSI s'est naturellement imposée comme référent pour la définition des normes de sécurité pertinentes pour assurer la protection des données et des systèmes d'information les plus sensibles, à commencer par la protection du secret de la défense nationale.

Pour ces mêmes raisons, l'ANSSI a été chargée de négocier les normes de sécurité visant à assurer la protection des données et les systèmes d'informations classifiées dans des cadres multinationaux (par exemple au sein de l'organisation de l'Atlantique nord, au sein de l'Union européenne, ...).

Cette activité normative s'est étendue progressivement au fil du temps et en même temps que l'affirmation de son rôle d'autorité nationale, pour couvrir notamment :

- la protection des échanges numériques entre les citoyens et l'administration d'une part et entre administrations d'autre part, par voie d'ordonnance au travers du référentiel général de sécurité (RGS) ;
- la sécurité des systèmes d'information de l'Etat, par voie de circulaire du Premier ministre au travers de la politique de sécurité des systèmes d'informations (PSSIE) ;
- la protection des informations sensibles de l'Etat (instruction interministérielle 901) ;
- la protection des systèmes d'information des OIV participant à soutenir leurs missions d'importance vitale, par voie législative et réglementaire au travers des articles 1332-6-1 à 1332-6-7 du code de la défense.

Plus récemment, l'ANSSI s'est vue confier la production d'une ordonnance et de décrets en Conseil d'Etat relatifs aux services de confiance dans le cadre de la loi pour une République numérique, s'agissant en particulier de l'identité électronique, du recommandé électronique

et des coffres forts numériques.

Enfin, l'ANSSI a participé, en tant que chef de file au niveau national, à la négociation des réglementations européennes suivantes et à en assurer l'interprétation ou la transposition au niveau national :

- le règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, dit règlement « eIDAS » ;
- la 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 directive « NIS ».

L'impact désormais avéré des réglementations portées ou négociées par l'ANSSI conforte le choix de confier à l'autorité nationale la définition des normes juridiques spécifiques à la sécurité numérique. Ceci vaut en particulier lorsqu'il s'agit de développer la confiance dans les usages numériques. A cet égard, la décision de désigner l'ANSSI comme autorité pour la de certification des moyens d'identité électronique va certainement dans le bon sens.

En outre, alors que la transformation numérique bat son plein, que les ruptures en termes technologiques et d'usages s'enchaînent dans le numérique, et dans la mesure où la sécurité numérique - condition essentielle de la confiance dans la transformation numérique - reste aujourd'hui peu régulée, il n'y a pas lieu de considérer que l'on est confronté à un empilement de normes dans le champ de la sécurité numérique. Dans ce contexte, il semble que les directives gouvernementales préconisant que la mise en place de toute nouvelle norme s'accompagne de la suppression de deux normes déjà existantes devraient connaître en l'espèce une exception pour le domaine de la sécurité numérique.

En accompagnement de cette exception l'ANSSI devra, dans les nouvelles normes qu'elle sera amenée à proposer, ainsi que dans la révision des normes existantes, porter une attention particulière à garantir la proportionnalité, la cohérence et la lisibilité des réglementations en matière de sécurité numérique, afin d'en simplifier la mise en œuvre par les organisations soumises à plusieurs d'entre elles.

Enfin, il apparaît que le respect des normes édictées par l'ANSSI est parfois insuffisant pour deux raisons. D'une part, à l'exemple du référentiel général de sécurité, la mise en œuvre des régimes de sanctions existants n'est parfois que difficilement envisageable car celles-ci sont trop peu proportionnées et ne permettent pas d'escalade. D'autre part, à l'exemple de la politique de sécurité des systèmes d'information de l'Etat publiée par voie de circulaire, le niveau des normes est parfois insuffisant dans la hiérarchie des normes. Une attention particulière devrait ainsi être portée à l'amélioration de l'efficacité des normes définies par l'ANSSI en garantissant des régimes de sanctions pertinents et des niveaux de normes les plus adaptés.

Les visas de sécurité

L'ANSSI délivre depuis de nombreuses années, sur la base d'évaluations approfondies lancées à l'initiative des fournisseurs concernés, des visas de sécurité portant sur une typologie étendue de produits de sécurité : matériels ou logiciels, réalisant des fonctions de chiffrement, de signature électronique, d'interconnexion entre réseaux sécurisés, d'authentification, etc. Ces visas sont essentiellement de trois types distincts :

- la certification atteste de la robustesse d'un produit de sécurité au regard des exigences (nature des fonctions de sécurité, niveau de l'attaquant) fixées par un commanditaire, qui n'est pas nécessairement l'État. Elle se présente ainsi comme une boîte à outils permettant à divers donneurs d'ordres (État, opérateurs privés - banques par exemple -, autorités indépendantes) de définir leurs critères de sécurité et de faire vérifier par un tiers la satisfaction de ces critères ;
- la qualification par l'État vaut recommandation d'usage dans un contexte donné ; elle implique une certification du produit complétée par la vérification d'impératifs de sécurité et d'actualisation réclamés aux fournisseurs dans la durée. La qualification vaut tant pour les besoins propres des administrations et services de l'État que pour ceux des OIV ;
- l'agrément est une décision réglementaire qui autorise l'utilisation d'une solution préalablement qualifiée au traitement d'informations classifiées.

Les méthodes appliquées par les centres d'évaluation privés certifiés par l'ANSSI, ont largement démontré leur pertinence en termes de garantie et de réactivité. Le cadre général de délivrance de visas de sécurité mis en place par l'ANSSI constitue en outre un levier très important pour le développement de la sécurité des produits fabriqués ou déployés en France.

Cependant, les besoins d'évaluation de produits de plus en plus variés s'accroissent. Il s'agit non plus uniquement de produits conçus spécifiquement pour assurer une fonction de sécurité des réseaux informatiques mais aussi des automates industriels, des objets connectés, etc. Si le cadre d'évaluation existant a pu être étendu avec succès à une proportion significative de ces nouveaux besoins, il est en revanche totalement inadapté à l'évolution prévisible des demandes de certification et de qualification futures.

Les prestataires

En complément de la qualification des produits, l'ANSSI a établi plus récemment un dispositif de qualification des prestataires de services, de sécurité informatique portant sur leur niveau de sécurité (compétence, la sécurité de leur propre système d'information, le cloisonnement des données client, ainsi que sur des engagements de qualité de service, définies dans des référentiels métiers.

Cette qualification concerne des prestataires de cybersécurité : *Prestataires d'audit en sécurité des systèmes d'information* (PASSI), *Prestataires de détection d'incidents de sécurité* (PDIS) et *Prestataires de*

réponse à incident de sécurité (PRIS).

Elle s'applique aussi à des prestataires de service numérique sécurisé, qui apportent des garanties dans l'exécution d'un service numérique plutôt qu'une expertise spécifique à la cybersécurité. Cette catégorie regroupe les prestataires de confiance prévus au titre du référentiel général de sécurité et du règlement eIDAS (prestataires de signature électronique, de fourniture de certificats électroniques, d'horodatage, etc.), et les prestataires d'informatique en nuage (*cloud*)[55].

Les prestataires de cybersécurité sont qualifiés sur la base d'une évaluation de leur compétence métier, d'une part, et des mesures techniques et organisationnelles par lesquelles ils assurent la protection des données de leurs clients, d'autre part. Ils apportent des expertises similaires à celles mises en œuvre par l'ANSSI dans ses propres missions, et constituent de ce fait un important vecteur de diffusion du savoir-faire de l'ANSSI. Leur concours permet en outre de faire face aux besoins du secteur privé. Le processus de qualification PASSI a commencé en 2013 et l'on compte, fin 2017, cinquante prestataires qualifiés ou en cours de qualification. Cette montée en puissance révèle à la fois le dynamisme de ce domaine d'activité et la recherche par les entreprises du secteur d'une accréditation par l'ANSSI.

Moins nombreux, les prestataires de service numérique sécurisés sont quant à eux évalués par l'ANSSI selon une logique de conformité à un référentiel fixant les exigences de sécurité applicables au service qu'ils délivrent.

3.2.2. Améliorer le cadre de certification pour améliorer la sécurité des produits

Le cadre de certification existant, quoique modulant le niveau d'exigence en fonction des besoins de sécurité, n'en demeure pas moins très centré sur des certifications à haut niveau. Il est mal adapté à l'évaluation de produits d'utilisation courante (à l'image des objets connectés), pour lesquels il présente un coût et des délais rédhibitoires.

C'est pourquoi la présente revue propose la mise en place, en complément du cadre de certification existant, réservé aux produits et prestations en haut du spectre, d'une certification élémentaire de cybersécurité. Cette dernière pourrait s'inspirer de dispositifs existants dans des contextes autres que la cybersécurité, comme le marquage « CE » requis

---

[55]Le référentiel général de sécurité, pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, est le cadre règlementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens. Il a pour objet le renforcement de la confiance des usagers dans les services électroniques mis à disposition par les autorités administratives et s'impose ainsi à elles comme un cadre contraignant tout en étant adaptable et adapté aux enjeux et besoins de tout type d'autorité administrative.

Le Règlement « eIDAS » n°910/2014 du 23 juillet 2014 a pour ambition d'accroître la confiance dans les transactions électroniques au sein du marché intérieur. Il établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.

pour la commercialisation de certains biens ou services au sein de l'espace européen. Cette certification élémentaire de cyber-sécurité procéderait essentiellement d'une analyse de conformité, sur la base d'un cahier des charges prédéfini. Ce contrôle de conformité pourrait être délégué à un organisme privé, avec une implication des pouvoirs publics limitée à des actions indirectes (agrément des centres d'évaluation privés). Cette approche apparaît adaptée à des certifications pour lesquelles certaines obligations du dispositif actuel, comme la réalisation d'une analyse de vulnérabilité « libre », hors cahier des charges, et la délivrance de certificats par l'ANSSI, semblent moins justifiées.

En réduisant les coûts et délais de certification, cette réforme est de nature à favoriser l'émergence d'une offre de produits cohérente avec le besoin. La mise en œuvre d'un mécanisme de certification élémentaire pourrait s'appuyer sur certains prestataires de contrôle de conformité avec l'aide de l'ANSSI. L'autorité nationale de cybersécurité pourrait contribuer à la définition des protocoles de certification élémentaire, accréditer les centres d'expertise et d'évaluation, en animer le réseau notamment par des cycles de formation.

Après une première mise en place basée sur le volontariat, l'incorporation de cette certification élémentaire dans la réglementation, en intégrant par exemple des règles élémentaires de sécurité dans les directives européenne relatives aux biens visés par le marquage « CE » en augmenterait significativement la portée et l'impact, transformant un différenciateur optionnel en prérequis d'accès au marché.

Enfin, il peut être relevé que la mise en place de mécanismes d'auto-déclaration de conformité à des exigences de sécurité constitue une demande récurrente de nombreux fournisseurs de solutions numériques, qui en mettent en avant le coût minimal. Un cadre auto-déclaratif n'apporte que des garanties faibles de sécurité, et ne constitue par conséquent pas une priorité pour l'État. Pour autant, il serait contre-productif de s'opposer à l'émergence de tels schémas à l'initiative du secteur privé, en particulier lorsque cette démarche est portée par un ensemble représentatif de fournisseurs de solutions de sécurité. Un accompagnement *a minima* de telles initiatives par l'État, portant notamment sur la définition des cahiers des charges associés, favoriserait la diffusion des bonnes pratiques de développement, y compris dans des secteurs peu enclins à se tourner vers la certification.

3.2.3. La responsabilité par milieu : impliquer l'ensemble des acteurs sectoriels pour élever notre niveau de cybersécurité

Lorsque les intérêts de la Nation le justifient, notamment s'agissant de défense et de sécurité nationale ou de services essentiels au maintien d'activités sociétales ou économiques critiques, une approche trans-sectorielle du risque cyber s'impose. La responsabilité en est alors confiée à une autorité interministérielle, l'autorité nationale de sécurité et de défense des systèmes d'information. Une telle approche garantit une appréhension homogène et ambitieuse du risque, indépendante dans ses objectifs des spécificités sectorielles, permettant de réduire le risque cyber et de préparer la gestion d'une éventuelle crise majeure. Cette approche est avant tout destinée à garantir un niveau minimal de cybersécurité des entités

les plus critiques, afin de protéger les intérêts fondamentaux de la France face à la cybermenace.

Bien que trans-sectorielle, ce type d'approche nécessite dans sa mise en œuvre une coordination étroite entre l'autorité nationale et les acteurs-clés de la régulation sectorielle, tant les tutelles ministérielles que les éventuels services à compétence nationale, établissements publics[56] et autorités administratives indépendantes[57], afin d'assurer une bonne articulation entre les différentes politiques s'appliquant aux secteurs.

Néanmoins, les démarches trans-sectorielles ne permettent pas d'appréhender finement la gestion des risques propres à chaque secteur. En outre, la transformation numérique, qui conduit notamment à la connexion massive des objets à Internet (dispositifs médicaux, véhicules, bâtiments, villes…), impose désormais la prise en compte au niveau sectoriel du risque de cyberattaques, et ce particulièrement lorsque ces objets sont susceptibles d'avoir un impact direct et matériel sur la sécurité des personnes. En effet, seuls les acteurs sectoriels disposent des connaissances métier nécessaires pour qualifier les impacts d'une éventuelle attaque informatique sur ces objets et donc pour évaluer de manière pertinente le risque cyber associé à leur déploiement.

Ces constats mettent en évidence le besoin désormais impérieux pour les acteurs-clés de la régulation sectorielle d'appréhender le risque de cyberattaques au même titre que les autres risques et, le cas échéant après une analyse de risque réalisée par experts métier, d'adopter des mesures appropriées, par exemple en émettant des exigences de cybersécurité adaptées.

Sensibiliser les acteurs-clés de la régulation sectorielle au risque de cyberattaques

Les acteurs-clés de la régulation sectorielle ne disposent généralement pas d'expertise en matière de cybersécurité. A ce titre, la compréhension et la prise en compte du risque de cyberattaques par ces acteurs sont extrêmement peu développées, voire inexistantes. A l'heure de la transformation numérique, il leur faut désormais appréhender ce risque, en s'appuyant sur les méthodes d'analyse de risque disponibles et en faisant appel à une assistance externe, fournie par des prestataires qualifiés, voire par l'ANSSI elle-même, afin d'analyser les risques cyber pertinents au niveau sectoriel et d'identifier ceux qui méritent une action afin d'être réduits.

Fournir des outils aux acteurs-clés de la régulation sectorielle

Lorsque le bilan de l'exposition au risque de cyberattaques a été réalisé dans un secteur et a conclu à la nécessité de réduire certains risques via des exigences réglementaires, que ce soit au niveau national ou européen, les acteurs-clés de la régulation du secteur doivent être en

[56] Par exemple, l'*Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail* (ANSES), l'*Agence nationale de sécurité du médicament et des produits de santé* (ANSM), la *Direction de la sécurité de l'aviation civile* (DSAC).

[57] Par exemple, l'*Autorité de contrôle prudentiel et de résolutions* (ACPR), l'*Autorité des marchés financiers* (AMF), l'*Agence nationale des fréquences* (ANFR), l'*Autorité de régulation des communications électroniques et des postes* (ARCEP), l'*Autorité de sûreté nucléaire* (ASN), la *Commission de régulation de l'énergie* (CRE).

mesure de concevoir les mesures de cybersécurité nécessaires, d'exprimer simplement leurs exigences de cybersécurité au sein des réglementations sectorielles dont ils ont la charge, et de contrôler le respect des exigences.

Néanmoins, ces acteurs ne détiennent pas, et ne seront généralement pas amenés à détenir, d'expertise en matière de cybersécurité. Par conséquent, ils devraient pouvoir s'appuyer sur des outils leur permettant de définir leurs critères de sécurité et de faire vérifier par des tiers compétents la satisfaction de ces critères. Le cadre européen de certification de cybersécurité proposé en septembre 2017 par la Commission européenne, dans le cadre du « paquet cyber » conçu à cette fin et actuellement en cours de négociation, doit permettre de répondre à ce besoin.

Prioriser l'engagement de ressources de l'ANSSI dans ses travaux avec les acteurs-clés de la régulation sectorielle

En s'appuyant sur son expertise en matière de sensibilisation, et grâce aux outils et méthodes qu'elle a développés en matière de gestion du risque de cyberattaques, l'ANSSI est en mesure d'accompagner efficacement les acteurs-clés de la régulation sectorielle afin de leur permettre d'appréhender le risque cyber en général, d'analyser les risques correspondants au niveau sectoriel qui les concerne et d'identifier ceux appelant une action correctrice (réduction du risque et renforcement du niveau de cybersécurité).

Néanmoins, en tant qu'autorité nationale, la priorité de l'ANSSI doit demeurer la protection des intérêts fondamentaux de la France à travers une approche trans-sectorielle du risque. Il importe donc que l'ANSSI priorise ses actions d'accompagnement des acteurs-clés de la régulation sectorielle.

Trois critères concourent naturellement à déterminer le niveau de priorité que l'ANSSI doit accorder à l'accompagnement des acteurs d'un secteur à un instant donné : l'arrivée prochaine ou en cours d'un phénomène de rupture lié à la transformation numérique du secteur (par exemple, les véhicules autonomes), le niveau de la cybermenace à l'encontre du secteur, et le niveau de risque sur la sécurité des personnes.

3.2.4. Les prestataires de confiance : développer une offre de services de cyberdéfense

Les prestataires de cybersécurité couvrent actuellement, par les expertises spécifiques qu'ils apportent, trois des quatre étapes du cycle de vie d'un système d'information sécurisé : la vérification de sécurité (PASSI), la gestion dans la durée de la sécurité (PDIS) et la réaction aux attaques (PRIS). En revanche, aucun schéma de qualification ne porte sur les compétences nécessaires à l'étape initiale de conception d'un système d'information sécurisé. Il est par ailleurs à noter que les prestataires existants ne couvrent pas strictement toutes les compétences contribuant aux trois autres étapes : il n'existe par exemple pas de prestataire spécialisé dans l'homologation de sécurité (*cf. glossaire*), ou dans le maintien en condition de

sécurité[58].

Les prestataires d'assistance à maîtrise d'ouvrage

Il apparaît donc souhaitable de compléter le catalogue de prestataires de cybersécurité qualifiés par un nouveau type de prestataire spécialisé dans la phase initiale de conception d'un système d'information sécurisé. En effet, certaines expertises spécifiques mobilisées à cette étape du cycle de vie, en particulier celles portant sur l'analyse de risque et sur l'architecture de sécurité, sont peu répandues au sein des administrations et entreprises, et dans les faits déjà largement sous-traitées par ces entités à des prestataires d'assistance à maîtrise d'ouvrage. La mise en place d'un schéma de qualification centré sur ces métiers apporterait des garanties significatives en matière de compétence et de confiance dans ce recours à l'externalisation.

La qualification de niveau élémentaire

Les différents référentiels de qualification de prestataires de cybersécurité sont actuellement conçus de manière à répondre au niveau d'exigence élevé propre aux systèmes sensibles des administrations et aux systèmes d'information d'importance vitale des OIV. Ce positionnement se retrouve notamment dans les contraintes imposées en matière de sécurité des systèmes d'information sous-jacents à ces prestations, qui doivent être aptes à traiter des informations *Diffusion Restreinte*. Ce niveau d'exigence a des répercussions naturelles sur le prix des prestations associées, qui n'est par conséquent pas totalement adapté aux besoins d'autres entités, ou de systèmes d'information moins critiques, pour lesquels la nature de la menace ne justifie pas nécessairement un tel niveau de prestation.

Il y aurait par conséquent un intérêt à explorer les possibilités de qualifications moins exigeantes, pour des niveaux de prestations moins ambitieux correspondant mieux aux besoins des systèmes d'information non critiques des entreprises, administrations et collectivités. Les référentiels associés auraient naturellement vocation à couvrir les mêmes compétences que les qualifications existantes, mais en relâchant certaines contraintes notamment d'architecture et de sécurité des systèmes d'information associés aux prestations.

À l'instar du dispositif de certification élémentaire proposé plus haut pour les produits, le rôle que l'État serait amené à jouer dans un tel cadre de qualification élémentaire de prestataires resterait à préciser. Une implication des pouvoirs publics, mettant à profit tant leur expérience que leur connaissance de la menace, dans la définition des référentiels de qualification paraît pertinente *a priori*. En revanche, l'intérêt d'une implication étendue au fonctionnement du schéma de qualification, une fois celui-ci établi, est plus discutable : ces qualifications pourraient potentiellement être déléguées à des acteurs privés spécialisés, l'État se bornant à vérifier l'aptitude de ces derniers à conduire des qualifications.

[58] Il convient cependant de souligner que ces compétences non couvertes relèvent plus particulièrement des obligations de l'entité responsable du système d'information, et sont par conséquent difficilement externalisables.

3.2.5. Le développement de la qualification de prestataires de services numériques sécurisés

Les prestataires de services numériques sécurisés qualifiés à ce jour se concentrent principalement dans des secteurs d'activité très spécifiques, liés notamment à la signature électronique. Une extension des assurances apportées par ces qualifications à des activités numériques plus généralistes semble pertinente, notamment du fait de l'apport important qu'elle pourrait avoir sur la sécurité d'entités qui externalisent très largement leur utilisation du numérique.

Les prestataires de cloud

Le développement de l'informatique en nuage (*cloud computing*) est une évolution très structurante des systèmes d'information. Outre ses avantages économiques ou fonctionnels, le *cloud* constitue une solution très attrayante pour des entités ne disposant que de compétences informatiques limitées, qui peuvent trouver chez les fournisseurs de *cloud* un socle de système d'information bien mieux maîtrisé que celui qu'elles seraient susceptibles de mettre elles-mêmes en place. En revanche, ce développement du *cloud*, entraînant une externalisation massive des systèmes d'information, et leur concentration sous le contrôle des principaux fournisseurs de *cloud*, crée un besoin renforcé de confiance envers ces fournisseurs. Ce constat a motivé l'élaboration par l'ANSSI du schéma de qualification de prestataires de *cloud* dénommé *SecNumCloud*.

La version définitive du référentiel associé ayant été rendue publique en septembre 2017, les premières qualifications devraient être prononcées courant 2018. Ce référentiel fixe un ensemble d'exigences techniques, juridiques et contractuelles qui déclinent, dans le contexte du *cloud*, les bonnes pratiques de sécurité numérique. La qualification *SecNumCloud* n'est en revanche adossée à aucune exigence réglementaire, et son attractivité pourrait être améliorée afin d'amener plus d'acteurs du *cloud* à consentir les efforts nécessaires à leur mise en conformité avec le référentiel. Outre le levier de la commande publique - relativement limitée à ce jour au demeurant - en matière de *cloud*, un facteur d'attractivité significatif pourrait être trouvé dans un rapprochement des exigences du référentiel avec les contraintes issues du nouveau règlement européen sur la protection des données personnelles (RGPD), entrant en vigueur mi-2018, qui aura un effet très structurant sur ce secteur d'activité.

Les prestataires d'infogérance

L'infogérance constitue un modèle alternatif et complémentaire à l'informatique en nuage : au lieu d'externaliser son système d'information dans un *cloud*, le client externalise la seule gestion (administration, mises à jour, supervision) de son système d'information, qui reste par ailleurs physiquement sous son contrôle. La qualité du service d'infogérance peut constituer un puissant levier pour améliorer le niveau de sécurité des clients de ce service, qui n'ont généralement par ailleurs pas la capacité de se sécuriser eux-mêmes. C'est pourquoi la mise en place d'un schéma de qualification des prestataires de service en infogérance sécurisée apparaît nécessaire.

3.2.6. La mise en place d'un cadre de certification harmonisé à l'échelle européenne

Un facteur important du manque d'attractivité de la certification de sécurité pour certains cas d'usage est le manque de reconnaissance internationale des certificats délivrés, au regard des investissements consentis pour obtenir ces certificats. En effet, les certifications établies en France au titre de la norme dite des « Critères Communs » ne bénéficient que d'une reconnaissance partielle au titre d'accords internationaux, notamment l'accord SOG-IS permettant la reconnaissance mutuelle entre 14 États européens, tandis que celles relevant de la *Certification de sécurité de premier niveau* (CSPN), moins coûteuses, ne sont reconnues qu'en France.

La Commission européenne a présenté, le 13 septembre 2017, un paquet de mesures relatives à la cybersécurité, qui propose notamment l'établissement d'un cadre réglementaire européen de certification de la sécurité des produits et services numériques. Cette initiative offre une opportunité unique d'harmoniser au niveau européen la certification de sécurité, et d'assurer par conséquent une reconnaissance étendue à l'ensemble des États membres, gage d'une plus grande attractivité. Les travaux de la Commission en la matière doivent donc être encouragés et soutenus.

Il conviendra cependant de veiller à ce que ce nouveau cadre et son implémentation pérennisent l'expérience acquise par les États membres précurseurs en matière de certification, dont la France, et intègre les bonnes pratiques établies à ce titre. En particulier, outre des certifications de conformité élémentaire selon les orientations présentées au paragraphe précédent, le cadre européen devra incorporer une composante de certification apte à répondre au plus hauts niveaux d'exigences de sécurité, indispensable à satisfaire les besoins des États et des activités industrielles les plus exposées, et intégrer à cette fin les principes essentiels qui garantissent l'efficacité du dispositif actuel et son adaptation au besoin.

Par ailleurs, il conviendra également de veiller à ce que l'harmonisation européenne n'obère pas la capacité nationale à délivrer des qualifications de sécurité, incorporant des critères complémentaires, pour répondre aux besoins relavant de la sécurité nationale.

Comme la qualification des produits de sécurité, celle des prestataires de service relève d'un dispositif national sans reconnaissance internationale, à la seule exception près des prestataires de confiance qualifiés au titre du règlement eIDAS. Cependant, une extension, totale ou partielle, du modèle français de qualification de prestataires présenterait une double utilité, en renforçant l'attractivité du dispositif pour des prestataires implantés sur l'ensemble du marché européen, d'une part, et en contribuant à améliorer significativement la sécurité du marché unique du numérique, d'autre part.

Une telle extension paraît tout particulièrement pertinente dans le domaine des prestataires de services numériques sécurisés, dans la mesure où les fournisseurs concernés ont généralement un marché et une offre étendus à l'ensemble du marché européen, voire à

l'échelle mondiale pour les principaux prestataires de *cloud*. Par ailleurs, la sécurité de ces services numériques constitue un volet important de la directive européenne *Network Information Security*, et un dispositif de validation de cette sécurité trouverait par conséquent toute sa place dans la mise en application de cette directive à partir de mi-2018. Enfin, les exigences portées par ces qualifications, et les procédures de vérification associées, semblent assez facilement intégrables dans le cadre harmonisé de certification de produits et de services récemment proposé par la Commission européenne. Dans ce cas de figure particulier, la qualification nationale deviendrait sans grande difficulté une certification au niveau européen.

La pertinence et la faisabilité d'une extension européenne des qualifications de prestataires de cyberdéfense paraît plus discutable au premier abord : les métiers correspondants constituent plus généralement des services de proximité, dont le marché demeure souvent local. Par ailleurs, la spécificité de ces qualifications, qui impliquent nécessairement une évaluation des compétences métier des prestataires, et non pas seulement d'exigences techniques ou organisationnelles sur leur système d'information, rend leur harmonisation au niveau multinational beaucoup plus complexe. En particulier, de telles évaluations semblent difficilement intégrables en l'état dans le cadre de certification proposé par la Commission européenne, qui nécessiterait des adaptations significatives pour permettre des tests de compétence.

Cependant, une extension européenne de ces qualifications présenterait un intérêt incontestable du fait notamment du large recours des institutions européennes à de tels prestataires, au travers de marchés sur lesquels une portion significative des prestataires qualifiés en France sont généralement candidats. La reconnaissance, *a minima*, des qualifications de prestataires de cybersécurité par les institutions européennes présenterait ainsi un double intérêt de valorisation des investissements consentis par les prestataires qualifiés, d'une part, et d'amélioration de la sécurité des institutions européennes, d'autre part.

3.3. L'économie de la cybersécurité

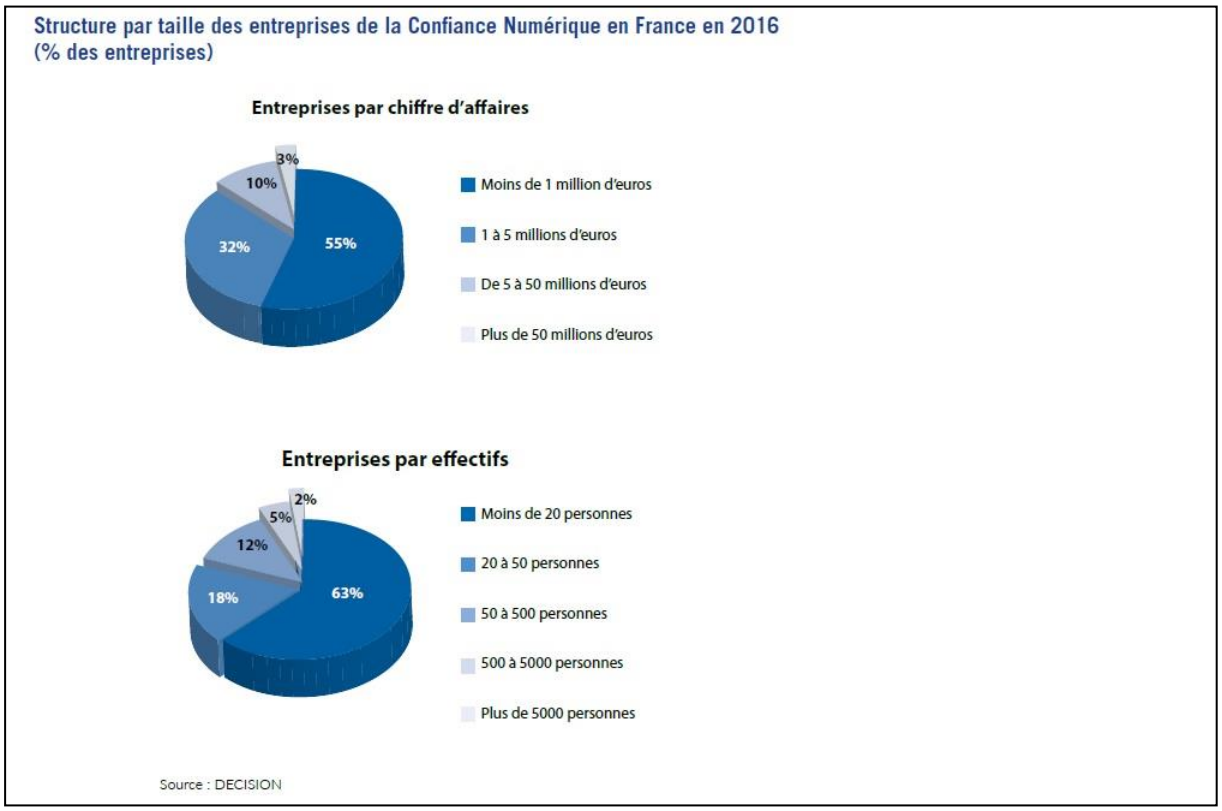
Pour assoir sa souveraineté numérique, la France devrait se doter d'une véritable stratégie industrielle. Une telle démarche passerait par l'identification des objectifs à atteindre en matière d'offre industrielle nationale ou de confiance pour répondre aux besoins de la Nation dans le domaine de la cybersécurité et par la définition des moyens à mettre en œuvre pour atteindre ces objectifs.

A cet égard, les réflexions conduites dans le cadre de la présente revue amènent à envisager le renforcement dans plusieurs directions de la base industrielle française et la fondation d'une base industrielle de cybersécurité européenne. Elles montrent également la nécessité pour l'Etat de disposer de produits de sécurité performants et certifiés.

3.3.1. La base industrielle nationale

Aujourd'hui, le développement d'une industrie de confiance ambitieuse dans le domaine des produits et services de cyberdéfense est indispensable pour relayer et étendre l'action de l'Etat, que ce se soit au niveau national ou européen. Il s'agit de développer une capacité industrielle qui soit en mesure d'offrir des produits et services à la fois d'un très haut niveau de sécurité tout en étant viable économiquement.

L'industrie française de la cybersécurité peut se caractériser par la présence de quelques grands groupes avec une empreinte internationale importante et de nombreuses petites ou très petites entreprises. Il n'existe en effet quasiment aucune entreprise de taille intermédiaire, qui plus est dans le domaine des produits de cyberdéfense.



L'activité couverte par les grands groupes est construite autour de trois axes.

Le premier est lié aux besoins gouvernementaux de haut niveau de sécurité pour lesquels l'Etat français a décidé de maintenir une capacité souveraine, en particulier dans le domaine de la cryptographie et du chiffrement. Ces hauts besoins de sécurité ont permis de faire émerger une offre civile. La France possède ainsi des équipements qui lui garantissent une maîtrise de la sécurité de ses réseaux, y compris face à des attaquants de très haut niveau technique. L'offre civile nationale peine toutefois à s'imposer à l'étranger et gagnerait à être renouvelée.

Le deuxième axe est lié au domaine de la carte à puce, avec des acteurs historiques tels que *Gemplus*, *Schlumberger* ou *Oberthur*. Ces acteurs s'appuient aujourd'hui sur les compétences et savoirs acquis pour développer des solutions d'authentification et de gestion d'accès de premier plan mondial.

Enfin, les sociétés de service informatique françaises ont su se positionner au niveau mondial pour superviser la sécurité des réseaux de leurs clients et opèrent aujourd'hui dans le monde entier. Ces industriels intègrent aussi des solutions de cybersécurité dans les systèmes d'information qu'ils conçoivent ou qu'ils administrent.

Ces trois domaines ont vocation à se rapprocher comme l'illustre le rapprochement entre *BULL* et *ATOS* ou plus récemment celui de *GEMALTO* et *THALES*.

Parallèlement à l'activité couverte par les grands groupes, quelques experts se lancent dans la création de start-ups. Les financements disponibles et le manque d'expertise dans le domaine de la cybersécurité leur permettent de se développer y compris en l'absence de stratégie industrielle performante et sans être contraints à conquérir des marchés à l'international. En effet, les prestations d'expertise de haut niveau qu'ils peuvent fournir auprès de clients français suffisent la plupart du temps à faire vivre ces petites entreprises dont les coûts de structure peuvent être assez réduits. Toutefois, malgré ces compétences techniques avérées, le fait, pour ces PME de devenir les champions internationaux reste un défi.

Face à ces constats, la présente revue a identifié trois axes de progrès :

- inciter les grands industriels français du secteur à compléter leur offre de produits et de services de cybersécurité à destination du domaine civil, afin de leur permettre de devenir des champions internationaux de la cybersécurité ;
- favoriser la création d'entreprises de taille intermédiaire (ETI) en aidant les PME les plus performantes à croitre rapidement et à procéder à des acquisitions pertinentes. C'est aujourd'hui la seule option offerte pour permettre à ces dernières d'atteindre une taille les mettant en situation de concurrencer leurs homologues étrangers ou de conquérir le marché européen. L'Etat soutiendra et encouragera ces stratégies de croissance externe en mobilisant les fonds d'investissement intéressés par le domaine de la cyberdéfense ;
- démultiplier le nombre de startups en incitant et en soutenant les experts de l'administration ou des grandes entreprises à se lancer dans ce challenge. Afin d'atteindre cet objectif, il est indispensable que l'Etat soutienne la mise en place d'accélérateurs, de start-ups studios et plus généralement de structures d'accompagnement des start-ups dédiés à la cyberdéfense. Les efforts devront être concentrés sur les entreprises innovantes dont la stratégie peut leur permettre d'atteindre une empreinte mondiale.

3.3.2. Définir une politique industrielle de cybersécurité et construire une base industrielle de cybersécurité européenne

La construction d'une base industrielle de cybersécurité et de cyberdéfense se heurte aujourd'hui à deux difficultés.

La première est l'absence d'un réel marché européen de la cybersécurité, ce qui ne permet pas, contrairement à ce que l'on peut observer pour les entreprises américaines ou chinoises, la croissance des entreprises sur la base du seul marché intérieur. Cela est dû à la fois à une hétérogénéité des pratiques et des normes entre pays, à certaines contraintes existant au

niveau européen qui peuvent paradoxalement complexifier l'accès global au marché, mais aussi au fait que le marché européen reste aujourd'hui facilement accessible aux entreprises non-européennes.

La seconde difficulté est une certaine différence de conception entre Etats membres de l'Union européenne sur la nature d'une « entreprise européenne ». Pour certains, il s'agit simplement d'une entreprise disposant de bases solides sur le territoire européen ou d'un siège social en Europe. Pour d'autres, il s'agit au contraire d'entreprises qui appartiennent, de manière stable et dans la durée, à des investisseurs européens.

En outre, la question des entreprises européennes de confiance pose très clairement la question de la sphère de souveraineté et du lien entre souveraineté et développement économique.

Ces problématiques ne doivent cependant pas freiner la volonté de la France de favoriser la construction d'acteurs européens de la cybersécurité. Plusieurs axes d'effort pourraient permettre la constitution d'une telle industrie.

Le premier effort consiste à identifier les domaines pour lesquels la France estime qu'une industrie européenne doit se mettre en place pour conserver ou même reconquérir une autonomie stratégique. Cet effort doit notamment se concrétiser par la mise en place de soutiens financiers européens non plus uniquement pour soutenir la recherche mais selon une approche bien plus large intégrant de manière cohérente l'ensemble des dimensions : programmes capacitaires, soutien à l'innovation, soutien à l'export, etc.

Le deuxième axe est de favoriser l'émergence d'un véritable marché européen soutenant le développement de solutions européennes performantes. Si cet axe d'effort ne doit pas s'opposer à une logique de marché ouvert, il constitue néanmoins une nécessité pour garantir l'autonomie stratégique de l'Europe et de ses Etats-membres dans le domaine du numérique.

La mise en place d'un schéma de certification européen permettrait par ailleurs de faire progresser les offres de sécurité au niveau européen tout en amenant les industriels à faire preuve d'une transparence accrue sur leurs solutions.

Enfin, pour certains domaines, la mise en place de dispositifs européens de protection des entreprises jugées sensibles face à des investisseurs étrangers, voire la possibilité de réserver à des entreprises européennes certains marchés publics sensibles, sont des conditions indispensables à la réussite de cette démarche. Ces marchés pourraient être ouverts à des acteurs étrangers sous réserve qu'ils s'imposent à la fois une transparence mais aussi des engagements d'indépendance.

3.3.3. Disposer de produits performants et certifiés

La qualification constitue un mécanisme éprouvé et bien adapté à la validation des exigences de sécurité de l'État pour des produits de sécurité classiques. La France pâtit cependant d'un catalogue de produits qualifiés insuffisant, tant en termes de diversité des fournisseurs que

de couverture de certains besoins des administrations ou OIV, notamment dans des domaines émergents comme celui des sondes de détection. Par ailleurs, le mécanisme actuel de qualification, centré sur l'évaluation de sécurité, ne prend pas en compte les attentes fonctionnelles au sens large (richesse des fonctionnalités, performances, ergonomie) du client, et souffre de ce fait d'une image négative (les produits qualifiés sont souvent perçus comme inférieurs sur le plan fonctionnel). Le travail précurseur de modernisation d'ores-et-déjà engagé pour la qualification des sondes de détection pourrait servir de modèle, sur la base d'un retour d'expérience, pour la qualification d'exigences fonctionnelles.

La qualification de sondes de détection d'attaques

La loi de programmation militaire relative à la période 2014-2019 a introduit, pour les OIV, une obligation de déploiement de sondes qualifiées de détection d'attaques. A ce titre, l'ANSSI a engagé un travail de définition des exigences qui sous-tendent la qualification de tels produits. Rompant avec les approches antérieures, ces exigences portent non seulement sur la sécurité intrinsèque du produit, mais également sur son efficacité fonctionnelle et sa performance. Les deux types d'exigences, sécuritaires comme fonctionnelles, doivent être analysées par les centres d'évaluation privés réalisant jusqu'à présent les seules évaluations sécuritaires. Les premières qualifications de sondes devraient être prononcées courant 2018. Ce chantier revêt un fort degré de priorité, tant au titre de la satisfaction des besoins réglementaires des OIV qu'en tant que précurseur de ce que pourrait être une qualification intégrant des exigences fonctionnelles.

Les tests fonctionnels des produits qualifiés

Au-delà de ce travail précurseur, il apparaît souhaitable de généraliser, autant que faire se peut, l'intégration de tests fonctionnels dans la démarche de qualification des produits. Cette généralisation pourra également s'inspirer, outre des travaux visant la qualification de sondes de détection, de l'approche mise en œuvre par l'OTAN, qui, pour l'acquisition de produits de sécurité, conjugue depuis de nombreuses années évaluation de sécurité (SECEVAL) et évaluation opérationnelle (OPEVAL). Il pourrait également être pertinent d'explorer différentes pistes pour la réalisation des tests fonctionnels, le modèle retenu pour les sondes (évaluation fonctionnelle et sécuritaire conduites par le même acteur) n'étant pas nécessairement transposable à tous les cas d'usage. La validation fonctionnelle pourrait ainsi être portée par d'autres types d'acteurs privés, par des *Instituts de recherche technologique* (IRT), voire par des clubs utilisateurs. Son résultat pourrait également différer en fonction du cas d'usage : attestation de conformité lorsqu'un cahier des charges précis peut être défini, ou classement par rapport à l'état de l'art du marché dans les autres cas.

La diversification des fournisseurs de produits qualifiés

Les fournisseurs de produits actuellement qualifiés sont dans leur vaste majorité français, ce qui contribue à une image réductrice du dispositif, nuit à la diversité des catalogues, et ne permet pas la satisfaction de certains besoins. Pourtant, cette prépondérance de fournisseurs nationaux ne résulte pas d'un choix, mais plutôt d'une conjonction de facteurs : faible

attractivité du dispositif pour des fournisseurs étrangers, faible lisibilité de ses critères, ou difficulté pour un acteur étranger à remplir certains des engagements associés à la qualification (accès de l'évaluateur au code source par exemple).

Une meilleure accessibilité du dispositif à de nouveaux fournisseurs, notamment étrangers, naturellement sous réserve du respect des exigences de sécurité et de confiance, serait de nature à renforcer le taux de couverture des besoins**.** En particulier, un plus grand recours à ce dispositif par des fournisseurs européens apparaît souhaitable au titre de la consolidation de l'autonomie stratégique européenne.

La publication en 2017 d'un processus de qualification détaillé, et de l'ensemble des critères objectifs et engagements associés, a contribué significativement à l'amélioration de la lisibilité d'un dispositif longtemps jugé opaque. Par ailleurs, l'extension par le biais de la LPM 2014-2019 du champ d'application de la qualification aux OIV, et non plus aux seules administrations, a nettement renforcé l'attractivité du dispositif. La capacité pour un fournisseur étranger de remplir certains engagements demeure en revanche problématique, pour différentes raisons (limites à l'exportation depuis le pays d'origine d'informations sensibles de conception, politique générale du fournisseur sur la protection de propriété intellectuelle, etc.). Dans la mesure où ces engagements sont directement liés à des considérations de sécurité et de confiance inhérentes à l'usage visé, il ne serait pas opportun de réduire le niveau d'exigence en la matière. Cependant, des approches alternatives (accès de l'évaluateur au code source sous le contrôle du fournisseur, plutôt que fourniture du code source) ou complémentaires (engagement réciproque de l'État vis-à-vis du fournisseur) pourraient être explorées afin de faciliter la tenue des engagements, et de favoriser une diversification des fournisseurs de produits qualifiés.

Un appui accru de la commande publique sur la qualification

Le recours à des produits qualifiés résulte généralement d'une simple recommandation d'usage, plutôt que d'une obligation. L'obligation faite aux OIV de mettre en œuvre des sondes de détection qualifiées constitue à ce titre une exception notable. *A contrario*, le taux d'utilisation des produits qualifiés par les administrations demeure très faible, la commande publique représentant, selon une étude conduite par l'ANSSI en 2015, à peine 10 % des achats de produits qualifiés.

Une plus grande exemplarité des administrations dans le recours aux produits qualifiés aurait de nombreux effets bénéfiques : amélioration du niveau de sécurité des administrations par l'utilisation de solutions vérifiées, renforcement de l'attractivité de la qualification, développement économique des fournisseurs de produits qualifiés, favorisant *in fine* leur amélioration sur le plan fonctionnel, etc. Si la mise en place d'une obligation généralisée de recours à de tels produits apparaît prématurée, notamment au regard de l'insuffisante couverture de certains besoins, des actions plus ciblées pourraient être menées, soit pour faciliter l'acquisition de ces produits par les administrations (marchés cadres interministériels, licences libératoires), soit pour en rendre l'utilisation obligatoire dans

certains contextes.

La portée internationale de la qualification

La qualification est un dispositif purement national, même si des approches comparables se retrouvent dans plusieurs pays, au moins pour les besoins étatiques. Dans la mesure où il s'agit d'un outil intimement lié à la préservation de la sécurité nationale, il n'apparaît pas opportun à ce stade de chercher à lui donner un portage réglementaire de niveau européen. En revanche, la promotion bilatérale ou multilatérale de ce modèle et de ses vertus auprès des autres États-membres de l'Union européenne semble justifiée au titre du partage des bonnes pratiques concourant à la défense des systèmes d'information régaliens et, partant, à la préservation de l'autonomie stratégique européenne. Une plus grande diffusion du modèle contribuerait par ailleurs à développer son acceptabilité et à encourager les fournisseurs de solutions à s'engager dans une telle démarche.

3.3.4. La notation « cybersécurité » et les enjeux de *compliance*

Les attaques informatiques d'envergure peuvent avoir des conséquences très importantes sur la santé financière des entreprises. L'Autorité des marchés financiers a d'ailleurs, dans sa « Cartographie des risques 2017 », mis en avant le risque cyber.

Pour ne prendre qu'un exemple, le logiciel malveillant *Notpetya* a créé de nombreux dégâts sur le système d'information de *SAINT-GOBAIN* et des pertes de production que l'entreprise évalue à 250 millions d'euros sur ses ventes et à 80 millions d'euros sur son résultat d'exploitation pour l'année 2017. Les conséquences de cette attaque risquent donc d'impacter les actionnaires de l'entreprise qui pourraient vouloir connaître le risque encouru en cas de nouvelle attaque du même type.

Pour répondre à cette interrogation légitime, de nombreuses sociétés proposent des prestations de notation cyber. Les plus grandes, aujourd'hui américaines, s'appellent *BITSIGHT*, *SECURITY SCORECARD* ou bien encore *QUADMETRICS* (rachetée par la société de notation de risque financier *FICO*) et proposent de noter la cybersecurité des entreprises, de leurs sous-traitants mais aussi celle d'un pays ou d'un secteur de l'industrie. Ces notations, qui sont réalisées aujourd'hui depuis l'extérieur des systèmes d'information, permettent ainsi de noter de nombreux acteurs à leur insu. Cette première appréciation du risque cyber n'est bien entendu pas satisfaisante mais elle constitue une première étape qui va inciter les marchés financiers, les assureurs mais aussi les clients à institutionnaliser ces notations. Les acteurs majeurs du domaine deviendront donc des références de fait qu'il sera difficile de déloger. Les entreprises, et même peut-être les Etats, devront alors financer leur propre notation auprès de ces sociétés. La note sera établie avec une évaluation extérieure dans un premier temps, mais rapidement les acteurs notés seront appelés à fournir des informations sur leur système d'information, à faire procéder à des audits interne et peut-être même à déclarer leurs incidents à ces nouvelles agences de notation.

Dans ce contexte, il est essentiel que l'Union européenne développe une offre en la matière, afin que les entreprises françaises et européennes ne soient pas soumises *de facto* à des règles

non maîtrisées. Une démarche incitative pourrait ainsi être mise en place pour favoriser l'émergence d'acteurs européens de la notation cyber. La France n'est pas démunie à cet égard et possède une offre de services de cybersécurité reconnue susceptible de faire émerger des sociétés compétitives dans ce nouveau domaine. La labellisation de cette offre française par l'Etat ou par des groupements d'entreprises privées pourrait favoriser une structuration de ce domaine et permettre une amélioration de la qualité des notations.

Cette démarche pourrait être soutenue par une modification des normes de comptabilité financière pour prendre en compte le risque cyber pour les plus grandes entreprises. Ainsi que le souligne le 87e rapport annuel de la Banque des règlements internationaux : « *Les technologies fondées sur de vastes volumes de données personnelles (…) s'accompagnent de nouveaux défis dans la protection de la vie privée et la sécurité des données. Les préoccupations croissantes en matière de cybersécurité soulignent les risques potentiels que présentent des services financiers reposant sur la technologie. Afin de maintenir l'intégrité des systèmes informatiques, il pourrait être nécessaire d'appliquer des critères de vigilance à l'égard de prestataires de services internes et externes éventuellement multiples* »[59].

Cette démarche pourrait être également encouragée par un financement de la notation cyber par des acteurs européens, en complément des projets déjà financés par exemple dans le cadre de projet de R&D ou de marchés publics qui concernent des domaines sensibles.

3.3.5. La mise en place d'un cercle vertueux de sécurisation des systèmes par le biais d'un mécanisme assurantiel pertinent

Le marché de l'assurance s'est toujours structuré de manière autonome. Pourtant l'assurance cyber peine aujourd'hui à s'imposer et le marché européen est loin d'être mature. Divers facteurs structurels expliquent la difficulté de modéliser une offre et de rencontrer le marché. Au sein d'une entreprise, le risque cyber doit être vu comme un risque parmi les autres et considéré sous un angle économique, propice à son assurabilité. En revanche, pour les assureurs, l'absence de données de référence sur le risque cyber, ainsi que son caractère potentiellement systémique constituent des difficultés aujourd'hui non surmontées.

L'absence de vocabulaire commun (standards techniques reconnus sur les remontées d'incidents de sécurité et classification) porte préjudice à une véritable comparaison internationale des dispositifs nationaux et des données recueillies dans chaque pays en matière de menace. De manière générale, des problèmes méthodologiques empêchent de déterminer des probabilités d'occurrence d'incidents de risque numérique, réduisant ainsi la capacité des responsables politiques à assigner effectivement les fonds publics, des assureurs à évaluer leur couverture ou des gestionnaires de risques à réduire ou transférer les risques identifiés.

Le recueil des informations quantitatives sur le risque cyber constitue une deuxième

[59] 87e rapport annuel de la Banque des règlements internationaux, p. 104 (https://www.bis.org/publ/arpdf/ar2017_fr.pdf).

difficulté majeure. Les informations relatives aux incidents sont peu ou pas partagées[60], il n'y a pas de lieu de centralisation d'une telle information et aucune réflexion n'a encore été menée quant à sa structuration. Par ailleurs, cette absence de statistiques empêche de modéliser l'offre (bien qu'en France, la plateforme gouvernementale cybermalveillance.gouv.fr commence à le faire et qu'à l'international d'autres initiatives aient été lancées). La constitution d'une base de données européenne répertoriant la majorité des incidents cyber serait à ce titre une avancée. Les données pourraient être agrégées afin d'analyser les tendances en matière de menaces, d'identifier des besoins en termes de sécurité pour les produits et services présents sur le marché, et de fournir des informations chiffrées sur les coûts. La mise en place actuelle de mécanismes d'obligation pour la notification d'incidents au sein de l'Union européenne (à travers notamment le GDPR, la directive NIS et le paquet télécom) pourra utilement contribuer à l'établissement d'un état des lieux du risque numérique.

Une dernière difficulté tient à la question de la valorisation des biens intangibles qui constituent 85 % de la valeur des entreprises aujourd'hui. Un actif informationnel tel qu'entendu dans une économie numérique est un incorporel qui n'est pas qualifié sur le plan juridique, ni quantifié sur le plan comptable. Il n'est donc pas un actif assurable. L'assurabilité de l'actif intangible représente un enjeu essentiel pour la valorisation de l'entreprise dans une économie numérique.

La mise en place d'une politique de management des risques cyber, intégrée au management des risques de l'entreprise, constitue un autre enjeu clé. Les sociétés cotées ont obligation depuis 2011 d'adopter des pratiques de management des risques, s'appuyant sur des outils de cartographie, un comité de gouvernance et des audits. Ces bonnes pratiques doivent être développées dans toutes les entreprises, tout en tenant compte de leur niveau de maturité et de leur taille, car elles permettent de sensibiliser les instances dirigeantes et constituent un pré-requis à la souscription raisonnée d'une offre d'assurance cyber.

3.4. Les enjeux humains

Le niveau de cybersécurité de notre société est directement lié aux comportements de l'ensemble des Français - particuliers, entreprises et administrations - et par conséquent à leur degré de compréhension et de maîtrise des enjeux de cybersécurité. Les services de l'État, les entreprises et les individus sont en effet de plus en plus connectés par des technologies offrant de nouveaux modes de travail, d'interaction et de transaction. Sous la pression de la mobilité, de l'utilisation massive des données ou encore de l'Internet des objets, le numérique se diffuse toujours plus rapidement et profondément. Si la diffusion de la culture de la sécurité numérique ne suit pas, alors les conditions d'une utilisation sereine et confiante de l'Internet comme des objets connectés ne pourront être réunies. C'est une

[60] Selon des estimations de l'OCDE, entre 60 et 89% des incidents ne seraient pas reportés.

approche pédagogique, positive et ancrée dans la réalité des différents publics de la culture de la sécurité numérique que la présente revue propose, afin d'en renforcer l'impact et d'éveiller au maximum l'intérêt de chacun aux enjeux du numérique. Il faut donner des clés aux entreprises, aux administrations et aux citoyens afin qu'ils deviennent acteurs de la sécurité du numérique, dans leurs vies personnelle et professionnelle.

C'est pourquoi, la cybersécurité doit être intégrée, de l'école élémentaire au lycée, au parcours de formation des élèves. Des approches ludiques doivent, parallèlement, en être proposées tout au long de la vie, adaptées aux différents degrés de familiarité qu'ont les Français avec les systèmes d'information et de communication et à leur usage des objets connectés du quotidien. Une plus forte diffusion de la culture de la sécurité numérique dans les entreprises et dans les administrations publiques apparait aussi souhaitable, tandis que des réponses doivent être apportées aux besoins de recrutement de spécialistes de la cybersécurité chez ces dernières. Notre pays ne peut en outre se contenter de former des spécialistes de la cybersécurité et de la cyberdéfense, il doit également se donner les moyens de les conserver et d'attirer les talents étrangers.

3.4.1. Eduquer dès le plus jeune âge aux enjeux de la cybersécurité

L'éducation dès le plus jeune âge à la cybersécurité doit constituer une priorité. Les enfants et les adolescents ont une pratique quotidienne, et précoce par rapport aux générations qui les ont précédés, des objets connectés, d'Internet et des réseaux sociaux. Selon une étude *IPSOS* « Junior Connect » datant de 2015, l'âge moyen du premier téléphone portable est de 9 ans et celui du premier *smartphone* de 12 ans. Les jeunes de 13 à 19 ans se connectent en moyenne 13h30 par semaine et 78 % d'entre eux sont inscrits sur les réseaux sociaux[61]. Or, nombre de ces jeunes ne maîtrisent pas les dangers liés à la communication d'informations personnelles, à la connexion avec des inconnus ou à la publication de photos privées[62].

Il appartient à l'école de la République d'éduquer les élèves à la cybersécurité. Cela doit passer par une première sensibilisation au numérique dès les années de maternelle et par une éducation au numérique incluant la maîtrise des exigences en matière de cybersécurité à l'école élémentaire, au collège et dans tous les cursus du lycée. L'éducation au numérique dès le plus jeune âge est structurante pour les comportements futurs. L'ouverture précoce aux grands concepts de la science des techniques informatiques donnera des clés aux élèves pour comprendre le monde qui les entoure et leur permettra plus tard de devenir acteurs de ce monde et non de simples consommateurs du numérique. Il s'agit d'apprendre aux élèves à utiliser le numérique dans tous les domaines de la vie, de leur permettre d'acquérir une culture numérique, de l'initiation au code à la compréhension de la logique des *computers*

[61] Au regard des tendances observées sur les dernières années, on peut estimer que ces chiffres sont, si ce n'est en augmentation, du moins stables depuis 2015.

[62] Selon la même étude *IPSOS* « Junior Connect », 57 % des 11-12 ans ont un profil *FACEBOOK* malgré l'interdiction de s'y connecter avant l'âge de 13 ans, 43 % ont déjà ajouté des inconnus à leur liste d'amis et 12 % envoyé des photos ou des vidéos à des inconnus.

sciences, en passant par l'acquisition de compétences en traitement de données et l'aptitude à adopter des comportements respectueux des règles de sécurité.

À l'école élémentaire, il est important de montrer les liens qui unissent les concepts de l'informatique et ceux qui sont enseignés dans les autres disciplines, puis ceux qui les unissent aux objets familiers du quotidien[63].

Au collège, l'enseignement des mathématiques et de la technologie, qui intègre l'apprentissage des algorithmes et de la programmation informatique, doit constituer le principal vecteur de transmission des règles de la cybersécurité.

Bien évidemment, l'apprentissage des règles de la cybersécurité ne doit pas s'arrêter aux portes des lycées, au risque de voir les futurs jeunes adultes rapidement dépassés par des enjeux qui ne manqueront pas de se renouveler extrêmement rapidement. C'est pourquoi il apparaît essentiel que des formations de sensibilisation aux enjeux de la cybersécurité soient intégrées dans les parcours des lycéens généraux, technologiques et professionnels, de la classe de seconde à la classe de terminale.

Les parcours de formation initiale et continue des enseignants, notamment de mathématiques et de technologie, devront intégrer cette exigence nouvelle d'une transmission aux élèves des règles de la cybersécurité. Des MOOC[64] dédiés aux enseignants en formation initiale et en formation continue pourraient être conçus par le ministère de l'éducation nationale avec le soutien de l'ANSSI. De nouvelles ressources pédagogiques dédiées à la sensibilisation des élèves aux règles de la sécurité informatique devront être régulièrement mises à disposition des enseignants[65].

L'efficacité de la sensibilisation des plus jeunes aux enjeux de la cybersécurité pourra être renforcée par des actions ludiques. Certains programmes ont d'ores-et-déjà démontré leur efficacité dans le domaine de la diffusion de la culture numérique. Le *Permis Internet* proposé aux enfants, programme national de prévention développé par la Gendarmerie nationale, la Police nationale, la Préfecture de Police et l'association *AXA Prévention*, permet ainsi de sensibiliser des enfants de CM2 et leurs parents à un usage d'Internet vigilant, sûr et responsable[66]. Le dispositif *Ecole Internet*, développé par l'association *Ville Internet* et qui promeut les usages d'Internet pour les élèves des écoles maternelles et élémentaires francophones en labellisant les écoles participantes, en valorisant leurs actions et en incitant

---

[63] L'apprentissage des règles d'utilisation d'Internet doit notamment constituer une priorité. Les élèves doivent connaître les principes de responsabilité civique et légale de l'internaute, les règles du téléchargement, apprendre à s'informer sur Internet mais aussi à maîtriser les réseaux sociaux et à protéger leur vie privée sur la toile.

[64] MOOC (*Massive Open On Line Course*) : formation en ligne ouverte à tous.

[65] Le portail du ministère de l'éducation nationale *Eduscol* propose déjà de premières ressources pédagogiques pour sensibiliser à l'informatique les élèves de primaire et de secondaire. La direction du numérique pour l'éducation de ce ministère gère par ailleurs une banque nationale de mutualisation de ressources appelée *Edu'base*.

[66] https://www.permisinternet.fr/.

à des échanges d'expériences, constitue également une initiative intéressante. En s'inspirant de ce dispositif, on pourrait par exemple imaginer des démarches de mise en valeur, voire de labellisation, des établissements d'enseignement les plus engagés en faveur de la cybersécurité.

La présente revue recommande la mise en place rapide d'un groupe de travail, sous le pilotage du ministère de l'éducation nationale, chargé de définir les actions à mener, et le cas échéant, les modifications à apporter aux programmes pour que tous les élèves sortent du système éducatif avec un niveau élevé de maîtrise des enjeux de la cybersécurité.

3.4.2. Sensibiliser le grand public par des actions pédagogiques

Si la sensibilisation du public scolaire aux enjeux de la cybersécurité est indispensable, une sensibilisation du grand public doit parallèlement être conduite.

Les initiatives d'ores-et-déjà existantes dans la diffusion de la culture du numérique constituent de premières bases sur lesquelles s'appuyer. On pense notamment au programme de service civique « les D-CoDeUrs », lancé en 2016, qui implique des volontaires engagés pour l'inclusion numérique, en ciblant prioritairement trois publics : les populations peu connectées (à qui sont proposées des ateliers dans des lieux de médiation numérique de proximité), les publics scolaires et périscolaires et des seniors (à travers des actions mises en place au sein de maisons de retraite ou de clubs du troisième âge). On pense également au collectif *EDUCNUM*, initié par la CNIL en mai 2013 et constitué de soixante structures[67], pour porter et soutenir des actions visant à promouvoir une véritable « culture citoyenne du numérique », notamment à travers l'initiation et la promotion d'actions de sensibilisation et de formations de tous les publics, notamment les plus jeunes, à un usage responsable et éclairé des technologies numériques. La plateforme cybermalveillance.gouv.fr assume quant à elle un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de la population française.

Mais il paraît essentiel d'aller plus loin en amplifiant les actions en cours, en communiquant de façon plus efficace et plus stratégique, et en développant des actions de sensibilisation spécifiquement dédiées aux enjeux de la cybersécurité.

La présente revue recommande ainsi que soit créée une application ludique, disponible sur *smartphone*, permettant aux Français de tester leur niveau de connaissances dans le domaine de la sécurité numérique et leur proposant, quel que soit leur niveau initial de maîtrise, de nombreux défis. La réalisation de cette application pourrait être prise en charge par l'ANSSI (qui propose déjà, avec le MOOC *SecNumacadémie*, un programme en ligne de sensibilisation à la sécurité du numérique qui s'adresse à tous[68]). L'agence pourrait notamment s'inspirer, pour concevoir cette application pédagogique sur la sécurité numérique, du projet de

[67] Entreprises, organismes, associations issues du monde de l'éducation, de la recherche, de l'économie numérique, de la société civile, de fondations d'entreprises et d'autres institutions.

[68] https://www.ssi.gouv.fr/particulier/formations/secnumacademie/.

plateforme en ligne d'évaluation et de certification des compétences numériques *PIX*, actuellement développé par les ministères de l'éducation nationale et de l'enseignement supérieur[69].

Une piste de recherche originale et innovante serait, par ailleurs, d'étudier l'apport des *nudges* pour le développement de l'autonomie des citoyens en matière de cybersécurité. Ces approches incitatives, fondées sur les sciences du comportement, ont connu une reconnaissance retentissante avec l'attribution du Prix Nobel d'économie 2017 à Richard THALER, l'un des pères de la « *nudge economy* ». Les *nudges* sont mis en œuvre dans l'accompagnement des politiques publiques aux Etats-Unis et au Royaume-Uni. En France, un chef de projet *nudge* a été recruté au SGMAP et pourrait être sollicité par l'ANSSI pour réfléchir à la mise en place de *nudges* pour inciter à un comportement plus responsable des utilisateurs face aux menaces cyber.

3.4.3. Diffuser la culture de la sécurité numérique au sein des entreprises et des administrations publiques

La diffusion de la culture de la sécurité numérique doit également être renforcée au sein des entreprises et des administrations publiques.

L'ANSSI publie à cette fin des guides comme le « Guide des bonnes pratiques de l'informatique », qui présente douze recommandations issues de l'analyse d'attaques réussies à l'adresse des TPE et des PME[70], ou le guide sur « La cybersécurité des systèmes industriels », qui propose, en l'illustrant par des situations réelles, aux acteurs concernés une méthodologie simple et adaptée pour sécuriser leurs systèmes industriels. L'agence publie également un référentiel d'exigences applicables aux prestataires de services d'informatique en nuage (*SecNumCloud*), élaboré en concertation avec les acteurs du marché. Parallèlement, les initiatives visant à promouvoir la cybersécurité au sein des entreprises sont nombreuses, de l'organisation en octobre 2017 par l'ENISA (agence européenne chargée de la sécurité des réseaux et de l'information) du « Mois européen de la cybersécurité »[71] aux actions conduites par le CIGREF[72] et le *Cercle européen de la sécurité et des systèmes d'information*, en passant par le *Forum International de la Cybersécurité* (FIC)[73] ou l'*European cyberWeek*[74]. Ces

---

[69] https://pix.beta.gouv.fr.

La plateforme *PIX* est un référentiel de compétences numériques en ligne pour une certification numérique tout au long de la vie. Son objectif est d'accompagner l'élévation du niveau général de connaissances et de compétences numériques.

[70] http://www.ssi.gouv.fr/publication/lanssi-et-la-cgpme-publient-le-guide-des-bonnes-pratiques-de-informatique/.

[71] https://www.ssi.gouv.fr/agence/cybersecurite/mois-de-la-cybersecurite-2017.

[72] Association dont la mission est de développer la capacité des grandes entreprises à intégrer et maîtriser le numérique.

[73] https://www.forum-fic.com. Le FIC est l'un des événements de référence en matière de cybersécurité et de confiance numérique, réunissant l'ensemble des acteurs en France et en Europe.

initiatives, à l'efficacité réelle, doivent être encore amplifiées, leur coordination renforcée et leur diffusion élargie au plus grand nombre d' acteurs économiques. Enfin, le ministère chargé de l'industrie va contribuer à cet effort, notamment en intégrant une dimension cybersécurité à son programme de soutien à la transformation numérique des entreprises.

Au sein des administrations publiques, centrales, territoriales et déconcentrées, la culture de la sécurité numérique doit être diffusée auprès de tous les agents, quel que soit leur niveau de responsabilité ou leur secteur de spécialisation. La maîtrise de la culture de la sécurité numérique doit être érigée en priorité des programmes de formation initiale et de formation continue. Le développement de modules de formation initiale et continue dans les écoles de la fonction publique nationale et territoriale et le développement des formations cyber à l'Institut des hautes études de défense nationale (IHEDN) et à l'Institut nationale des hautes études de sécurité et de justice (INHESJ) apparaissent ainsi indispensables. L'encadrement doit se saisir des problématiques de sécurité numérique, qui ne peuvent relever de la seule responsabilité des personnels et des directions chargés de la sécurité informatique. L'intégration de celle-ci dans la définition des missions des cadres de la fonction publique devrait être envisagée.

3.4.4. Développer l'offre de formation professionnelle aux enjeux de la cybersécurité

Le niveau d'ambition de la France dans les domaines de la cyberdéfense et de la cybersécurité est aujourd'hui contraint par ses capacités en matière de ressources humaines, notamment s'agissant des ingénieurs spécialisés en informatique et en télécommunications (réseaux informatiques, sécurité, informatique, crypto-analyse, etc.). La construction d'une culture nationale du numérique solide passe par la formation des experts de demain.

Des démarches associatives et syndicales existent pour promouvoir les métiers du numérique et faire tomber les réflexes d'autocensure de certains publics au regard de ces métiers. Le *Syntec Numérique* (syndicat professionnel des entreprises de services du numérique, des éditeurs de logiciels et des sociétés de conseil en technologies) s'est ainsi engagé dans de nombreuses actions pour renforcer l'attractivité des formations dans le numérique, comme le programme *JEM'NUM* (« Journée des entreprises et des métiers du numérique ») ou l'association *Pascaline* pour inciter les jeunes à aller vers les écoles d'ingénieurs (*cf.* encadré ci-après). Des associations comme *Femmes du Numérique* ou *Informatique au féminin* sensibilisent, quant à elles, les jeunes afin de combattre les préjugés sur les femmes qui exercent dans l'informatique.

[74]https://european-cyber-week.eu/fr/accueil/.

Les initiatives du Syntec Numérique en faveur de l'attractivité des formations dans le numérique

Les *Journées des entreprises et des métiers du numérique* (JEM'NUM) organisées par le *Syntec Numérique* sont des journées d'échanges entre les étudiants, les universités et les entreprises du numérique. Ces forums constituent l'occasion pour les étudiants de connaître les formations proposées par les universités dans le domaine du numérique et de rencontrer les entreprises de la filière numérique. Ils permettent également aux universités de présenter aux entreprises du numérique leurs cursus de formation, leurs réponses aux besoins en compétences du secteur et de construire des partenariats. Ils sont enfin pour les entreprises de la filière numérique une vitrine pour présenter l'attractivité de la filière et les opportunités qu'elle ouvre.

Créée en 2006, l'association *Pascaline* (http://www.assopascaline.fr) est un espace d'échanges et de réflexions entre les entreprises et les établissements d'enseignement supérieur du numérique dont l'objectif est le développement de l'attractivité des formations et des métiers du numérique auprès des jeunes générations. L'association réunit quatre-vingt-cinq établissements d'enseignement supérieur et 2 700 entreprises du secteur regroupées autour du *Syntec Numérique* et du syndicat d'entrepreneurs dans l'industrie du numérique *CINOV-IT*.

Lancé par l'ANSSI en 2013, à la suite de la publication du Livre blanc sur la défense et la sécurité nationale, le projet *CyberEdu* promeut quant à lui l'intégration de la sécurité numérique dans les formations supérieures en informatique non spécialisées en sécurité des systèmes d'information par la fourniture de contenus pédagogiques remis aux enseignants. Afin de prolonger les actions engagées par l'ANSSI pour initier cette démarche, une association réunissant des enseignants en informatique, spécialistes et non spécialistes en sécurité, a été créée pour la porter dans toute la France, notamment au travers de colloques. Elle labellise aussi des formations supérieures françaises en informatique qui ne relève pas du domaine de la sécurité du numérique. Bien que la démarche *CyberEdu* soit initialement destinée aux formations du numérique, l'association envisage dans le futur de s'adresser à d'autres types de formations, pour sensibiliser tous les acteurs ou utilisateurs de la chaîne des systèmes d'information.

Seconde initiative notable portée par l'ANSSI, *SecNumedu* est un label de formations initiales en cybersécurité de l'enseignement supérieur. L'objectif de cette labellisation est d'apporter l'assurance aux étudiants et aux employeurs qu'une formation dans le domaine de la sécurité du numérique répond à une charte ainsi qu'aux critères définis par l'ANSSI en collaboration avec les acteurs et les professionnels du domaine (établissements d'enseignement supérieur, industriels…). Le label joue également en faveur du renforcement et du développement des enseignements relatifs à la sécurité du numérique. Il s'appuie sur un référentiel de labellisation, dont l'élaboration a été pilotée par l'ANSSI avec la contribution d'industriels, d'écoles, du *Pôle d'excellence Cyber* et du ministère de l'éducation nationale, de l'enseignement

supérieur, de la recherche et de l'innovation. Il est attribué pour une durée de trois ans renouvelable et permet à la formation qui en bénéficie, de figurer au catalogue *SecNumedu* de l'ANSSI. Une quarantaine de formations ont été labellisées *SecNumedu*.

L'ANSSI a, enfin, conduit une démarche d'identification des métiers de la cybersécurité et un titre d'expert en sécurité des systèmes d'information (certification de niveau I - bac +5) a été enregistrée au *Répertoire national des certifications professionnelles* (RNCP).

3.4.5. Perfectionner la gestion des compétences dans les services chargés de la cyberdéfense de l'Etat : conserver nos talents et en attirer

Par ailleurs, l'ANSSI mène plusieurs actions pour la formation et la sensibilisation à la cybersécurité dans le cadre de son Centre de formation à la sécurité des systèmes d'information (CFSSI)[75]. Le Centre de formation propose des formations courtes sur des thématiques telles que la cryptographie, l'analyse de risque ou l'audit de sécurité, et accueille près de 2000 personnes, principalement issues de l'administration, chaque année. Il dispense également une formation longue sur treize mois, débouchant sur la délivrance d'un titre « expert en sécurité des systèmes d'information » équivalent à un bac+5.

Pour compléter ce dispositif de formation interne, l'ANSSI pourrait aussi labelliser des formations continues en cybersécurité à destination des agents du secteur public et permettre ainsi une démultiplication de sa capacité de formation. Cette stratégie devrait permettre d'instaurer une formation minimale en cyberdéfense pour l'ensemble des cadres de direction et en particulier ceux dont les services ou directions doivent défendre les intérêts des entreprises de cyberdéfense.

Les grands employeurs de la cyberdéfense que sont l'ANSSI et le ministère des armées n'ont aujourd'hui pas de difficultés particulières pour recruter les talents dont ils ont besoin. Ils sont cependant confrontés à un turnover important de leurs équipes qui nécessite de consacrer un effort conséquent au recrutement et à l'intégration de ces nouveaux experts. Cette mobilité présente cependant de nombreux avantage car elle permet à ces experts de diffuser le savoir et la bonne parole de l'ANSSI ou du ministère des armées au sein des entreprises qui les accueillent. Il convient toutefois de veiller à ce que ces compétences ne se fassent pas happer par les grands acteurs américains ou chinois du numérique au détriment des entreprises française ou européennes.

A l'inverse, les autres employeurs non spécialisés en cyber, qu'ils soient publics ou privés, peinent à recruter des personnels compétents en cyberdéfense et surtout à les conserver. En effet, dans des structures non spécialisés en cyber, le spécialiste peut rapidement se retrouver isolé et bloqué dans sa progression à la fois par ce qu'il aura peux de débouchés en interne mais surtout parce que sa hiérarchie voudra le conserver à ce poste. Cette absence de perspective est une des causes principales de la difficulté à recruter et conserver des

[75] https://www.ssi.gouv.fr/particulier/formations/.

spécialistes de qualité.

Trois pistes peuvent permettre de résoudre cette difficulté.

La première serait de regrouper les compétences cyber au sein d'une même structure qui travaille au profit de plusieurs entités. Ainsi, les régions pourraient mettre en place, en liaison avec l'ANSSI, des pôles de compétence cyber à même de soutenir par exemple l'ensemble des collectivités territoriales. Les spécialistes seraient alors regroupés et pourrait conduire une approche cohérente sur l'ensemble d'une région, que ce soit pour la fourniture d'avis technique, la rédaction de spécification ou la mise en place de marché cadre d'acquisition de solution de cybersécurité.

La seconde solution consisterait à gérer des parcours de carrière interministériels. Ce type de parcours est déjà mis en place pour les grands corps de l'état mais les contractuels qui constituent la majorité des personnels recrutés en cyber ne sont pas concernés et ont les plus grandes difficultés à changer d'administration sans avoir à démissionner. L'ANSSI pourrait ainsi être chargée de piloter ces parcours de carrière et permettre de véritables progressions interministérielles pour ces agents.

Enfin, la dernière solution consisterait à valoriser au sein des parcours professionnels des différentes administrations, le passage par un poste dans le domaine de la cyberdéfense. On peut ainsi imaginer par exemple que les postes de directeur informatique ou de directeur du numérique ne soient accessibles qu'à des personnels pouvant justifier d'une expérience cyber antérieure.

Conclusion

La revue stratégique cyberdéfense a permis, pour la première fois de façon aussi approfondie, de dresser un panorama complet de la cybermenace. Il en ressort que cette menace continue à croitre de manière extrêmement rapide. Un certain nombre de facteurs systémiques y contribuent, dont la numérisation croissante de la société, une prise de conscience toujours insuffisante des enjeux de cybersécurité, la grande accessibilité et la prolifération des outils malveillants ainsi que la professionnalisation des groupes d'attaquants. Les conséquences d'une cyberattaque de grande ampleur pourraient désormais être critiques pour la Nation.

Face à des risques multiples pouvant avoir des conséquences les plus graves et des effets dévastateurs et/ou systémiques l'Etat doit consolider son organisation, autour de quatre chaines opérationnelles dédiées à la protection, aux actions militaires, au renseignement et à l'investigation judiciaire. La nécessaire coordination de ces chaines et la définition d'une stratégie à long terme implique également la création ou la revitalisation d'instances de pilotage, de direction, de gestion de crise et de coordination technique.

La protection des réseaux sensibles de l'Etat et des infrastructures critiques doit demeurer une priorité. La coopération entre l'Etat et les acteurs privés, au premier rang desquels les opérateurs de communications électroniques, est à ce titre essentielle et doit être renforcée. Il est également nécessaire de développer les capacités des forces de sécurité et du système judiciaire pour qu'ils soient en mesure de répondre à l'explosion du nombre de délits cybercriminels, en dotant les services enquêteurs et judiciaires de compétences spécialisées. L'Etat doit enfin apporter un soutien aux collectivités territoriales dans le renforcement de leur cybersécurité, notamment en encourageant le développement de pôles de compétences mutualisés.

La France doit affermir sa doctrine dans le cyberespace et entretenir des relations diplomatiques spécifiques dans ce domaine. Suivant les partenaires, ces dialogues peuvent être soit coopératifs (par exemple pour permettre une entraide en cas d'attaque d'ampleur régionale ou mondiale) soit assertifs afin de contenir le niveau de la menace.

Il est par ailleurs indispensable de sensibiliser l'ensemble des acteurs (grand public, entreprises de toute taille, administrations) à cette menace. Cette sensibilisation doit se traduire par la prise en compte de la cyberdéfense dans l'éducation, du plus jeune âge jusqu'aux études supérieures. Elle pourrait également se traduire économiquement avec la modification des normes comptables afin de prendre en compte ce risque, ou le développement des assurances couvrant le risque cyber.

Les enjeux économiques liés à l'ensemble de ces mesures doivent encore être affermis et mieux cartographiés. Dans tous les cas, il est nécessaire que la France encourage et accompagne le développement industriel dans le domaine de la cyberdéfense, en entretenant une offre industrielle nationale, facilitant l'incubation de *start up* et contribuant à l'émergence européenne de leaders mondiaux. Si les enjeux sont majoritairement à cette échelle

européenne, comme par exemple l'émergence d'un *cloud* de confiance, ceux liés à la souveraineté (numérique) ne doivent pas pour autant être oubliés.

Enfin, il est essentiel de développer les capacités des forces de sécurité et du système judiciaire pour qu'ils soient en mesure de répondre à l'explosion du nombre de délits liés à cette cybermenace grandissante en dotant les services enquêteurs et judiciaires de compétences spécialisées. Les initiatives comme ACYMA doivent être encouragées.

Recommandations prioritaires

Recommandations		Calendrier de mise en œuvre	Développement dans la revue
Consolidation de l'organisation de cyberdéfense française	• Mettre en place 4 chaînes opérationnelles : chaîne « protection », chaîne « action militaire », chaîne « renseignement », chaîne « investigation judiciaire ». • Mettre en place un comité directeur cyber chargé de suivre la mise en œuvre des décisions prises en matière de développement et d'organisation générale du domaine par le Conseil de Défense et de Sécurité Nationale (CDSN). • Mettre en place un comité de pilotage de la cyberdéfense qui s'attache à améliorer la connaissance de la menace d'origine cyber, à élaborer une politique industrielle, réglementaire et normative de souveraineté numérique et à mettre en place une doctrine officielle de réponse globale à une crise cyber. • Mettre en place un centre de coordination des crises cyber (C4) chargé de la gestion des crises non majeures.	Immédiat et court terme	2.2. Consolider l'organisation de la cyberdéfense
Renforcement de la sécurisation des systèmes d'information de l'Etat	• Soumission pour avis à l'ANSSI des projets informatiques les plus importants et les plus sensibles de l'Etat dès leur phase de lancement. • Raccordement progressif de tous les ministères à la plateforme d'accès à Internet du réseau interministériel de l'Etat (RIE) et pleine utilisation des services qu'elle offre.	Immédiat et court terme, étude d'impact juridique transmise, économique en cours de finalisation	2.3.1. La protection des systèmes d'information de l'Etat

Recommandations		Calendrier de mise en œuvre	Développement dans la revue
	• Imposer la couverture complète par un dispositif de supervision de la sécurité des services informatiques utilisés par l'Etat, y compris dans les cas où ces services sont externalisés, et permettre à l'ANSSI d'imposer à cette fin la mise en place de ses systèmes de détection ou de systèmes de détection équivalents.		
Renforcement de la protection des opérateurs d'importance vitale (OIV)	• Renforcement du niveau d'exigence des règles de sécurité qui s'appliquent aux OIV des secteurs des communications électroniques et de l'approvisionnement en énergie électrique. •	Court terme avec étude d'impact financière et juridique	2.3.2. La protection des OIV
Renforcement de la protection des activités essentielles	• Un socle commun de règles élémentaires de sécurité proportionnée permettant de protéger les acteurs fournissant des services essentiels. • Recherche d'une harmonisation au sein de l'Union européenne des règles de cybersécurité s'appliquant aux opérateurs de services essentiels.	Court et moyen terme	2.3.3. La protection des activités essentielles
Implication accrue des opérateurs de communications électroniques et des hébergeurs	• Permettre à l'ANSSI de s'appuyer sur des systèmes de détection mis en œuvre par les opérateurs de communications électroniques pour détecter les attaques informatiques Permettre à l'ANSSI, lorsqu'elle a connaissance d'une menace particulièrement sérieuse, de mettre en place sur le réseau d'un opérateur de communications électroniques ou le système d'information d'un hébergeur, un dispositif de détection local et temporaire	Court terme avec étude d'impact financière et juridique	2.3. Améliorer la protection des activités sensibles

Recommandations		Calendrier de mise en œuvre	Développement dans la revue
Amélioration de la cyberprotection des collectivités territoriales	• Soutien à la création, par les collectivités territoriales elles-mêmes, d'un réseau de correspondants en cybersécurité. • Amélioration de l'intégration des besoins et des contraintes spécifiques aux collectivités territoriales dans les référentiels de l'ANSSI et dans ses catalogues de produits et services qualifiés.	Moyen terme	2.3.4. La protection des collectivités territoriales
Renforcement de la lutte contre la cybercriminalité	• Conduite d'une réflexion sur la pertinence d'enquêter de manière plus systématique sur les actes de cybercriminalité, y compris en l'absence de plainte, lorsque les informations recueillies laissent entrevoir l'existence probable d'infractions pénales. • Action d'entrave contre les plateformes criminelles les plus populaires afin de diminuer le sentiment d'impunité qui anime un certain nombre de cybercriminels. • Développement d'un réseau de collaboration actif entre magistrats et enquêteurs en Europe et à l'international.	Moyen terme	2.4. Renforcer la lutte contre la cybercriminalité
Promotion de normes de comportement responsables dans le cyberespace	• Renforcement des mécanismes de contrôle des exportations dans le domaine cyber pour les éléments les plus dangereux • Création, au niveau français ou européen, d'un *think tank* de portée international dédié aux questions géostratégiques et juridiques de cyberdéfense au sein duquel les idées de la France pourraient trouver un relais.	Moyen terme	2.5. L'action internationale de la France dans le domaine cyber 3.1.5. Réguler la production et l'exportation des armements et des activités offensives cyber

Recommandations		Calendrier de mise en œuvre	Développement dans la revue
Encadrement de l'activité des acteurs privés dans le cyberespace	• Lancement d'une initiative française dans le cadre du G20 en vue de réguler les activités du secteur privé ayant un impact sur la sécurité internationale du cyberespace. • Promouvoir l'interdiction du *Hackback* par des acteurs du secteur privé dans le cyberespace. • Poser au niveau international un principe de responsabilité de sécurité des acteurs privés systémiques dans la conception et la maintenance de leurs produits et services numériques.	Court terme	2.5. L'action internationale de la France dans le domaine cyber
Définition d'une doctrine d'action face à une attaque cyber	• Adoption d'un schéma de classement des attaques informatiques. • Définition des options de réponse aux incidents cyber.	Immédiat	2.5.3. Définir une doctrine d'action
Structuration d'une politique industrielle en matière numérique reposant sur la maîtrise de technologies clés	• Mise en place d'une équipe interministérielle chargée d'analyser les technologies clés et de faire émerger des solutions de confiance en lien avec les industriels (veille technologique et proposition de choix dédiés à l'émergence des technologies clés • Maintien d'une industrie nationale à la pointe dans le domaine du chiffrement des communications. • Développement d'une nouvelle génération de radios professionnelles mobiles au profit des forces de sécurité et des unités de secours. • Soutien à la recherche et développement dans le domaine de l'intelligence artificielle appliquée à la cyberdéfense.	Court terme	3.1. La souveraineté numérique, composante essentielle de la souveraineté nationale

Recommandations		Calendrier de mise en œuvre	Développement dans la revue
Communications sécurisées	• Identifier un compostant critique maitrisé par la France et intégré dans des équipements terminaux pour pouvoir faire de la téléphonie mobile sécurisée. • Développer des techniques de chiffrement et de cloisonnement logiciels. • Etudier de nouveaux services, apparentés à la radio professionnelle, basés sur les technologies civiles (5G) pour apporter de la résilience.	Court et moyen terme	3.1.2 trois technologies essentielles à notre souveraineté numérique
Cloud	• Etablir une politique globale de l'Etat de recours au cloud. • Encourager le développement de solutions de chiffrement pour le cloud. • Soutenir une autonomie stratégique dans ce domaine. • Etablir un cadre de confiance global afin d'orienter le marché vers des produits qualifiés SecNimCloud.	Court et moyen terme	3.1.4 Pour l'informatique en nuage, inventer une stratégie de valorisation
Amélioration du cadre actuel de certification afin de contribuer à l'amélioration de la sécurité des produits	• Mise en place d'une certification élémentaire de cybersécurité, sur le modèle du marquage « CE » requis pour la commercialisation de certains biens ou services au sein de l'espace européen.	Moyen terme	3.2.2. Améliorer le cadre de certification pour améliorer la sécurité des produits

Recommandations		Calendrier de mise en œuvre	Développement dans la revue
Consolidation de notre base industrielle nationale de confiance dans le domaine de la cyberdéfense	• Réaliser et entretenir une cartographie industrielle • Soutien à l'émergence d'au moins un acteur industriel national de référence dans le domaine de la *Threat intelligence* (analyse de la menace) et de l'élaboration de marqueurs apte à concurrencer les grandes entreprises américaines, russes et israéliennes du domaine.	Court et moyen terme	3.3. L'économie de la cybersécurité
	• Inciter les grands industriels français à compléter leur offre de produits et de service à destination du domaine civil, afin qu'ils y deviennent des champions internationaux de la cybersécurité capables de concurrencer les géants de la cybersécurité américains, russes, chinois ou israéliens. • Soutien aux stratégies de croissance externe des PME dédiées à la cyberdéfense les plus performantes par la mobilisation des fonds d'investissement intéressés par le domaine de la cyberdéfense pour favoriser la création d'entreprises de taille intermédiaire (ETI) françaises dans ce secteur. • Soutien à la mise en place d'accélérateurs, de start-ups studios et plus généralement de structures d'accompagnement des start-ups dédiés à la cyberdéfense, en concentrant les efforts sur les entreprises innovantes dont la stratégie peut leur permettre d'atteindre une empreinte mondiale.		

Recommandations		Calendrier de mise en œuvre	Développement dans la revue
Appui à la prise en compte par le secteur privé des enjeux cyber	• Soutien à l'apparition d'acteurs nationaux ou européens de notation cyber. • Etudier le soutien au développement d'un mécanisme d'assurance cyber pertinent en aidant à mieux estimer les risques. • Soutien à la mise en place d'une valorisation du risque CYBER au sein des normes comptables et à la prise en compte dans les documents comptables et financiers.	Moyen terme	3.3. L'économie de la cybersécurité
Intégration des règles de la cybersécurité dans les apprentissages transmis par l'Ecole de l'école élémentaire à la classe de terminale	• Une éducation au numérique incluant la maîtrise des exigences en matière de cybersécurité à l'école élémentaire, au collège et dans tous les cursus du lycée. • Des MOOCS sur la transmission des règles de cybersécurité dédiés aux enseignants en formation initiale et en formation continue conçus par le ministère de l'Education nationale avec le fort soutien de l'ANSSI.	Moyen terme	3.4. Les enjeux humains

Recommandations		Calendrier de mise en œuvre	Développement dans la revue
Diffusion de la culture de la sécurité numérique dans toute la société	• Création par l'ANSSI d'une application ludique, disponible sur *smartphone*, permettant aux Français de tester leur niveau de connaissances dans le domaine de la culture de la sécurité numérique et leur proposant de nombreux défis. • Etude de l'apport des *nudges* pour le développement de l'autonomie des citoyens en matière de cybersécurité. • Intégration d'une dimension cybersécurité au programme de soutien à la transformation numérique des entreprises du ministère de l'économie et des finances et du secrétariat d'état au numérique. • Perfectionnement de la gestion des compétences dans les services chargés de la cyberdéfense de l'Etat.	Moyen terme	3.4. Les enjeux humains

Annexes

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Le Premier Ministre

Paris, le 21 JUIL. 2017
№ - 7023

NOTE
à l'attention de
Monsieur le Secrétaire général de la défense et de la sécurité nationale

Objet : Mandat pour une revue stratégique de cyberdéfense.

Face à une menace d'origine cyber qui ne cesse de croître dans ses formes et son intensité, la prise en compte des questions de cybersécurité est un impératif. De nombreuses initiatives ont déjà été lancées et des capacités significatives ont déjà été mises en place. Cependant, de nombreux chantiers restent à instruire et d'importants efforts doivent encore être consentis.

La menace d'origine cyber doit se voir opposer un dispositif national de protection et de défense informatique qui repose sur des capacités et des compétences diverses et qui implique de nombreux acteurs étatiques ou privés. La conduite d'une revue stratégique nationale et globale de cyberdéfense doit permettre de développer et de structurer un tel dispositif national. La responsabilité de sa mise en œuvre vous est confiée.

Sur la base d'un retour d'expérience du modèle mis en place, séparant les missions défensives et offensives, cet exercice validera et assumera formellement le choix du dispositif français de cyberdéfense. Les principes de l'articulation entre ces deux volets pourront être utilement décrits dans un document dont la diffusion sera restreinte si nécessaire. Les éléments de gouvernance et de doctrine déjà existants en matière de défense et de protection, telle que la stratégie nationale de sécurité du numérique, seront pris en considération dans la revue, qui proposera par ailleurs les éléments de gouvernance restant à produire, y compris au travers d'éventuelles mesures législatives.

Tout en s'attachant l'adhésion du plus grand nombre aux enjeux de sécurité du numérique, et à la lumière d'une nécessaire mise en perspective à l'échelle européenne, les enjeux de souverainetés numérique et économique seront mis en évidence.

Sur le fond, cette revue abordera notamment les points suivants :

- l'analyse de la menace et la prévention ;
- la réaction, la gestion et les options de réponse en cas de crise majeure ;
- les moyens de détection, de caractérisation et d'attribution des actes de cyber malveillance, de cybercriminalité, ou de tout type de cyberattaque ;
- les aspects internationaux liés au cyberespace, notamment dans le domaine juridique ;
- l'organisation de la capacité nationale de lutte informatique et son contrôle ;
- la structuration d'une politique industrielle en matière de sécurité du numérique, définissant le cœur de souveraineté numérique au sens industrie et technologies, permettant d'équilibrer les relations avec les acteurs industriels étrangers, tout en garantissant la bonne résilience de l'Internet français et des activités souveraines de l'Etat.

Hôtel de Matignon - 57, rue de Varenne - 75007 PARIS - Téléphone : 01 42 75 80 00

Les conclusions de cette revue s'attacheront à proposer une programmation des moyens humains et budgétaires en cohérence avec les enjeux sécuritaires et sociétaux posés par le numérique. Une partie des moyens de cyberdéfense relevant du ministère des armées, cette programmation sera réalisée en concordance avec celle issue de la revue stratégique des armées.

L'organisation des travaux s'appuiera sur des groupes de travail interministériels, et favorisera une large consultation des acteurs de la politique nationale de cyberdéfense.

Par ailleurs, cet exercice impliquera les « forces vives du numérique » soit un large panel de contributeurs qu'il s'agisse d' acteurs publics ou privés, d'opérateurs de communication et de service, de régulateurs, d'experts industriels ou universitaires, de parlementaires, de citoyens ou encore de partenaires internationaux.

Cette démarche fera l'objet d'un rapport public – ainsi que, autant que de besoin, d'éventuels compléments classifiés.

Un point d'étape sera fait à la fin du mois de septembre 2017. Il dégagera les principales orientations proposées et les arbitrages nécessaires, en cohérence avec la revue stratégique des armées. Un rapport me sera également remis à la fin de cette année. Le respect de ces deux échéances permettra d'élaborer les premiers textes législatifs ou réglementaires, et de mettre en place les éléments de programmation budgétaire dès le début de l'année 2018.

Edouard PHILIPPE

Annexe 2 – Liste des sigles utilisés dans la revue stratégique de cyberdéfense

AMF	Autorité des marchés financiers
ANSSI	Agence nationale de la sécurité des systèmes d'information
APT	Advanced Persistent Threat
AQSSI	Autorité qualifiée SSI
CERT	Computer Emergency Response Team
CIA	*Central Intelligence Agency*
CNCTR	Commission nationale de contrôle des techniques de renseignement
CNRLT	Coordonnateur national du renseignement et de la lutte contre le terrorisme
CSIRTs	*Computer Security Incident Response Teams*
CSPN	Certification de Sécurité de Premier Niveau
CVE	*Common Vulnerabilities and Exposures*
DDOS	Technique du déni de service
DGA	Direction générale de l'armement
DGSE	Direction générale de la sécurité extérieure
DGSI	Direction générale de la sécurité intérieure
DHS	*Department of Homeland Security*
DINSIC	Direction interministérielle du numérique et du système d'information et de communication de l'Etat
ESSI	Expert en sécurité des systèmes d'information
ETI	Entreprise de taille intermédiaire
GCHQ	Government Communication Headquarters
GGE	Groupe des experts gouvernementaux sur la cybersécurité
IA	Intelligence Artificielle
IP	Internet Protocole
LIA	Lutte informatique active
LID	Lutte informatique défensive
LPM	Loi de programmation militaire
NSA	National Security Agency
OIV	Opérateur d'importance vitale

OTAN	Organisation du traité de l'Atlantique nord
PASSI	Prestataires d'audit en sécurité des systèmes d'information
PDIS	Prestataires de détection d'incidents de sécurité
PRIS	Prestataires de réponse à incident de sécurité
PDIS	Prestataire de détection d'incidents de sécurité
PME	Petites et moyennes entreprises
PPDR	*Public Protection and Disaster Relief*
PRIS	Prestataire de Réponse à Incidents de Sécurité
PSSIE	Politique de sécurité des systèmes d'informations
RGPD	Règlement général européen sur la protection des données personnelles
RIE	Réseau interministériel de l'Etat
SGDSN	Secrétariat général de la défense et de la sécurité nationale
STAD	Système de traitement automatisé de données
TNP	Traité de non-prolifération

Annexe 3 – Liste des figures

Annexe 4 – Liste des encadrés

Annexe 5 – Glossaire

Agrément de produit : validation par l'ANSSI de la capacité d'un produit à protéger des informations classifiées.

APT - *Advanced Persistant Threat* : groupe d'attaquants informatiques disposant de compétences élevées et de ressources importantes, en mesure de conduire des attaques informatiques sophistiquées, souvent caractérisé par un ensemble d'outils ou de techniques spécifiques.

Botnet : réseau de machines compromises par un attaquant, structuré de façon à lui permettre de leur transmettre des ordres et de les actionner à sa guise.

Certification de produits : validation de la sécurité d'un produit par le biais d'une évaluation menée par un acteur tiers qualifié par l'ANSSI.

Cheval de Troie : programme en apparence légitime, mais qui possède une fonction cachée malveillante.

Code malveillant *(malware)* : tout programme développé dans le but de nuire à un système d'information.

Common Vulnerabilities and Exposures (CVE aussi appelée One-day) : vulnérabilité dans un produit informatique connue de la communauté de la sécurité informatique et ayant généralement fait l'objet d'un correctif de sécurité. Les CVE sont répertoriées par l'année et un numéro d'identifiant unique. Ainsi la CVE 2017-0143 est la faille dénommée ETHERNAL BLUE et utilisée par le rançongiciel WANNACRY.

***Computer Emergency Response Team* (CERT) ou *Computer Security Incident Response Team* (CSIRT)** : centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous.

Darkweb : ensemble des sites Internet qui fonctionnent sur des réseaux uniquement accessibles via des logiciels, des configurations ou des autorisations spécifiques, permettant généralement une forme d'anonymat.

Défiguration (ou défacement): attaque informatique consistant à modifier la présentation d'un site Internet.

Déni de service (DoS) : attaque informatique ayant pour but de rendre indisponible un service en submergeant ses ressources informatiques de trafic inutile. Lorsque l'attaque est conduite à l'aide de plusieurs sources de trafic malveillant, on parle de déni de service distribué (DDoS).

Exploit : code malveillant associé à une vulnérabilité affectant un équipement informatique, permettant à un attaquant d'en prendre le contrôle en exploitant cette vulnérabilité.

Flooding : action qui consiste à « inonder » une information en la noyant sous une pluie

d'informations inutiles pour la rendre inaccessible.

Hackback : contre-attaque informatique utilisée en réponse à une attaque informatique dans l'objectif de faire cesser l'attaque, de récupérer des données volées ou d'infliger à l'attaquant une sanction.

Hameçonnage *(fishing)* : technique consistant à amener, souvent par le biais d'un e-mail frauduleux, un individu à communiquer des informations confidentielles (mots de passe, données bancaires...) sur Internet, à ouvrir un fichier piégé ou à cliquer sur un lien malveillant.

Homologation de sécurité : décision formelle, prise par le responsable d'une organisation, qui atteste qu'il assume les risques pesant sur la sécurité d'un système d'information.

Implant : code malveillant utilisé par un attaquant pour se maintenir et évoluer dans un système d'information infecté et produire les effets recherchés (exfiltration de données, sabotage...).

Infrastructure d'attaque : ensemble de serveurs contrôlés par un attaquant et utilisés pour conduire une attaque informatique.

Labellisation : label donné par l'ANSSI à un produit ou services correspondant à un cahier des charges qu'elle a défini.

Latéralisation : phase d'une attaque informatique consistant pour un attaquant à étendre son contrôle sur le système d'information ciblé en se propageant au sein du réseau infecté.

Pare-feu *(firewall)* : équipement logiciel ou matériel permettant de filtrer ou bloquer des flux de données pour protéger un système d'information.

Porte dérobée *(backdoor)* : fonctionnalité cachée d'un équipement informatique, prévue par son éditeur ou implantée par un acteur malveillant, permettant d'y accéder à l'insu de son utilisateur légitime.

Pot de miel *(honeypot)* : technique de cyberdéfense consistant à leurrer un attaquant en l'attirant vers une fausse cible afin d'observer son mode opératoire.

Qualification de prestataire : validation par l'ANSSI de la capacité d'un prestataire à réaliser des prestations.

Qualification de produit : certification de sécurité pour laquelle l'administration a défini le périmètre de l'évaluation.

Rançongiciel : programme malveillant qui chiffre les données présentes sur un système d'information et demande une rançon en échange de leur déchiffrement.

Remédiation : à la suite d'une attaque informatique, ensemble des actions destinées à éradiquer l'attaquant du système d'information victime et à durcir sa sécurité.

Script kiddies : terme péjoratif désignant des néophytes qui utilisent sans réelles compétences des outils d'attaque informatique conçus par d'autres.

Sinkholing : technique de cyberdéfense consistant à rediriger du trafic malveillant vers un serveur maîtrisé afin d'observer le mode opératoire d'un attaquant.

Système de commande et de contrôle : partie d'une infrastructure d'attaque utilisée pour superviser et piloter l'ensemble des codes malveillants déployés dans le cadre d'une attaque.

Ver : code malveillant autonome qui se réplique lui-même afin de se propager à d'autres machines.

Vulnérabilité : erreur de conception ou faiblesse dans un équipement informatique susceptible de permettre à un attaquant de conduire une action malveillante à son encontre.

Zero-day : vulnérabilité dans un produit informatique n'ayant fait l'objet d'aucune publication et dont la communauté de la sécurité informatique n'a pas connaissance.

Annexe 6 - Les quatre phases du cycle de vie du système d'information

- **Concevoir un système d'information sécurisé**

La conception d'un système d'information constitue une étape primordiale de sa sécurisation, qui s'applique aussi bien à un développement logiciel ponctuel qu'à la mise en place et à l'intégration d'un système d'information complet. Elle doit permettre la définition d'une stratégie globale de sécurisation, et des grands choix qui la sous-tendent, tant sur le plan technique (architecture générale du système et positionnement des fonctions de sécurité, choix de développement ou de configuration) qu'organisationnel (définition des rôles et responsabilités, des procédures à élaborer et de la politique de sécurité applicable).

En règle générale, ces choix doivent découler conjointement de la déclinaison de bonnes pratiques génériques, applicable à tout système, et d'une analyse de risque spécifique au système considéré. Les bonnes pratiques applicables, qui forment un socle de sécurité global, peuvent être issues d'un cadre réglementaire applicable (par exemple les mesures de sécurité fixées par des arrêtés sectoriels applicables aux OIV), ou à défaut de la déclinaison d'un ensemble de bonnes pratiques élémentaires, adaptables à tout système d'information, généralement dénommées pratiques d'hygiène informatique. L'analyse de risque vise quant à elle à compléter ce socle, en définissant méthodiquement les biens essentiels du système à protéger et les scénarios de menace applicables, pour en déduire des mesures complémentaires.

Les mesures de prévention *in fine* adoptées, si elles sont propres au système étudié, n'en déclinent pas moins en général de quelques grands principes éprouvés de protection, ou de mitigation des impacts, qu'il est utile de rappeler ici :

- la défense en profondeur, qui consiste à mettre en place des barrières de sécurité redondantes réparties dans l'ensemble du système d'information, de manière à contrer la possible défaillance d'une barrière donnée ;
- le principe de moindre privilège, qui vise à ne conférer à chaque composant (logiciel, serveur, etc.) ou acteur du système d'information que les seuls droits dont il a strictement besoin pour remplir son rôle, de manière à limiter la portée de sa défaillance ou malveillance éventuelle ;
- la séparation des rôles, qui complète le point précédent en limitant de fait les privilèges qu'il est nécessaire d'accorder à un acteur donné ; la sécurité du rôle d'administration, et son isolation stricte, revêtent une importance toute particulière au regard des techniques d'attaques couramment rencontrées ;
- le cloisonnement logique, qui consiste à diviser le système d'information, sur différents plan (réseau, matériel, logiciel), en compartiments logiques aussi étanches que possible entre eux, de manière là encore à limiter la portée d'une attaque ;

- le bon usage de la cryptographie, et notamment le chiffrement systématique des données sensibles lors de leur transmission ou de leur stockage, et l'authentification robuste de tous les accès au système ;
- la sécurisation des interfaces du système, de manière à valider l'innocuité de toutes les données entrantes (validation de format et de provenance, recherche de codes malveillants connus, etc.).

Ces choix, impérativement documentés, doivent également garantir à terme la capacité de maintenir et superviser le système dans la durée, notamment par l'inclusion de mécanismes de mise à jour des différents composants du système, par l'élaboration d'une politique de journalisation adaptée à l'investigation des incidents potentiels, et par le positionnement adéquat de moyens de détection d'attaques adaptés au système.

- **Vérifier la sécurité**

À l'issue de la conception d'un système d'information (qu'il s'agisse de sa conception initiale ou de celle d'une évolution significative), il est impératif de procéder à une vérification formelle de sa sécurité, en respectant un principe fondamental de séparation des rôles et responsabilités entre les acteurs qui conçoivent ou développent le système, et ceux qui le vérifient *in fine*. Cette vérification, qui complète sur le plan sécuritaire la recette fonctionnelle du système, doit poursuivre un triple objectif de validation de la conformité du système avec sa spécification et ses exigences de sécurité, de test indépendant de vulnérabilité, qui vise à simuler l'interaction d'un attaquant avec le système pour en identifier les vulnérabilités résiduelles, et d'engagement formel de responsabilité quant à l'adéquation du système avec ses besoins de sécurité.

Dans le cas d'un produit de sécurité individuel (logiciel par exemple), la certification de sécurité, ou des dispositifs complémentaires comme la qualification ou l'agrément de sécurité, constitue généralement le vecteur privilégié de vérification de la sécurité. Elle repose sur une évaluation par un organisme tiers, dont la compétence et l'indépendance sont reconnues, pour la validation de conformité et le test de vulnérabilité, et sur une décision de certification prononcée par l'ANSSI, qui engage sa responsabilité et atteste de la résistance adéquate du produit.

A contrario, dans le cas d'un système d'information complet, la vérification de la sécurité repose généralement sur une procédure d'homologation du système. Celle-ci s'appuie sur un audit de sécurité du système, conduit par un tiers, afin de jauger la conformité du système aux bonnes pratiques et sa résistance à un attaquant, et sur une décision d'homologation, qui autorise formellement la mise en service du système sur la base des résultats de l'audit et d'une actualisation de l'analyse de risque initiale. Cette décision ne peut être prise que par l'autorité d'emploi du système, seule à même de juger du bon équilibre entre les besoins sécuritaires et fonctionnels applicables à celui-ci.

- **Gérer la sécurité dans la durée**

Le niveau de sécurité initialement établi lors de la mise en service du système d'information

doit faire l'objet d'une gestion active pour être maintenue dans la durée. Celle-ci, portée par une organisation clairement établie, poursuit un double objectif. Le premier est le maintien en conditions de sécurité des mesures préventives, notamment à travers la mise à jour régulière des composants logiciels du système, la gestion des obsolescences matérielles et l'actualisation régulière des droits des utilisateurs. Le second est la supervision de la sécurité effective du système, en particulier par la collecte et l'analyse régulière de ses journaux de fonctionnement, afin d'y détecter d'éventuels événements anormaux, et par la mise en œuvre de moyens spécialisés de détection d'attaques informatiques (sondes de détection réseau, antivirus ou agents de détection déployés sur les postes informatiques, etc.).

Les mécanismes de détection d'attaques s'appuient généralement sur une base de marqueurs, ou signatures, caractéristiques d'attaques connues, qui doit être régulièrement actualisée. La vérification de l'authenticité des mises à jour de cette base, comme de celles des composants logiciels du système, constitue un point d'attention important.

Lorsque le système d'information à protéger présente une étendue significative, la conduite efficace des différentes opérations de gestion de la sécurité nécessite la mise en place d'un centre opérationnel de sécurité, ou *Security Operations Center* (SOC). Véritable poste de pilotage de la sécurité du système, celui-ci dispose d'outils et de personnels spécialisés, et est alimenté en permanence par les différents moyens de supervision du système, de manière à présenter à tout instant un tableau à jour de l'état de sécurité, des faiblesses connues et opérations planifiées, et des événements anormaux, dysfonctionnements ou attaques en cours. Intégré au cœur du cycle de vie du système, il constitue un vecteur primordial d'amélioration continue de sa sécurité, et l'instance de décision permettant de déclencher le traitement réactif d'une attaque.

- **Réagir aux attaques**

L'identification d'une attaque avérée doit provoquer l'activation de procédures de réaction et de traitement d'incident. Dans la mise en œuvre de celles-ci, la tentation naturelle de bloquer ou d'évincer au plus vite l'attaquant doit être tempérée par la nécessité d'observer celui-ci afin de mieux comprendre son mode d'action. Ainsi, à de rares exceptions près où l'urgence primerait, le déclenchement des opérations de remédiation active doit être précédé d'une phase d'analyse passive, visant à mieux cerner la méthode et les outils mis en œuvre par l'attaquant, les faiblesses qu'il exploite ou cherche à exploiter, le périmètre qu'il est effectivement parvenu à compromettre au sein du système d'information, et dans la mesure du possible les finalités de son action.

La discrétion est une composante essentielle de cette phase d'observation, l'attaquant ne devant en aucun cas découvrir qu'il a été identifié. L'analyse mobilise généralement un vaste panel de compétences techniques, comme l'analyse de code malveillant, l'analyse forensique de journaux ou supports informatiques, ou encore l'audit de configuration, et doit faire l'objet d'un pilotage adapté qui en garantisse l'exhaustivité, la cohérence et la discrétion.

La finalisation de cette phase d'analyse permet l'élaboration d'un plan de remédiation, qui vise en priorité l'éviction effective de l'attaquant et la restauration du système dans un état

nominal, mais également l'adoption de mesures préventives complémentaires (mesures dite de « durcissement »), immédiatement avant ou après la restauration, de telle sorte que l'attaquant ne reprenne pas subséquemment pied au sein du système. Dans le cas où le système compromis est de grande taille et a fait l'objet d'une compromission à grande échelle, la remédiation se fait généralement par phases successives, avec la création dans un premier temps d'un cœur de confiance sain, à périmètre réduit, puis l'extension progressive et planifiée de ce périmètre sain au reste du système.

Il est à noter qu'au-delà des attaques effectivement réussies, l'identification de tentatives d'attaque en échec peut dans certains cas constituer également un incident notable, justifiant la mise en œuvre de mesures réactives. En effet, ces tentatives sont potentiellement préfiguratrices d'autres opérations hostiles à venir, dont elles constitueraient par exemple la phase exploratoire visant à mieux cerner les défenses du système. Dans ce cas, la mise en œuvre d'un plan de réaction peut s'imposer, avec *a minima* une phase d'observation et le cas échéant la mise en œuvre de mesures de sécurité permanentes ou temporaires.

Dans tous les cas, l'achèvement des travaux de réaction à une attaque doit donner lieu à un travail de capitalisation et de retour d'expérience, entraînant le cas échéant l'élaboration d'un plan d'amélioration de la sécurité du système d'information, qui se traduira par l'engagement d'un nouveau cycle de conception et vérification.

Annexe 7 – Les options de réponse aux attaques informatiques

- **Prévenir et gérer les crises via la coopération internationale**

En cas d'incident ou de crise cyber, national ou international, et ce quelle que soit la qualification retenue pour cet incident ou cette crise, la France pourra activer certains mécanismes au niveau politico-diplomatique afin de participer à la gestion de cette crise, à sa résolution et au contrôle de toute potentielle escalade.

- *Premier objectif : prévenir les crises et décourager les agressions*

Avant même que ne soit présentée des options de réponse à une crise cyber, il convient de rappeler que le premier objectif poursuivi par la France est la prévention de telles crises. Outre le renforcement de la résilience globale du cyberespace, de la coopération entre les Etats et de la régulation internationale de l'espace numérique, cela passe également par une stratégie visant à décourager toutes agressions. A travers ses prises de position, la France signale ainsi les comportements qu'elle estime acceptable et ce qui ne l'est pas et se réserve la possibilité de notifier à l'agresseur ces derniers ainsi que les moyens à sa disposition visant à sanctionner les comportements agressifs.

La France répondra également aux engagements qu'elle a pris envers ses alliés et ses partenaires de l'Union européenne et de l'OTAN qui seraient confrontés à des attaques de ce type, dans le respect de leur souveraineté et en tenant compte de leur responsabilité principale en matière de protection des réseaux. La solidarité avec nos partenaires ne peut être effective qu'en appui d'un effort de cyberdéfense mené par tous au niveau national.

Parfois, la réponse appropriée à une attaque informatique pourra être donnée à plusieurs. Dans tous les cas, elle se fondera sur une décision entièrement souveraine, de la France, comme de ses alliés.

- *Deuxième objectif : contribuer sur le plan international au traitement d'une attaque*

  - Dévoiler l'attaque

La révélation d'éléments concernant l'attaque constitue une première forme de réponse dans la mesure où ceux-ci peuvent limiter les capacités d'action de l'attaquant voire se montrer déstabilisant pour ce dernier. Par ailleurs, cette démarche ouvre potentiellement la voie à une réponse publique de la part de la France.

  - Contribuer à la résolution technique de l'incident

La coopération internationale est un élément clé dans le traitement des attaques transitant par un Etat tiers. C'est pourquoi la France a promu dans le cadre des Nations Unies la norme selon laquelle « *les Etats devraient répondre aux demandes appropriées visant à atténuer les conséquences d'activités informatiques malveillantes dirigées contre une infrastructure essentielle d'un autre*

État et exercées depuis leur territoire »[76]. Cette norme, qui a l'avantage d'être neutre quant à l'attribution, pourrait à terme favoriser la mise en place d'une « chaîne de responsabilité » permettant à l'Etat victime de bénéficier de l'assistance des Etats par lesquels transite l'attaque.

Dans la mise en œuvre pratique de la norme portant sur la responsabilité des Etats, le réseau diplomatique pourra être mis à contribution.

– Communiquer efficacement sur une attaque en cours

La France devra être en mesure de répondre aux sollicitations pour information de ses partenaires. Une communication sur une attaque subie permet en effet d'instaurer un lien de confiance avec nos partenaires et d'éventuellement obtenir leur soutien ultérieur dans le cas où une réponse serait envisagée.

Une telle communication pourrait également être portée par les représentants français au sein du COPS ou du Conseil de l'Atlantique Nord (éventuellement au titre de l'article 4 du Traité de l'Atlantique Nord, relatif aux consultations politiques à la demande d'un Allié).

▪ *Troisième objectif : participer à la résolution de la crise*

Les risques de perception erronée due à la complexité de l'attribution, de même que la difficulté à apprécier l'ampleur d'une agression et à définir une réponse proportionnée sont autant de facteurs qui pourraient complexifier une stratégie de maîtrise de l'escalade en cas de crise. Le recours à des instruments multilatéraux et bilatéraux de diplomatie préventive devra dès lors être privilégié.

Au niveau bilatéral, la France s'efforcera de développer des mécanismes d'échange et de désescalade avec les autres puissances cyber. Complémentaire aux dispositifs existants, tels que les liaisons d'Etat ou les relations diplomatiques, ceux-ci pourront s'articuler autour de deux axes :

- l'établissement d'un canal de communication entre responsables de haut niveau en matière de cyberdéfense, activable notamment en cas d'incident cyber majeur à des fins de dialogue ;
- l'établissement d'un processus de notification permettant notamment l'envoi de requêtes formelles telles qu'en matière d'entraide (e.g. demande de coopération officielle des autorités sur une activité malveillante transitant par l'un des deux pays et ciblant l'autre).

De tels mécanismes permettraient :

- de réduire le risque d'attribution erronée d'attaques dont la France serait victime, en laissant la possibilité au pays suspecté d'apporter les éléments lui permettant

[76] Rapport du groupe d'experts gouvernementaux de l'ONU sur la cybersécurité de juin 2015.

éventuellement de se disculper ou les mesures qu'il aurait prises en matière de *cyber-diligence* ;

- de favoriser le dialogue comme premier outil dans la résolution de différends entre les deux pays susceptibles de porter atteinte à leurs intérêts fondamentaux réciproques.

Signal de la volonté des autorités françaises d'œuvrer à préserver la paix et la sécurité internationale dans le cyberespace, ce type de mécanisme constitue une « mesure de renforcement de la confiance » conforme aux recommandations des rapports du groupe d'experts gouvernementaux de l'ONU sur la cybersécurité agréées par les deux Etats en 2013 et 2015.

De tels réseaux viendraient compléter ceux mis en place au niveau régional par certaines organisations comme l'OSCE (qui gère depuis 2013 un réseau de points de contacts technique et diplomatique visant à faciliter la communication entre Etats en cas de crise cyber et mécanisme de consultation de crise pour les Etats parties à une crise cyber, avec une possible médiation par l'OSCE ou par un Etat participant tiers).

Au niveau de l'ONU, une saisine du Conseil de sécurité au titre de l'article VI de la Charte des Nations Unies (Résolution pacifique des différends) pourrait être envisagée, notamment en l'absence d'« agression armée », si la France estime que la situation est suffisamment grave pour être qualifiée de menace contre la paix et la sécurité internationales.

Une mobilisation du Conseil de sécurité à l'initiative de la France pourrait prendre la forme d'une réunion d'urgence ou d'une expression formelle du Conseil (déclaration à la presse, déclaration présidentielle, résolution).

Une autre possibilité pourrait être de saisir, si les conditions le permettent, les mécanismes régionaux de coopération et d'assistance dans le domaine cyber, que ce soit au sein de l'OSCE ou de l'OTAN et de l'Union européenne. En effet, ces deux dernières organisations permettent à la France de bénéficier chacune d'un mécanisme d'assistance par l'invocation des articles 4 et 5 du Traité de l'Atlantique Nord et par l'article 42.7 du Traité de l'Union européenne. La coopération policière et judiciaire, européenne comme internationale, pourrait également être recherchée.

- **Recourir à des mesures de rétorsion**

Si la prévention, la coopération et la négociation ne produisent pas les effets escomptés, la France pourrait choisir de recourir à des mesures de rétorsion.

  - *Au niveau national*

A la différence des contre-mesures ou des représailles, les mesures de rétorsion sont des actes contraignants mais licites et légaux au sens du droit international par nature. Elles n'impliquent ainsi pas l'obligation de justifier juridiquement leur adoption.

Ainsi, pour tout incident cyber la concernant, quel que soit le niveau de gravité de celui-ci,

et pour laquelle elle suspecterait l'implication, directe ou indirecte, d'un Etat, la France pourrait activer une gamme de mesures de rétorsion réversibles contre cet Etat, par exemple dans les domaines diplomatiques ou économiques.

Une action coordonnée peut également être conduite pour engager des poursuites judiciaires contre les responsables individuels d'une agression attribuée à un Etat.

- *Au niveau de l'Union européenne*

L'UE et ses Etats Membres se sont récemment accordés sur un cadre prévoyant une réponse diplomatique conjointe aux crises cyber. Ces mesures relèvent de mécanismes de coopération internationale, de prévention et de communication, mais prévoient aussi des types de réponse plus contraignants tels que les sanctions.

A ces actions pourraient s'en ajouter d'autres, relevant de compétences communautaires : en réponse à des pratiques de cyberespionnage à visée économique, par exemple, la Commission européenne pourrait demander l'ouverture d'un contentieux devant l'Organe de règlement des différends de l'OMC, sur le fondement d'une violation des accords ADPIC.

- **Adopter des contre-mesures**

En vue de répondre à une situation qui comporte à son avis la violation d'une obligation internationale par un autre Etat, la France pourrait adopter, outre des mesures de rétorsions, des mesures non-conformes à ses obligations internationales ; on parle de contre-mesures. L'adoption de telles mesures est licite si les conditions suivantes sont réunies :

- l'action de la France est conduite en réponse à un fait internationalement illicite initial (y compris un usage de la force), et a pour unique but la cessation de celui-ci ;
- l'action de la France est nécessaire et proportionnée à cet objectif, et doit rester pacifique (en dessous du seuil du recours à la force).

Ces contre-mesures pourront être de nature cyber, ou non. En effet, les moyens pour riposter à une attaque n'étant pas conditionnés pas le type d'armes employés, en cas d'attaque informatique, la France, comme chaque Etat, pourra choisir de riposter par d'autres moyens d'action, comme par exemple par l'adoption de sanctions.

- **Autres options de réponse**

Conformément aux principes fondamentaux du droit international, la licéité du recours à la force armée par un Etat sur le territoire d'un autre Etat est limitée à trois hypothèses :

- si l'Etat sur le territoire duquel l'intervention armée a lieu y consent ;
- si une résolution du Conseil de sécurité des Nations Unies, placée sous chapitre VII

de la Charte, autorise une telle intervention ;

- si l'Etat intervient sur le fondement de la légitime défense (individuelle ou collective) pour faire face à une agression armée au sens de l'article 51 de la charte, et dans l'attente d'une action du Conseil de sécurité.

Une attaque informatique majeure visant la France, eu égard aux graves dommages qu'elle causerait, pourrait constituer une « agression armée » au sens de l'article 51 de la Charte des Nations Unies et justifier ainsi l'invocation de la légitime défense. L'usage éventuel de la force par la France en retour pourrait alors inclure des actions en matière de lutte informatique offensive, sans se limiter à ces seuls moyens.

Annexe 8 – Déclinaison en actions opérationnelles du soutien français à apporter aux initiatives répondant au besoin croissant de coopération face à des attaques d'ampleur européenne

L'approche française sera fondée sur 4 axes,

Axe 1 : Maintenir une posture claire en matière de répartition des compétences et de préservation de la souveraineté nationale en matière de réponse opérationnelle

Assumer que la coopération opérationnelle y compris sectorielle, ne peut fonctionner que sur une **base exclusivement volontaire** pour permettre le développement de la confiance, en excluant notamment toute contrainte en matière de partage d'informations entre Etats et avec les institutions de l'Union européenne (ex : notifications d'incidents) ou de réponse à un incident ;

Axe 2 : Promouvoir le renforcement des capacités nationales cyber sur les plans humain et technique, notamment via un soutien accru de l'UE aux Etats

[Action 1] **Proposer l'adoption par le Conseil de l'UE d'un « engagement de cyberdéfense » (« *Cyberdefence Pledge* »)** engageant souverainement tous les Etats à renforcer leurs capacités nationales, associé à un mécanisme de « parrainage » entre Etats afin d'accompagner les efforts des Etats qui en expriment le besoin. Un tel engagement a déjà été pris par les Etats membres de l'Alliance Atlantique lors du Sommet de 2016 ;

[Action 2] Continuer à inviter l'UE à **renforcer son action en soutien à la formation** d'experts cyber, via notamment le projet de l'AED et du CESD d'établissement d'une plateforme dédiée à l'enseignement et à la formation ;

[Action 3] Inviter l'UE à **renforcer son soutien financier direct aux Etats** engagés dans le renforcement de leurs moyens humains et matériels en matière de réponse opérationnelle (sur le modèle du mécanisme d'interconnexion en Europe – « *Connecting Europe Facility* ») ;

[Action 4] Soutenir le **renforcement significatif du budget de l'ENISA** en appui de ses activités de soutien au développement capacitaire des Etats, et de son rôle de facilitateur de la coopération opérationnelle entre Etats-membres.

Axe 3 : Encourager le développement de la coopération opérationnelle au sein de l'UE

[Action 5] Soutenir l'élaboration par le Conseil de l'Union européenne, sur proposition de la commission européenne, d'un **cadre européen de gestion des crises cyber** clarifiant les rôles et responsabilités, les mécanismes et les outils ;

[Action 6] Contribuer au développement des outils et procédures (notamment les

« standard operating procedures » (SOPs) portées par l'ENISA) appelés à soutenir la **coopération en cas d'incidents** et de crises ;

[Action 7] Continuer à **participer aux exercices européens** dédiés à la cybersécurité, contribuer à leur évolution et veiller à l'inclusion d'une dimension cybersécurité au sein des autres exercices de gestion des crises de l'Union européenne ;

[Action 8] Promouvoir la **coopération mais aussi désormais la coordination entre autorités nationales de cybersécurité** au niveau européen en cas d'incidents ou de crises (trouver un accord entre Etats-membres sur la répartition des rôles) ;

[Action 9] Continuer de soutenir le **« réseau des CSIRTs »** (partage d'informations, participation au développement de ses outils et procédures, etc.) créé par la directive NIS comme instance privilégiée de coopération opérationnelle multilatérale entre Etats membres au sein de l'UE, avec un soutien accru de l'ENISA dans son fonctionnement.

Axe 4 : Promouvoir un modèle adapté d'assistance aux Etats en cas d'incident, en soutenant notamment le développement d'un secteur privé européen de confiance fournissant des services de cybersécurité mobilisables en cas de crise

[Action 10] Promouvoir l'établissement d'un **cadre européen de certification des produits et services de cybersécurité** (détection, réponse à incidents, audit, etc.) et tenir à la disposition de l'ensemble des Etats membres un catalogue européen des fournisseurs certifiés auquel faire appel en cas d'incidents courants et graves ;

[Action 11] **Examiner l'opportunité de conclure un contrat-cadre européen de fournisseurs et prestataires certifiés**, financé par l'Union européenne et pouvant être utilisés sur demande d'Etats en cas d'incident grave ou de crise cyber après accord du Conseil de l'Union européenne ;

[Action 12] Proposer au sein du Conseil de l'Union européenne, la formalisation d'un **processus d'assistance mutuelle** entre Etats en cas d'incident grave ;

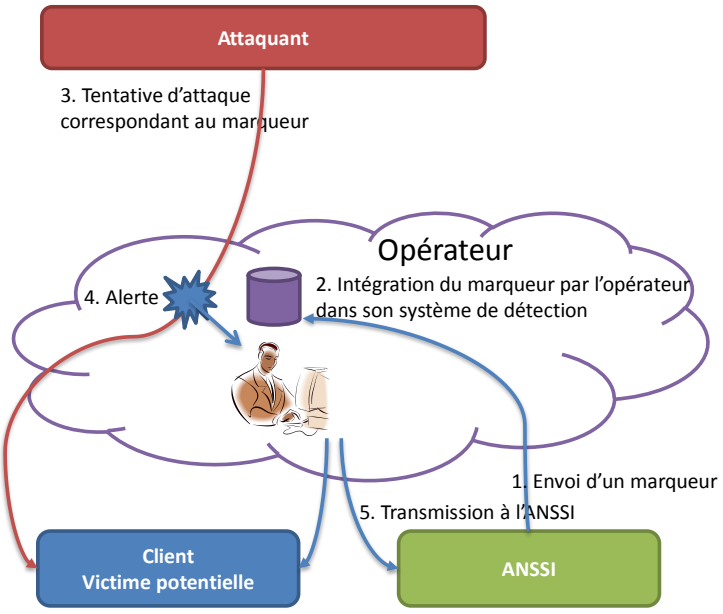
[Action 13] En appui d'Etats qui formaliseraient une demande d'assistance, **examiner l'opportunité d'établir une force de remédiation rapide** (« *Rapid Reaction Team* ») européenne composée de représentants d'Etats-membres volontaires, au mandat limité à de l'assistance stratégique dans les cas les plus graves et dont l'activation prendrait, comme à l'OTAN, appui sur un mécanisme de décision de niveau politique - dans ce contexte, la question de l'applicabilité et du recours à la clause de solidarité en cas d'attaques cyber doit être étudiée plus précisément.

Annexe 9 – Description opérationnelle des mesures cyber incluses dans le projet de loi de programmation militaire

Les opérations de cyberdéfense conduites par l'ANSSI en 2017 ont révélé l'apparition de nouveaux modes d'attaques informatiques. Les attaquants utilisent dorénavant des moyens indirects pour atteindre leurs cibles, tels que la prise de contrôle d'équipements d'accès à Internet, la compromission de prestataires afin d'atteindre leurs clients, ou la location de serveurs auprès d'hébergeurs français pour conduire des attaques.

Face à ces nouvelles menaces, une implication accrue des opérateurs de communications électroniques et des hébergeurs, dont les serveurs et les réseaux servent de relais aux attaquants, est nécessaire.

Implication des opérateurs de communications électroniques dans la détection des attaques informatiques



Etape 1 : L'ANSSI transmet à l'opérateur un marqueur technique relatif à un attaquant donné (ex : adresse IP d'un serveur appartenant à l'attaquant, site Internet piégé)

Etape 2 : L'opérateur inclut le marqueur transmis par l'ANSSI dans son système de détection

Etape 3 : L'attaquant cherche à compromettre une victime *via* une communication malveillante (communication depuis l'adresse IP malveillante, courriel contenant un lien vers le site piégé)

Etape 4 : Une alerte de sécurité est générée par le système de détection

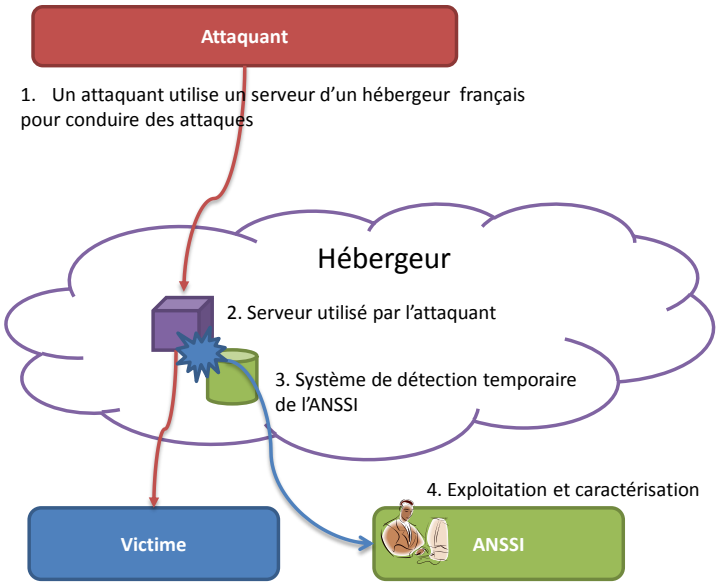
Etape 5 : L'opérateur transmet l'alerte à l'ANSSI, ainsi que les éléments techniques nécessaires à la caractérisation de l'attaque si la victime est un OIV ou une autorité publique

Le premier volet du dispositif proposé consiste à autoriser les opérateurs de communications électroniques à mettre en œuvre des systèmes de détection dans leurs réseaux afin de détecter les attaques informatiques visant leurs abonnés. Il s'agit de dispositifs techniques qui comparent l'activité d'un réseau à des marqueurs d'attaque. A l'image des scanners à rayons X utilisés dans le monde physique, ces dispositifs analysent automatiquement le trafic sans s'intéresser au contenu, en se limitant à le comparer aux marqueurs d'attaque. Tout est réalisé en temps réel et le trafic n'est pas conservé.

Pour leur permettre de détecter des attaques sophistiquées, l'ANSSI fournira aux opérateurs des marqueurs d'attaque. Il s'agit d'éléments techniques propres à certains attaquants, tels que l'adresse IP d'un serveur malveillant ou le nom d'un site Internet piégé. L'élaboration de tels éléments constitue une activité propre à l'ANSSI, de très haute technicité, impliquant une part importante des ressources humaines et techniques de son centre opérationnel.

En cas d'attaque informatique associée à l'un de ces marqueurs, les systèmes de détection déployés par les opérateurs produiront une alerte de sécurité, contenant uniquement les informations techniques liées à l'attaque. L'opérateur informera alors l'ANSSI de cette alerte et, si l'attaque détectée concerne un organisme d'importance vitale ou une autorité publique, l'ANSSI pourra demander des informations techniques complémentaires pour caractériser l'attaque et établir des mesures de protection et de remédiation adaptées en lien étroit avec la victime.

Supervision locale et temporaire par l'ANSSI en cas de menace sérieuse



Etape 1 : Un attaquant utilise un serveur d'un hébergeur français pour mener une attaque

Etape 2 : L'ANSSI détecte ou est informée de l'utilisation par un attaquant de ce serveur

Etape 3 : L'ANSSI déploie un dispositif de détection temporaire au plus près du serveur

Etape 4 : L'ANSSI exploite le dispositif et recueille les informations strictement nécessaires à la caractérisation de la menace et à l'identification des victimes

Le second volet du dispositif consiste à autoriser l'ANSSI, lorsqu'elle a connaissance d'une menace grave, à mettre en place un dispositif de détection local sur un serveur d'un hébergeur ou un équipement d'un opérateur de communications électroniques contrôlé par un attaquant. Le système de détection alors déployé produit uniquement des données visant à caractériser l'attaque, telles que les caractéristiques des programmes malveillants utilisés par l'attaquant, les adresses IP de son infrastructure d'attaque ainsi que celles de ses victimes.

Cette technique est au cœur de l'activité opérationnelle de l'ANSSI. Elle permet de comprendre en temps réel les caractéristiques d'une attaque ainsi que d'en identifier les victimes, et donc d'ajuster de façon réactive les mesures de détection, de protection et de remédiation qu'elle met en œuvre.