INSTITUT
MONTAIGNE

Cybermenace : avis de tempête

RAPPORT NOVEMBRE 2018

Think tank indépendant créé en 2000, l'Institut Montaigne est une plateforme de réflexion, de propositions et d'expérimentations consacrée aux politiques publiques en France et en Europe. À travers ses publications et les événements qu'il organise, il souhaite jouer pleinement son rôle d'acteur du débat démocratique avec une approche transpartisane. Ses travaux sont le fruit d'une méthode d'analyse et de recherche rigoureuse et critique, ouverte sur les comparaisons internationales. Association à but non lucratif, l'Institut Montaigne réunit des chefs d'entreprise, des hauts fonctionnaires, des universitaires et des personnalités issues d'horizons divers. Ses financements sont exclusivement privés, aucune contribution n'excédant 1,5 % d'un budget annuel de 4,5 millions d'euros.

Il n'est désir plus naturel
que le désir de connaissance

INSTITUT
MONTAIGNE

Cybermenace : avis de tempête

NOVEMBRE 2018

SOMMAIRE

INTRODUCTION

À l'heure où les systèmes sont de plus en plus interconnectés et les réseaux de plus en plus imbriqués, la transformation numérique est à la fois marqueur de progrès et catalyseur de risques. Si les bénéfices apportés par le numérique ne sont plus à prouver, ces derniers ne seront pérennes qu'à la seule condition que les systèmes soient sécurisés et que les données soient protégées. Le secrétaire d'État au Numérique, Mounir Mahjoubi, le rappelle : la cybersécurité est la condition absolue de la réussite de la numérisation[1].

Les attaques de l'été 2017 (WannaCry et Notpetya) ont eu des conséquences graves pour les acteurs touchés. Malgré les dégâts infligés, elles ont eu l'avantage de marquer les esprits. Elles sont notamment la preuve que le risque d'une attaque large touchant l'ensemble du tissu économique (ce que nous appelons ici un « cyber ouragan ») est réel. Comme nous allons le voir, ce risque systémique ne peut être contré efficacement qu'en encourageant la coopération et la solidarité entre acteurs.

Notre rapport souligne ce besoin vital d'un changement de paradigme. À l'échelle des États, la cybermenace peut être interprétée soit comme un risque pandémique, pouvant toucher l'ensemble des nations de manière égale, soit comme une arme géopolitique, dont le contrôle donnera un avantage considérable. Aujourd'hui, le contexte général de réaffirmation des nations et d'affaiblissement du multilatéralisme tend à renforcer la deuxième interprétation. Toutefois, les attaques de mai et juin 2017 nous rappellent que le risque

[1] « La cybersécurité, condition absolue de la réussite de la numérisation (Mahjoubi) », *L'Express,* 2018.

cyber menace virtuellement tous les acteurs de la communauté internationale, et nécessite donc une réponse globale et coordonnée de la part des États.

Ce changement de paradigme, de la compétition vers la collaboration, doit également s'opérer concrètement et rapidement au niveau national. C'est là l'objet du présent rapport. Le risque d'une cyberattaque majeure touchant l'économie française doit inciter les acteurs publics et privés à collaborer pour mettre en oeuvre des régulations et des initiatives efficaces face au risque cyber. Celles-ci doivent être encouragées avant qu'une attaque de trop grosse ampleur ne touche le pays.

Les propositions de ce rapport insistent sur la solidarité pour augmenter la cyberrésilience du tissu économique français. Trop souvent, une cyberattaque est vécue comme une maladie honteuse. Il faut désormais dépasser cet obstacle pour libérer l'information et enclencher un changement d'état d'esprit : en cas de cyberattaque, au lieu de monter le pont-levis, il devrait être plus aisé de notifier ses clients, chercher de l'aide en dehors des murs de l'entreprise ou encore prévenir ses pairs sur l'attaque en cours pour qu'ils s'en prémunissent…

I

LA CRISE

Ce récit fictif est fondé sur des menaces bien réelles, qui pourraient un jour être à l'origine d'un « cyber ouragan » détruisant une large partie des ressources numériques du pays.

2 février 2022, gare de Paris-Montparnasse, 7 h 10

Gérard, conducteur-mécanicien affecté au Paris-Brest de 7h35, s'installe dans sa cabine et réalise les vérifications précédant chacun de ses départs. La tablette numérique de contrôle démarre, la radio fonctionne. La routine de mise en marche commence.

7 h 30

Gérard adresse la traditionnelle « bienvenue à bord » aux passagers du TGV 8603, lorsque soudain, sa tablette s'arrête. Il vient de perdre sa connexion avec les services centraux de Montparnasse. Dans la solitude de sa cabine, il peste contre le centre logistique qui doit encore réaliser des opérations de maintenance durant ses heures de travail. Après quinze années passées aux commandes des trains qui sillonnent la France, Gérard a l'habitude de faire face à ces situations. Tout en éteignant son microphone, il entame la procédure de redémarrage de l'informatique embarquée. Quelques secondes plus tard, la tablette s'arrête de nouveau. Les données de navigation ne s'afficheront pas ce matin. Gérard sait qu'il lui est impossible de démarrer, car lancé à plus de 300 km/h, conduire à vue serait un pari insensé. Il se décide à lancer l'alerte auprès du chef de gare, et fait descendre les 516 passagers de son

train. Au même moment, les TGV à destination de Bordeaux et La Rochelle subissent le même sort. Le hall de Montparnasse se remplit de passagers qui s'entassent résignés dans le froid parisien.

Une centrale d'achats en périphérie de Paris, 7 h 40

Au sud-est de la capitale, au-delà de sa proche banlieue, trône le célèbre marché de Rungis et sa myriade d'entrepôts qui accueillent chaque jour les produits qui garnissent les supermarchés franciliens. Tous les matins, les employés se pressent sur la zone de chargement dans une chorégraphie bien rodée. Les camions de livraison défilent devant eux, et déversent dans leurs bras les marchandises du jour. Mais aujourd'hui les étalages resteront vides. Une file interminable de fourgons sont arrêtés le long des entrepôts, et leurs chauffeurs, intrigués, descendent peu à peu des véhicules. Au premier étage du bâtiment principal de Rungis, les préparateurs de commandes et les logisticiens s'attroupent devant le bureau du directeur du site. Les ordinateurs permettant de gérer les commandes et l'approvisionnement des magasins parisiens ne répondent plus. L'Île-de-France s'apprête à connaître un jour de jeûne.

8 h 00

La situation se dégrade. Plusieurs chaînes de télévision nationales ont arrêté de transmettre, émettant une image figée en noir et blanc. À Lyon, la ligne du métro automatique s'est brutalement arrêtée, et la foule déboussolée s'amasse sur les quais alors que les premières annonces indiquent un ralentissement généralisé sur toutes les lignes de métro. La France se fige. L'aéroport Charles de Gaulle n'est pas épargné. Les passagers du deuxième aéroport européen se massent sous des panneaux

éteints, et les agents de l'aérogare sont vite dépassés par leurs demandes. Fort heureusement, ni les appareils ni les services de contrôle de la circulation aérienne n'ont été impactés. Dans le même temps, des utilisateurs alertent sur les réseaux sociaux qu'un numéro d'appel d'urgence est injoignable dans certaines régions. L'incident ne semble pas s'être propagé de manière égale sur tout le territoire national. Le préfet de la Préfecture de Police de Paris se coordonne toutefois avec le ministère de l'Intérieur pour se tenir prêt à augmenter la capacité d'intervention des experts cybersécurité de la Police nationale.

8 h 10

Le Premier ministre active la cellule interministérielle de crise, et y convoque le commandant de la Cyberdéfense (COMCYBER) et le Directeur Général de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Les quelques médias encore en capacité d'émettre diffusent des images de la crise, et spéculent sur l'origine de cette situation encore inimaginable il y a quelques minutes. La piste de la cyberattaque semble privilégiée.

9 h 00

La situation reste très critique. Les médias viennent de recevoir la confirmation par des sources proches du dossier que les pannes étaient le fruit d'une attaque « cyber », et qualifient désormais la situation de « cyber ouragan ». Les téléspectateurs hébétés découvrent l'existence de cette menace jusqu'alors inconnue.

Il est 9 h 01, la bourse de Paris dévisse…

Accélération rapide, 3 jours plus tard…

La France est durement impactée par le cyber ouragan. Les derniers bilans dressés par les autorités font état de plus de 15 000 PME touchées, ainsi que 12 grandes entreprises, dont quatre dans des secteurs stratégiques. Trois ministères sont toujours paralysés par les défaillances informatiques, et près de dix millions d'ordinateurs et de serveurs sont bloqués par l'attaque sur le territoire national. Fort heureusement, les services de sécurité, de santé, ainsi que les fournisseurs d'électricité n'ont été que partiellement impactés. Les opérateurs télécoms épargnés par la cyberattaque se veulent rassurant et ouvrent leur réseau aux clients des autres compagnies.

Les investigations ont permis d'identifier un dénominateur commun aux structures touchées. Elles font toutes appel au même fournisseur d'ordinateurs et de serveurs. Une cyberattaque visant ce fournisseur, au cœur d'une guerre économique entre plusieurs grandes puissances, a entraîné la destruction du matériel concerné. L'opération, qui semblait cibler quelques pays, a dérapé et a touché un grand nombre d'États à travers le monde. Elle s'est auto-propagée par Internet et les réseaux d'entreprises en quelques heures. L'origine et la motivation de l'attaquant restent encore à déterminer, mais les médias n'hésitent pas à évoquer la possibilité d'une cyberguerre.

La nature très spécifique de cette cyberattaque impose le remplacement de tous les appareils touchés, même si leurs données restent accessibles. Cependant, le recouvrement des données nécessite une action manuelle longue et coûteuse sur toutes les machines hors d'usage. Face à l'ampleur des conséquences de l'attaque naissent des initiatives de solidarité spontanées. Les équipes informatiques des entreprises encore fonctionnelles viennent prêter main-forte aux autres structures,

et les fournisseurs de matériels informatiques tentent tant bien que mal de leur fournir de nouvelles machines. Les experts estiment qu'une reprise partielle est envisageable dans les deux semaines à venir, mais qu'il faudra certainement plusieurs mois avant de pouvoir rééquiper toutes les structures touchées par l'attaque avec du matériel neuf. En attendant, une partie du tissu économique devra se passer du numérique …

II

L'ÉTAT DE LA MENACE

Ce chapitre présente les motivations des acteurs malveillants et procède à une analyse du contexte géopolitique dans lequel ils opèrent avant d'évaluer la faisabilité technique d'un scénario de « cyber ouragan ». Dans un second temps, les cyberattaques systémiques de ces dernières années seront étudiées afin de mettre en relief les conséquences financières qui en découlent. Enfin, un regard prospectif sera porté pour anticiper la menace de demain.

2.1. Une menace globale en pleine expansion

L'actualité le démontre, les cyberattaques peuvent toucher tous les secteurs d'activité et tous types d'organisations, de la TPE locale aux grands groupes multinationaux. Le second rapport[2] du ministère de l'Intérieur sur « L'état de la menace liée au numérique en 2018 » publié en mai 2018 annonce que « près de 80 % [des entreprises] ont constaté au moins une [cyberattaque] en 2017 ». L'augmentation en intensité et en nombre de ces agressions numériques a entraîné une médiatisation accrue du sujet. C'est durant le printemps 2017 qu'un véritable basculement en magnitude a été opéré avec deux incidents majeurs : WannaCry et NotPetya. Ces cyberattaques ont détruit des milliers de systèmes informatiques et arrêté l'activité de nombreux acteurs industriels à travers le monde[3], entraînant des

[2] Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces, *État de la menace liée au numérique en 2018,* 2018.

[3] Parmi les victimes, de WannaCry et NotPetya, on peut citer les cas du leader mondial des transports maritimes Maersk, Renault et Saint-Gobain en France, le transporteur FedEx (*via* sa filiale TNT Express) ou encore le géant pharmaceutique américain Merck.

impacts financiers de l'ordre de plusieurs milliards d'euros. Ces deux catastrophes cyber, aux impacts sans précédent, ont démontré la fragilité systémique de nos économies vis-à-vis du risque cyber. De plus, il est à noter que de telles attaques ou sabotages peuvent engendrer des impacts potentiellement catastrophiques dans le monde physique avec la numérisation des procédés industriels, voire mettre en péril des vies humaines.

En plus de leur montée en intensité, les cyberattaques recensées à travers le monde ces dernières années montrent le caractère polymorphe de la menace et la multitude des acteurs à son origine :

- Des individus isolés. Ces individus sont généralement poussés par une volonté de nuire à l'organisation ciblée, et alimentés par des motivations qui peuvent être idéologiques ou parfois financières. Ils peuvent être internes à l'organisation (on parle alors de « *rogue employee* »), ou externes.

- Des hacktivistes[4]. Il s'agit de groupes plus ou moins organisés, motivés par des motifs idéologiques et qui agissent dans le but de dégrader l'image de marque ou la réputation des structures ciblées, notamment en perturbant la gouvernance de l'organisation.

- Des groupes mafieux organisés, attirés principalement par le gain financier. En effet, le cybercrime est profitable : à titre d'illustration, certains revendeurs de rançongiciels peuvent gagner jusqu'à 100 000 dollars par an[5]. L'avènement de ce type de menace mafieuse est caractéristique d'un phénomène d'effritement de la

[4] Mot-valise provenant de la contraction de *hacker* et activiste.

[5] Carbon Black, *The Ransomware Economy,* 2017.

frontière entre criminalité traditionnelle et cybercriminalité. Le rapport 2016 « *Internet Organized Crime Threat Assessment* »[6] d'Europol indique que pour la première fois dans certains pays européens, le cybercrime a surpassé le crime traditionnel en nombre d'incidents reportés. Et la *National Crime Agency* britannique de préciser dans son rapport 2016 « *Cyber crime assessment* »[7] que la part de crimes liés au numérique a représenté 53% du nombre total d'incidents reportés en 2015 au Royaume-Uni.

- Des groupes menaçants liés aux États. Mercenaires ou groupes liés aux services de renseignements étatiques, ces groupes d'attaquants s'inscrivent dans des logiques de sabotage, d'espionnage ou de déstabilisation des États. Les attaques perpétrées par ce type d'organisation peuvent être hautement ciblées et discrètes, mais aussi parfois ostentatoires et destructives. Il a été observé, par exemple, que des acteurs étatiques ont mené des campagnes de cyberattaques visant à déstabiliser les campagnes présidentielles américaines en 2016[8] et françaises en 2017[9]. En février 2016, d'autres motivations entrent en jeu : une cyberattaque visant le réseau interbancaire SWIFT a permis de dérober 81 milliards de dollars à la *Bank of Bangladesh via* le compte qu'elle détenait auprès de la *Federal Reserve Bank of New York.* Cette attaque ciblée et sophistiquée, potentiellement perpétrée avec des complices à l'intérieur de la *Bank of Bangladesh,* a été particulièrement discrète et n'a éveillé les soupçons qu'à la suite d'une faute d'orthographe[10]. Les autorités

[6] Europol, *Internet Organised Crime Threat Assesment (IOCTA) 2016,* 2016.

[7] NCA Strategic Cyber Industry Group, *Cyber Crime Assessment 2016,* 2016.

[8] « 2016 Presidential Campaign Hacking Fast Facts », *CNN,* 2018.

[9] « Cyberattaques contre l'équipe Macron : le point sur la situation », *Challenges,* 2017.

[10] Les attaquants avaient mal orthographié le mot anglais « *foundation* » en écrivant « fandation », ce qui a poussé la *Deutsche Bank,* en tant qu'intermédiaire du virement, à enquêter auprès de la banque émettrice qui ignorait la nature de ce virement.

américaines investiguent sur des liens potentiels avec la Corée du Nord et le groupe Lazarus[11].

- En filigrane de ce triptyque d'acteurs, il existe aussi une économie grise, plus ou moins souterraine, de développement d'outils d'attaque et de recherche de vulnérabilités qui alimentent ces groupes menaçants. La revue stratégique de cyberdéfense de février 2018[12] attire ainsi l'attention sur les failles dites « *zero-day* », des failles inconnues de l'éditeur du produit et donc au potentiel nuisible redoutable, qui se monnaient sur des plateformes plus ou moins licites et constituent un véritable marché des failles de sécurité. La revue va plus loin en observant une « ubérisation » de ce marché, avec des plateformes de spécialistes de la revente de failles critiques qui dégagent des profits d'ampleur.

Les frontières sont très poreuses entre ces acteurs. On peut parfois constater des hybridations entre les groupes[13], voire des cas où les groupes s'aident involontairement en ouvrant la voie pour les suivants[14]. Une vision simplifiée de cette analyse pourrait se présenter sous la forme d'une dualité : une menace non ciblée, diffuse et courante, pouvant toucher tout un chacun, et une menace sophistiquée, touchant des structures hautement ciblées.

---

[11] « U.S. preparing cases linking North Korea to theft at N.Y. Fed », *The Wall Street Journal,* 2017.

[12] Secrétariat général de la défense et de la sécurité nationale (SGDSN), *Revue stratégique de cyberdéfense,* 2018.

[13] « Feds charge 9 with $30M insider trading, hacking scheme », *Bank Info Security,* 2015.

[14] A titre d'illustration, la cyberattaque WannaCry attribuée au groupe Lazarus (soupçonné d'entretenir des liens avec la Corée du Nord) a tiré parti d'une faille dite « *zero-day* » dérobée à la NSA américaine par le groupe *The Shadow Brokers*. Cette faille a aussi été exploitée dans le cas NotPetya.

De plus, il règne un véritable sentiment de facilité et d'impunité dans l'économie souterraine du cyberespace, entretenu par la difficulté d'identification des cybercriminels par les forces de l'ordre. Ce sentiment est également renforcé par le niveau de sécurité insuffisant des organisations. À cet égard, la revue stratégique de cyberdéfense écrit : « l'accroissement du niveau général de la menace n'est que faiblement compensé aujourd'hui par l'amélioration du niveau de sécurité des systèmes ». De plus l'absence d'attribution légale avant 2014, avec le cas emblématique du piratage de *Sony Pictures Entertainment* attribué par les États-Unis à la Corée du Nord, a participé à accroître ce sentiment d'impunité.

Une lutte contre la cybercriminalité qui s'organise

Face à l'impunité des cybercriminels, la réponse pénale s'organise doucement. Des cas médiatiques de démantèlements de réseaux cybercriminels en démontrent l'efficacité. Mais il est à noter que ces actions ont demandé des efforts importants et coordonnés. Quelques cas notables récents :

- Le démantèlement de deux des plus larges places de marché noir du *dark web, Alphabay* et *Hansa*, spécialisées dans la vente de produits stupéfiants. L'opération a été menée par Europol et les autorités américaines (FBI, DEA) et néerlandaises *(Dutch National Police)* en juillet 2017[15].

[15] « Massive blow to criminal dark web activities after globally coordinated operation », Europol, 2017.

- Le 26 mars 2018, Europol annonce l'arrêt du cerveau présumé du gang de cybercriminels *Anunak/Carbanak*[16], spécialisé dans le « cyber-braquage » de banques. Depuis 2013, le groupe serait à l'origine du vol de plus d'un milliard d'euros et s'est notamment démarqué en piratant les distributeurs automatiques de billets (DAB). Le démantèlement du réseau de cybercriminels fut l'objet d'une enquête complexe et le fruit d'une coopération transfrontalière entre notamment l'EC3 *(Europol's European Cybercrime Center)*, l'EBF *(European Banking Federation),* la police nationale espagnole, le FBI, les autorités roumaines, biélorusses, taïwanaises…

- En juin 2018, c'est la douane française, à travers la DNRED, qui a permis le démantèlement d'une des plus importantes places de marché noir du *dark web* français, le forum *Black Hand*[17]*.*

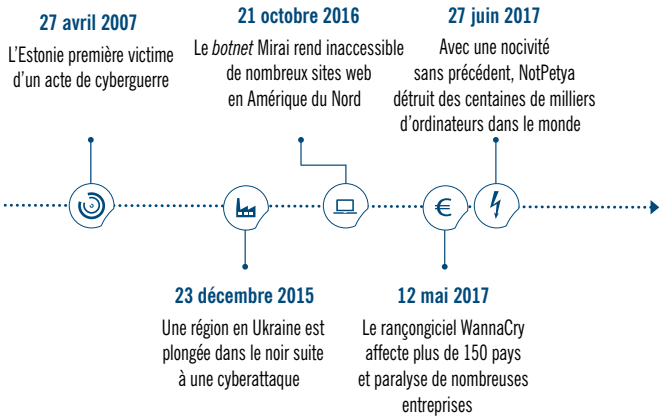
[16] « Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain », Europol, 2018.

[17] « Démantèlement du forum "Black Hand" par la DNRED », Douane.gouv.fr, 2018.

2.2 Une histoire marquée par des cyberattaques aux effets systémiques

Un « cyber ouragan » reposerait sur une attaque large touchant de multiples acteurs. Loin d'être une pure invention de l'esprit, ce type d'attaques a déjà eu lieu comme nous le détaillons dans une liste non-exhaustive ci-dessous.

Figure 1 – Quelques exemples marquants



27 avril 2007, l'Estonie première victime d'un acte de cyberguerre

L'Estonie a été victime de cyberattaques massives orchestrées selon elle par la Russie. Des attaques par déni de service distribué (DDoS) ont paralysé des activités essentielles du pays pendant plus d'une

quinzaine de jours[18] : des banques, des ministères ou encore des sites de médias se sont vu bombardés de requêtes provenant de *botnets* situés dans plus de 60 pays, c'est-à-dire des machines compromises et à la main des attaquants, ce qui a rendu les sites inaccessibles. Des numéros d'urgence ont même été rendus indisponibles pendant de courtes périodes. La paralysie du pays était d'autant plus grave que l'Estonie était alors l'un des pays pionniers de la transformation digitale de la société et des services publics : en 2007 déjà, plus de 80 % des déclarations fiscales y étaient réalisées par Internet[19].

23 décembre 2015, près de 230 000 habitants sont plongés dans le noir dans l'ouest de l'Ukraine pendant plusieurs heures

Un logiciel malveillant introduit chez le fournisseur d'électricité ukrainien *via* un fichier Excel piégé a permis de donner aux attaquants accès au système industriel et de prendre le contrôle des systèmes de contrôle et d'acquisition des données (SCADA). Une fois le SCADA compromis, les attaquants ont désactivé 30 postes électriques à distance conduisant ainsi à la coupure d'électricité de la moitié des foyers de la région d'Ivano-Frankivsk durant plus de trois heures.

21 octobre 2016, un grand nombre d'utilisateurs en Amérique du Nord ne peuvent plus se connecter à des services comme Twitter, Paypal, Spotify, Netflix…

En 2016, il s'agissait alors de la plus grosse attaque par déni de service distribué (DDoS) jamais enregistrée (avant l'arrivée de *IoTroop/*

[18] « L'Estonie tire les leçons des cyberattaques massives lancées contre elle pendant la crise avec la Russie », *Le Monde,* 2007.

[19] « Les cyberattaques massives d'origine russe contre l'Estonie préoccupent l'Alliance atlantique », *Le Monde,* 2007.

Reaper en 2017) : des dizaines de millions d'adresses IP utilisées pour générer plus d'un téraoctet de données par seconde. L'attaque a été dirigée vers l'entreprise américaine Dyn, hébergeur DNS qui opère des infrastructures Internet, rendant ainsi impossible la connexion vers des sites Internet populaires comme Twitter, SoundCloud ou encore Reddit pendant plus de dix heures. L'attaque a été rendue possible par le *botnet* Mirai, un réseau composé de plusieurs centaines de milliers d'objets connectés vulnérables, dont un grand nombre de caméras connectées non protégées.

12 mai 2017, de nombreuses entreprises se retrouvent paralysées à la suite d'une attaque par rançongiciel affectant plus de 150 pays

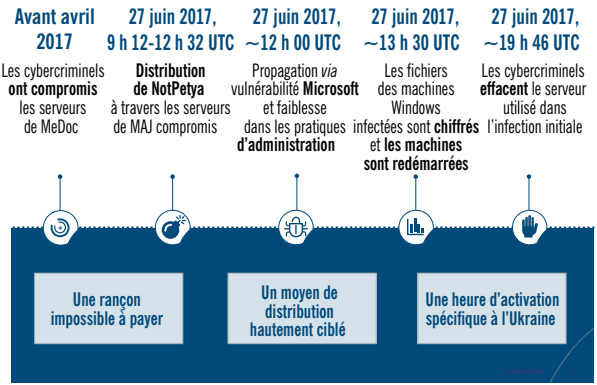
C'est plusieurs centaines de milliers de postes de travail qui ont été victimes du rançongiciel WannaCry : les postes de travail sont rendus inopérants et tenus en otage jusqu'à paiement d'une rançon. Le ver informatique s'est propagé de façon indiscriminée en quelques heures uniquement, et a causé des pannes et dysfonctionnements majeures sur le système national de santé britannique (NHS), chez Renault en France ou encore Vodafone, FedEx ou Telefónica. Comment cela a-t-il été rendu possible ? Le 14 avril 2017, le groupe cybercriminel « *The Shadow Brokers* » a publié un outil d'attaque basé sur la faille de Windows MS17-010 dérobée à la NSA américaine. Bien que Microsoft ait publié un correctif en mars de la même année, cela n'a pas empêché le groupe Lazarus (qui entretient des liens avec la Corée du Nord) d'exploiter la vulnérabilité avec succès au sein des entreprises qui n'ont pas déployé le correctif. Cependant, un coup de chance a permis de mettre un terme à l'attaque : un chercheur britannique a découvert l'existence d'un « mécanisme d'arrêt d'urgence », ou « *killswitch* » dans le logiciel malveillant qui a permis de bloquer la propagation rapidement.

27 juin 2017, une attaque fulgurante avec une nocivité sans précédent détruit plusieurs centaines de milliers d'ordinateurs à travers le monde

En moins d'une heure, la cyberattaque NotPetya a détruit les postes de travail de ses victimes incluant Saint-Gobain en France, le plus grand armateur Maersk, le géant pharmaceutique Merck, FedEx… L'épicentre de l'attaque s'est situé en Ukraine, représentant près de 80% des infections. En Ukraine, l'attaque a paralysé un très grand nombre d'activités essentielles liées aux secteurs financiers, du transport, de l'énergie, des médias ou encore des grandes administrations. Les dégâts seront estimés à plus de dix milliards de dollars à travers le monde[20]. Certaines entreprises ont mis plus d'un mois avant de rétablir un fonctionnement normal, tandis que d'autres ont annoncé avoir perdu des données de façon définitive. A l'origine de l'attaque ? Une petite entreprise éditant un logiciel de comptabilité ukrainien. Après avoir compromis cette société, les attaquants ont exploité la procédure de mise à jour du logiciel pour introduire le logiciel malveillant au sein des entreprises ciblées, puis la propagation au sein de ces entreprises a exploité la même faille (MS17-010) utilisée par WannaCry quelques semaines auparavant, ainsi que des faiblesses sur la gestion des mots de passe d'administration du système d'information (SI).

[20] « The untold story of Notpetya, the most devastating cyberattack in history », *Wired,* 2018.

Figure 2 – Chronologie de la cyberattaque NotPetya



Source : *Wavestone*

2.3. Un « cyber ouragan » possible en France et en Europe

L'écrit de fiction présenté en première partie dépeint un scénario catastrophe aux effets systémiques et paralysants. Ce type de scénario est-il envisageable en France et en Europe ? Cette question en amène deux autres :

- Est-ce techniquement réalisable ?

- Qui aurait intérêt à réaliser une telle attaque ?

2.3.1. Un scénario systémique techniquement réaliste appuyé par une dépendance technologique forte associée à une interconnexion croissante

Une exposition systémique forte

Le fonctionnement de toutes les sociétés repose aujourd'hui sur le numérique. Ce marché est dominé par un nombre très limité d'acteurs :

- Les systèmes d'exploitation Windows occupent 83 % du marché des systèmes d'exploitation sur les postes de travail[21].

- Les microprocesseurs Intel représentent près de 79 % des microprocesseurs d'architecture x86 en circulation dans le monde[22].

Ceci crée une fragilité systémique. Une cyberattaque ciblant l'application de mise à jour des systèmes d'exploitation Windows pourrait par exemple avoir des impacts catastrophiques. De plus, la plupart de ces systèmes ont été conçus sans intégrer la cybersécurité par défaut et des failles sont régulièrement découvertes. Sans mentionner le fait qu'il est aujourd'hui encore difficile pour les entreprises de suivre la cadence des mises à jour de tous leurs éditeurs et fournisseurs.

Un grand nombre de technologies critiques qui constituent la colonne vertébrale d'Internet et le cœur du monde numérique sont vulnérables car elles ont été développées à un moment de l'histoire où les enjeux de cybersécurité étaient moindres. Des failles connues dans les proto-

[21] Statista, *Global operating systems market share for desktop PCs, from January 2013 to July 2018,* 2018.

[22] Statista, *Distribution of AMD and Intel x86 computer processors worldwide, from 2012 to 2018, by quarter,* 2018.

coles BGP ou DNS présentent un fort potentiel d'interruption de services. Ces protocoles assurent le bon fonctionnement d'Internet : le premier pose les fondements permettant aux systèmes de trouver et partager les chemins pour établir des communications ; le second permet de traduire les noms de domaine, simples à manipuler par l'humain, en adresses IP, faciles à traiter par les machines. À titre d'exemple, un incident sur ces systèmes peut amener un pays entier à être isolé d'Internet, comme ce fut le cas au Japon en 2017[23]. Des attaques sur les autorités de certification d'Internet, qui permettent de s'assurer que le site Internet visité est véritablement celui qu'il prétend être, peuvent avoir des conséquences dramatiques sur la confidentialité des échanges, mais ce scénario revêt aussi un potentiel important de pannes et de dysfonctionnements. Des cas emblématiques de ce type d'attaques ont eu lieu en 2011, comme Comodo et DigiNotar[24]. La situation s'améliore, car il existe des solutions techniques pour se prémunir contre les sites présentant un certificat frauduleux, mais qui restent toutefois complexes à mettre en œuvre de manière étendue.

Une interconnexion croissante entre les systèmes

Les entreprises et les administrations se décloisonnent et s'ouvrent davantage vers l'extérieur. Au-delà du cadre de l'entreprise, les objets connectés font de plus en plus partie de notre quotidien et s'invitent dans nos maisons : capteurs domotiques, smartphones et autres caméras connectées… Les technologies investissent les usages métiers : en 2017, le nombre d'objets connectés dans le monde est estimé à plus de dix milliards et les prédictions pour 2020 des différents instituts de recherche placent le chiffre entre 26 milliards

[23] « Google routing blunder sent Japan's Internet dark on Friday », *The Register,* 2017.

[24] « Another fraudulent certificate raises the same old questions about certificate authorities », *Ars Technica,* 2011.

et 212 milliards d'objets connectés à travers le monde (Gartner, ABIresearch, Cisco, Idate, IDC). Cette dynamique exacerbe le risque systémique en augmentant les effets de propagation en cas de cyberattaques destructives.

Par ailleurs, l'adoption grandissante du *cloud* public par les entreprises participe aussi au risque systémique, car les infrastructures *cloud* sont opérées en grande majorité par Microsoft, Google et Amazon. Un rapport du Gartner[25] estime que les revenus des acteurs du *cloud* public vont augmenter de 21,4 % en 2018. Parmi les acteurs du *cloud* public, *Amazon Web Services* reste en tête avec 33 % de parts de marché, *Microsoft Azure* tente de réduire l'écart avec 13 % de parts et *Google Cloud Platform* ne couvre que 6 % du marché[26]. Ces trois acteurs représentent à eux seuls plus de la moitié du marché des services d'infrastructures *cloud*.

La possibilité de viser spécifiquement les systèmes cibles

Il est techniquement possible de cibler une attaque sur une zone géographique ou une organisation particulière.

- En ciblant les ordinateurs avec un clavier français. Cela ouvre la possibilité de cibler un pays uniquement. Par exemple, il a déjà été observé des cas de logiciels malveillants conçus pour éviter d'infecter des ordinateurs ukrainiens[27] ou des cas de rançongiciels offrant un déchiffrement gratuit pour les victimes russes[28].

[25] « Gartner forecasts worldwide public cloud revenue to grow 21.4 percent in 2018 », *Gartner,* 2018.

[26] « Microsoft narrows Amazon's lead in cloud, but the gap remains large », *CNBC,* 2018.

[27] « Malware trying to avoid some countries », *WeLiveSecurity,* 2009.

[28] « Sigrun ransomware author decrypting Russian victims for free », *Bleeping Computer,* 2018.

- En visant des logiciels métiers spécifiques. Ce fut notamment le cas lors de l'attaque NotPetya, où les attaquants ont ciblé un logiciel de comptabilité ukrainien, nommé « MeDoc », pour se propager au sein des entreprises ukrainiennes.

- En dirigeant l'attaque vers des adresses IP correspondant à une zone géographique ou à une entreprise spécifique.

Toutefois, le ciblage ne peut être fiable à 100 %, car peu efficace d'une part (des utilisateurs utilisant un clavier anglais peuvent se trouver en France ou en Russie, les adresses IP peuvent aussi être dynamiques et ne pas être représentatives d'une zone géographique…) et d'autre part la propagation peut déraper et passer hors du contrôle de l'attaquant, comme ce fut le cas pour NotPetya.

Une initiative pour limiter les risques

Fondé par deux *think tanks* indépendants, le *Hague Center for Strategic Studies* et le *East West Institute,* le *Global Commission on the Stability of Cyberspace* (GCSC) est constitué de membres représentant un panel large de régions géographiques et issus de tous secteurs d'activité. La commission œuvre à établir le dialogue entre les différentes communautés du cyberespace sur les questions de cybersécurité à l'échelle internationale. Le GCSC appuie les réglementations et normes permettant d'assurer la sécurité et la stabilité du cyberespace.

Le GCSC a lancé en novembre 2017 un appel à protéger le cœur public d'Internet[29]. Cette norme appelle tous les acteurs à ne pas

[29] Global Commission on the stability of cyberspace, *Call to protect the public core of the Internet,* 2017.

soutenir ou permettre des actions qui menacent le fonctionnement global de l'Internet (DNS, routage…). Cette norme inclut une notion d'intention : même sans l'intention d'impacter le cœur d'Internet, la résultante reste répréhensible et il s'agit d'une action préjudiciable. Cette norme doit aboutir à des résolutions dans le but d'éviter les attaques paralysantes à grande échelle. Ce groupe devrait aussi travailler à une norme sur ce qui relève des actions offensives par les acteurs privés pour clarifier leurs responsabilités. Le but est d'empêcher que les outils d'attaque ne soient utilisés par des personnes non légitimes et dans un cadre malveillant.

2.3.2. Des acteurs menaçants en mesure de déclencher un « cyber ouragan »

La pensée commune porte à croire que des attaques destructives et systémiques pourraient être lancées par la Russie, la Corée du Nord, l'Iran, la Chine ou encore les États-Unis. Il s'agit en effet des États qui ont démontré leurs capacités offensives en matière cyber et qui ont attribué ou se sont vu attribuer des cyberattaques.

Toutefois, ces États, médiatiquement connus pour être actifs offensivement, n'ont potentiellement que très peu d'intérêts à réaliser des attaques d'ampleur qui pourraient paralyser un pays tout entier comme la France ou un autre pays européen. Il est peu probable qu'une telle attaque au potentiel destructeur soit expressément commanditée par un État, et ce pour plusieurs raisons :

- Il existe aujourd'hui un fort degré d'interdépendance économique

entre les États. Par exemple, dans le cas des relations sino-américaines, certains officiels américains déclarent régulièrement que la Chine pose une menace pour la sécurité nationale des États-Unis, alors que l'import-export entre les deux pays est très développé (sans mentionner que la Chine détient une majorité de la dette américaine).

- Une attaque systémique avec un large spectre d'action pourrait avoir des conséquences lourdes en termes de représailles.

- Une telle attaque pourrait avoir des conséquences jusque sur le territoire national de l'État commanditaire, comme l'a montré le cas de NotPetya, attribué de façon semi-collective[30] par les membres du *Five Eyes* à la Russie, mais ayant paralysé également des entreprises russes.

Dans le contexte géopolitique actuel, peu de pays pourraient être qualifiés d'acteur menaçant dans le scénario d'un « cyber ouragan ». Le seul facteur de variation constituant un risque dans ce scénario est l'isolation d'un pays, combinée à une économie faible. L'addition de ces deux facteurs limite les impacts de répercussions négatives en représailles.

Il est nécessaire de préciser ici qu'il s'agit d'une interprétation du contexte géopolitique actuel qui peut être amené à changer avec le temps. De plus, il faut noter que, dans l'espace numérique, il est difficile de garantir avec une certitude absolue qu'un système est dépourvu de toute compromission. Ainsi, il peut exister une incertitude concernant une éventuelle compromission silencieuse

[30] Les membres du *Five Eyes* ont tous attribué l'attaque à la Russie dans la même fenêtre de temps de manière individuelle sans apparente concertation.

voire dormante des systèmes en vue d'un acte de cyberguerre éventuelle dans le futur. Cela souligne une double temporalité de la cybermenace : d'une part un temps court dans lequel évoluent les cybercriminels et d'autre part un temps long dans lequel les États inscrivent leurs initiatives de cyberdéfense ou de cyberguerre.

Le scénario le plus probable est donc celui d'une cyberattaque où les attaquants sont dans l'incapacité de circonscrire la portée et les effets de leurs attaques, dans le temps et dans l'espace. Il pourrait correspondre à :

- Une opération étatique dont la portée et les effets échapperaient aux attaquants avec des conséquences imprévisibles.

- Une attaque provenant d'un acteur non étatique qui aurait dérobé directement ou indirectement des outils d'attaques, avec des dégâts collatéraux non intentionnels et non prévus ou avec une volonté idéologique de destruction.

Alors que chaque État développe son arsenal numérique, une prise de conscience des États sur leur responsabilité semble nécessaire. Si un parallèle est tiré avec le domaine militaire traditionnel, quelles seraient les conséquences de voir un missile Tomahawk américain entre les mains d'acteurs menaçants[31] ? Les outils d'attaque les plus sophistiqués et les plus dangereux sont développés par les États, alors même qu'il existe un risque d'« effet boomerang ». Du fait de la nature dématérialisée du domaine cyber, une fois utilisés, ces outils peuvent être récupérés et exploités par des acteurs malveillants. En effet, contrairement aux armes conventionnelles, les outils d'attaque dans le cyberespace ne

[31] « Russia claims it has a US Tomahawk cruise missile and will use it to improve its own weapons », *CNBC,* 2018.

sont pas automatiquement détruits après utilisation. Les États à l'origine de l'outil peuvent ainsi se retrouver sous les feux de leur propre arme.

Pour conclure, plus qu'un acte volontaire et conscient de cyberattaque systémique d'un État envers un autre État, le scénario de vol ou de perte d'un outil d'attaque étatique et une utilisation par un tiers malveillant semble plus vraisemblable.

Une perspective inquiétante mais qui n'a pas encore émergé : un cyberterrorisme disruptant les systèmes

Aujourd'hui, les groupes terroristes font usage du numérique majoritairement à des fins de planification, de propagande et de recrutement. Une évolution vers des actions offensives est-elle possible ? Un certain nombre d'experts ont tiré la sonnette d'alarme sur la possibilité d'un « cyber-11-septembre », mais il n'y a aujourd'hui eu aucun cas connu de disruption majeure de l'espace numérique provoquée par des groupes terroristes.

Toutefois, la montée en compétences de ces organisations est possible avec les ressources et les outils rendus disponibles sur la toile[32]. Et si les groupes terroristes ne semblent pas disposer aujourd'hui de telles capacités, la crainte réside dans le fait que les compétences existent chez des mercenaires ou autres intermédiaires, comme le précise Guillaume Poupard, directeur général de l'Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI[33].

[32] Les outils d'attaque sont aujourd'hui disponibles sur les places de marché noir, véritable économie souterraine (voir Lillian Ablon, Martin C. Libicki, Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar,* 2014).

[33] « Cyberattentats : la menace djihadiste grandit », *Ouest France,* 2017.

Cette utilisation de cyberattaques à des fins terroristes n'est pas considérée par les États comme la menace cyber la plus probable comme l'a avancé le général Michael Hayden, l'ex-directeur de la NSA et de la CIA américaine[34], en 2014. Il est nécessaire de noter que ces considérations peuvent changer avec le temps.

2.4. Des attaques aux impacts financiers potentiellement accablants pour nos économies

Aujourd'hui, il existe peu d'exemples concrets montrant les impacts réels d'un « cyber ouragan ». Le cas emblématique qui s'en approche le plus est NotPetya. La Maison-Blanche affirme que les dégâts causés par le rançongiciel à travers le monde dépassent les dix milliards de dollars, et une étude Wavestone[35] montre que le temps de remédiation par les victimes a dépassé les 80 jours pour certaines organisations.

Le spécialiste de l'assurance britannique, *Lloyd's of London,* a publié un rapport en juillet 2017 intitulé « *Counting the Cost: Cyber exposure decoded* »[36]. Le rapport quantifie les impacts financiers potentiels de deux scénarios :

- Une cyberattaque ciblant un fournisseur de services *cloud* qui conduit à une interruption de service.

[34] « Cyberespionage, not cyber terror, is the major threat, former NSA Director says », *Threatpost,* 2014.

[35] Wavestone, *Notpetya : 5 mois après, quels sont les impacts,* Wavestone, 2017.

[36] Lloyd's, *Counting the cost – cyber exposure decoded,* 2017.

- Une cyberattaque exploitant une vulnérabilité dans un système largement utilisé dans le monde.

Selon l'étude de Lloyd's, le premier scénario pourrait induire des pertes allant de 4,6 milliards de dollars à 53,1 milliards de dollars. Le second scénario pourrait engendrer des pertes allant de 9,7 milliards de dollars à 28,7 milliards de dollars. Le *City Risk Index* de Lloyd's estime le coût potentiel d'une cyberattaque ciblant la ville de Paris à hauteur de 1,1 milliard de dollars[37]. En comparaison, le risque d'inondation à Paris est estimé à 1,16 milliard de dollars.

[37] Lloyd's, *Lloyd's city risk index – Europe,* 2018.

Figure 3 - Impact potentiel d'un scénario de cyberattaque ciblant un fournisseur de services *cloud*[38]

Secteur	% des entreprises étudiées (incluant celles qui ne sont pas assurées)	Pertes (en Md$)	
		Perte importante	Perte considérable
Services financiers	10 %	1,2	16,72
Services tech et software	4 %	0,214	1,79
Hôtellerie/ Commerce de détail	11 %	0,332	3,08
Santé	3 %	0,06	0,853
Autres	72 %	2,7	30,6
Toutes les industries	100 %	4,6*	53,05**
Durée		12 – 18 heures	2,5 - 3 jours

Source : https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost (p. 29).

* Intervalle de confiance 95 % : (1,60 - 10,85).

** Intervalle de confiance 95 % : (15,62 – 121,41).

[38] Les pertes figurant dans ce tableau sont dues à une baisse d'exploitation éventuelle qui entraînerait des pertes de revenus ainsi que des dépenses supplémentaires. Les industries mises en évidence dans le rapport comprennent les services financiers, les logiciels et les services techniques, l'hôtellerie et le commerce de détail, et les soins de santé. Elles représentent les principaux secteurs qui investissent dans des cyberassurances. Les pertes globales ont été calculées de manière à représenter l'ensemble des coûts économiques de l'incident pour l'économie en général et, à ce titre, comprennent tous les secteurs de la sécurité.

Des intervalles de confiance ont également été inclus dans la catégorie des pertes « toutes industries » afin de donner une idée de la variabilité de la perte projetée compte tenu du niveau des données disponibles sur le risque.

Figure 4 - Impact potentiel d'un scénario de cyberattaque exploitant en masse une vulnérabilité largement répandue[39]

		Pertes (en Md$)	
Secteur	% de la population	Perte importante	Perte considérable
Services financiers	10 %	2,41	7,37
Services tech et software	4 %	0,311	0,784
Hôtellerie/ Commerce de détail	11 %	1,19	2,93
Santé	3 %	0,615	1,75
Autres	72 %	5,15	15,89
Toutes les industries	100 %	9,68*	28,72**

Source : https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost (p. 40).

* Intervalle de confiance 95 % : (4,12 – 15,63).
** Intervalle de confiance 95 % : (20,50 – 34,22)

Si ces chiffres s'inscrivent dans un intervalle très large dû à l'incertitude de certains facteurs comme le temps d'interruption des services, ils permettent d'introduire un premier ordre de grandeur quant aux impacts financiers potentiels.

En juin 2018, une étude du Fonds Monétaire International (FMI) a évalué l'impact financier potentiel des cyberattaques sur le secteur financier[40]. L'étude indique que les pertes potentielles des institutions financières victimes de cyberattaques peuvent aller de 9 % du bénéfice net mondial des banques, soit environ 100 milliards de dollars, jusqu'à

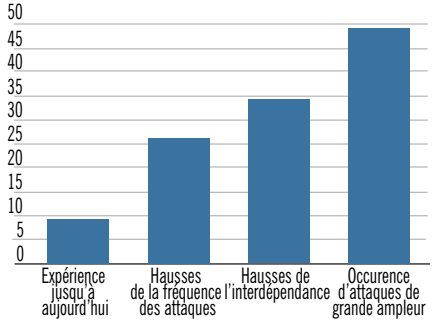
[39] Les pertes couvrent les entreprises des États-Unis, du Canada, du Royaume-Uni et de l'Union européenne avec un chiffre d'affaires annuel supérieur à 20 millions de dollars.

[40] Fonds monétaire international, *Estimer le cyberrisque pour le secteur financier,* 2018.

représenter près de 50 % du bénéfice net mondial, soit plus de 555 milliards de dollars, dans le cas d'un scénario extrême d'attaques destructives massives qui pourraient mettre en péril l'ensemble du secteur financier. Cette même étude observe aussi que les pertes estimées sont « de plusieurs ordres de grandeur supérieures à la taille du marché actuel de la cyberassurance ». Le marché de la cyberassurance est aujourd'hui certes en croissance, mais la couverture globale du marché n'est pas suffisante : l'existence d'un risque systémique pousse les assureurs et réassureurs à se protéger contre le risque d'accumulation, à défaut de pouvoir évaluer finement l'exposition des entreprises au risque cyber.

Figure 5 - Impact potentiel des cyberattaques sur les bénéfices des banques (en pourcentage du bénéfice net)

À l'échelle mondiale, les cyberattaques pourraient faire subir aux institutions financières des pertes allant de 9 % de leur bénéfice net (sur la base de l'expérience jusqu'ici) à la moitié de leurs bénéfices dans le pire scénario.



Source : https://www.imf.org/external/french/np/blog/2018/062218f.htm

L'étude des impacts financiers d'une cyberattaque est un exercice difficile, car il faut prendre en compte une multitude de facteurs variables et parfois non mesurables :

- Des coûts directs : pertes opérationnelles pour investiguer l'attaque et reconstruire les systèmes, le coût de notification des clients impactés le cas échéant, le coût pour gérer les litiges et autres obligations légales, le coût des amendes potentielles, le coût pour gérer les relations publiques…

- Des coûts indirects : pertes de chiffre d'affaires dues à l'interruption des services ou à la perte de confiance des clients, pertes potentielles d'avantages concurrentiels en cas de fuite de données stratégiques, des primes d'assurance qui peuvent augmenter à la suite d'un sinistre, pertes d'image de marque…

À cela s'ajoutent aussi l'absence manifeste de données sur le nombre d'incidents de sécurité et la difficulté à évaluer le risque cyber, qui participent à rendre l'analyse difficile.

Les différentes études présentées plus haut montrent qu'il n'y a aujourd'hui pas de consensus entre les acteurs quant au montant des impacts financiers potentiels d'une cyberattaque. Ce rapport ne s'est pas prêté à cet exercice difficile, mais l'Institut Montaigne appelle de ses vœux qu'une étude soit réalisée par les autorités compétentes. En effet, compte tenu du fait que certains organes de l'État collectent désormais des données sur les incidents de sécurité et que le cadre réglementaire (RGPD) évolue pour imposer des obligations de notification d'incidents, les autorités vont petit à petit disposer de données plus granulaires permettant de préciser et de perfectionner l'analyse.

2.5. Une évolution de la menace qui nécessite d'être anticipée

De l'intelligence artificielle...

Il est certain que la menace va évoluer en s'amplifiant, si bien que la revue stratégique de cyberdéfense parle d'évolution vers un « Far-West cybernétique » si les enjeux de cybersécurité ne sont pas pris en compte efficacement. Cette perspective a notamment poussé l'université de Californie à Berkeley à créer en 2015 le *Center for Long-Term cybersecurity*[41], un hub de recherche menant des travaux prospectifs pour anticiper les concepts futurs de cybersécurité et les impacts potentiels sur l'humain, les machines et la société en général.

Il existe notamment une crainte forte de voir se développer des attaques automatisées grâce aux avancées de l'intelligence artificielle (IA). La possibilité de perte de contrôle en termes de portée, de vitesse de propagation et de nocivité par les concepteurs laisse craindre des scénarios catastrophes d'ampleur. Ce scénario où un État expérimente de nouvelles technologies d'IA pour mener des attaques intelligentes qui s'auto-développent présente un terreau propice à la genèse d'une attaque systémique non-intentionnelle à très large échelle dont les conséquences ne peuvent être prévues. Par ailleurs, comme exploré par la suite dans ce rapport, le lien entre la cybersécurité et l'IA est double. Si l'IA représente d'une part une source de menace inquiétante par sa vélocité et la possibilité d'être exploitée par des groupes malveillants, elle incarne aussi une opportunité formidable pour sécuriser les systèmes, prévenir les intrusions et réagir plus rapidement.

[41] Voir le site du Center for Long-Term Cybersecurity à l'adresse suivante : https://cltc.berkeley.edu/

… À des attaques destructives aux impacts dans le monde physique

Depuis la fin de l'année 2017, on peut observer des premiers signes d'un basculement d'une cybercriminalité motivée par l'appât du gain vers des attaques volontairement destructives, avec des impacts dans le monde physique et des dommages potentiellement humains. L'étude du cas NotPetya montre que les attaquants n'étaient pas motivés par le gain financier et l'émergence du groupe d'attaquants XENOTIME fin 2017 fait apparaître une perspective alarmante[42]. En effet, ce groupe d'acteurs se spécialise dans des cyberattaques visant les systèmes instrumentés de sûreté (SIS), c'est-à-dire les systèmes qui contrôlent les procédés industriels pour les empêcher de rentrer dans des états dangereux pour les personnes, l'environnement et les biens. Compromettre ces systèmes peut donc mener à des situations extrêmement dangereuses impliquant la perte de vies humaines ou des dommages environnementaux irréversibles.

L'ombre de cette menace est particulièrement grande si on considère le développement des nouveaux usages numériques qui intègrent de plus en plus notre quotidien :

- La voiture de demain est électrique, connectée et autonome. En cas de cyberattaque, l'utilisateur peut perdre le contrôle du véhicule. Pire encore, de multiples accidents peuvent avoir lieu simultanément.

- L'Internet des objets va changer durablement les façons de se déplacer, d'habiter ou encore de se soigner[43]. En cas de compro-

[42] « Xenotime », *Dragos,* 2018.

[43] Wavestone, *L'IoT citoyen, un levier de création de valeur pour les français,* 2018.

mission, le citoyen pourrait ne plus pouvoir rentrer dans son domicile ou voir son historique médical modifié.

- Avec l'avènement de la 4e révolution industrielle, les procédés industriels du futur sont connectés et l'industrie sait valoriser la donnée. En cas de cyber ouragan, c'est peut-être la distribution d'eau ou les réseaux de transports en commun qui peuvent être interrompus.

Cette dynamique montre que, demain, ce ne seront plus les usines ou les entreprises qui seront interrompues en cas de cyberattaques, mais c'est plutôt le fonctionnement de notre quotidien et notre sécurité physique qui pourraient être affectés.

III

LE NIVEAU DE SÉCURITÉ DU TISSU ÉCONOMIQUE FRANÇAIS AUJOURD'HUI

Sous la dynamique d'un niveau général de la menace qui s'intensifie et des systèmes vulnérables à l'interconnexion croissante, les questions de cybersécurité représentent aujourd'hui des enjeux essentiels pour pouvoir continuer à tirer profit des bénéfices du numérique. Le chapitre suivant s'attelle à expliciter le niveau de protection actuel des acteurs économiques français et propose une analyse de la réponse du marché de la cybersécurité.

L'ANSSI, acteur de premier plan de la stratégie nationale pour la sécurité du numérique

La menace d'origine cyber a été prise en compte pour la première fois par le gouvernement dans le livre blanc sur la défense et la sécurité nationale de 2008. Ce livre blanc retient le risque d'une attaque informatique contre les infrastructures nationales comme l'une des menaces majeures les plus probables des quinze prochaines années. Ce constat a conduit le gouvernement à décider de renforcer significativement les capacités nationales en matière de cyberdéfense. La création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le 7 juillet 2009, a été la première étape de cet engagement[44]. Service à compétence nationale, l'ANSSI est rattachée au secrétaire général de la défense et de la sécurité nationale (SGDSN), qui assiste le Premier ministre

[44] Agence nationale de la sécurité des systèmes d'information (ANSSI), *Défense et sécurité des systèmes d'information : stratégie de la France,* 2011.

dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

L'agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. D'abord, centrée en priorité autour de la sécurité des systèmes d'informations de l'État, l'ANSSI a désormais une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale, ainsi que celle de contribuer à la sécurité de la société de l'information, notamment en participant à la recherche et au développement des technologies de sécurité et à leur promotion[45].

3.1. Les Opérateurs d'Importance Vitale et les Opérateurs de Services Essentiels au cœur de la réponse des États

Depuis l'entrée en vigueur de la Loi de Programmation Militaire (LPM) en décembre 2013 en France et l'adoption de la directive *Network and Information Security* (NIS) par l'Union européenne en juillet 2016, les États ont identifié les secteurs les plus critiques au fonctionnement de la Nation et au maintien de sa sécurité et de sa défense, et qui assurent le fonctionnement de l'économie et de la société. Ces travaux ont, par rebond, permis d'identifier les acteurs publics et privés exerçant des activités dans ces secteurs critiques.

[45] « Historique de l'ANSSI », site de l'ANSSI, 2018.

En France, c'est plus de 200 structures de toutes tailles qui ont été identifiées comme « indispensables au bon fonctionnement et à la survie de la Nation »[46] par les ministères coordonnateurs. L'Hexagone est le premier pays à s'appuyer sur la réglementation pour « définir un dispositif efficace de cybersécurité de ses infrastructures d'importance vitale », avec la publication dès 2016 des arrêtés sectoriels fixant les règles relatives à la sécurité des systèmes d'information des OIV prévues par l'article 22 de la LPM 2014-2019. D'autres pays, comme le Royaume-Uni, ont aussi emprunté la voie de la réglementation en complément de l'existant : dans ses efforts de transposition de la Directive européenne NIS (Directive (UE) 2016/1148 *Network and Information Security*) en droit national, le gouvernement britannique avait annoncé son intention de sanctionner jusqu'à hauteur de 4 % du chiffre d'affaires mondial consolidé[47] tout opérateur de services essentiels victime de cyberattaques et n'ayant pas mis en place les actions de sécurité appropriées pour les éviter ou en réduire les conséquences. Les sanctions ont désormais été limitées à 17 millions de livres sterling[48].

L'Allemagne adopte une approche différente, plus collaborative, pour la protection des infrastructures critiques : le BSI Act[49] allemand (BSIG) indique, sous la section 8a(2), que les opérateurs d'infrastructures critiques peuvent établir leur propre standard d'exigences de sécurité spécifique à leur industrie, sous contrôle de la BSI *(Federal Office for Information Security)* et de la BKK *(Federal Office of Civil Protection and Disaster Assistance)*. Il existe notamment des initiatives

[46] « Protection des OIV en France », *ANSSI,* 2018.

[47] « New fines for essential service operators with poor cyber security », *GOV.UK,* 2017.

[48] « Government acts to protect essential services from cyber attack », *GOV.UK,* 2018.

[49] German Federal Office for Information security, *Act on the Federal Office for Information Security,* 2009.

de groupes de collaboration comme le UP KRITIS[50] qui rassemble des acteurs publics et des structures privées pour proposer des cadres de référence dans le but d'augmenter la résilience des infrastructures critiques. L'Allemagne comptabilise, en 2017, 205 opérateurs d'infrastructures critiques et plus de 500 infrastructures critiques[51]. Des réflexions sont en cours et vont plus loin dans la démarche collaborative en considérant la possibilité pour les opérateurs d'infrastructures critiques de s'auto-déclarer auprès des autorités.

De façon coercitive ou collaborative, la situation progresse doucement mais sûrement et les acteurs majeurs investissent dans la cybersécurité de leurs systèmes les plus sensibles (dénommés Systèmes d'Information d'Importance Vitale ou SIIV dans la LPM). Ces dépenses peuvent être très lourdes et atteindre au maximum plusieurs dizaines de millions d'euros selon les secteurs[52]. Plus que des considérations financières, ces acteurs sont confrontés à des problématiques de manque de compétences et de capacité à faire avancer les chantiers de sécurisation.

[50] Voir la page web à l'adresse suivante : https://www.kritis.bund.de/SubSites/Kritis/EN/activities/national/cipimplementationplan/cipimplementationplan_node.html

[51] « The state of IT Security in Germany 2017 », German Federal Office for Information Security, 2017.

[52] Wavestone, *Sécuriser un SIIV : bilan financier,* 2017.

3.2. Les grandes entreprises[53], une mobilisation encore hétérogène

L'année 2017 a marqué les esprits en matière de cybersécurité. Bien qu'ayant causé sur son passage la destruction de milliers de systèmes informatiques, l'incident NotPetya a permis de faire progresser la prise de conscience. Les RSSI de grands groupes communiquent déjà régulièrement entre eux de manière informelle sur les risques encourus, et les comités exécutifs commencent à prendre en compte le sujet. En janvier 2018, le président de Maersk s'est prononcé devant ses pairs réunis lors du forum économique mondial à Davos sur les dommages causés par la cyberattaque[54]. Toutefois, cette prise de conscience reste très dépendante du secteur d'activité :

- Les banques sont les plus matures en matière de cybersécurité. Depuis longtemps tributaires du numérique pour fonctionner, les banques ont traité le sujet en priorité : JPMorgan Chase & Co annonçait en 2016 investir 500 millions de dollars pour protéger la banque contre les cybercriminels[55], tandis que Société Générale communiquait en 2017 dédier près de 650 millions d'euros à un programme sur trois ans pour la cybersécurité du groupe[56]. Il est intéressant de noter que l'empreinte économique et la solidité financière des banques leur permettent de débloquer de lourds

[53] À noter que certaines grandes entreprises peuvent être OIV ou OSE. Le découpage présenté dans ce rapport n'est pas exclusif et ne présume pas du statut d'OIV ou d'OSE des entreprises.

[54] « Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack », *Bleeping Computer,* 2018.

[55] « Why J.P. Morgan Chase & Co. Is Spending A Half Billion Dollars On Cybersecurity », *Forbes,* 2016.

[56] « Accelerate on digital and innovation », Société Générale, 2017.

investissements en cas de test. Les banques ont le meilleur niveau de protection contre les scénarios de « cyber ouragan ».

- Les sociétés dans le secteur du service et particulièrement les sociétés en B2C *(Business to Consumer)* se développent aussi sur le volet cybersécurité. Le secteur est marqué par la question de la confiance numérique. La prise de conscience des consommateurs sur leurs droits en matière de vie privée et de traitement des données personnelles pousse ces sociétés à investir en cybersécurité pour les rassurer. Mais c'est principalement l'évolution du régime des sanctions et les diverses réglementations, à l'instar de la norme PCI-DSS[57] ou du RGPD[58], qui ont poussé les sociétés de services à investir dans un souci de mise en conformité avec des budgets souvent négociés *a minima*. Le secteur affiche un niveau de protection intermédiaire face au scénario de « cyber ouragan ».

- Avec une moindre utilisation des outils numériques, les industries présentent le niveau de protection le plus bas par rapport aux autres secteurs. Il est aussi intéressant de noter que cette faible numérisation peut parfois représenter une forme de résilience vis-à-vis des attaques informatiques. Mais le secteur ne fait toutefois pas exception, une connectivité croissante peut être constatée sur le marché et l'avènement de l'industrie 4.0 va contribuer à augmenter leur surface d'exposition aux risques cyber. Les industriels n'ont pas toujours pris la mesure du risque, et par ailleurs, l'histoire a montré plusieurs cas de cyberattaques causant l'arrêt

[57] *Payment Card Industry Data Security Standard.*
[58] Règlement général sur la protection des données.

des usines : des sites de production de Renault[59] et de Honda[60] se sont retrouvés à l'arrêt en 2017 et en 2018, touchée par un virus informatique. Le constructeur taïwanais de micro-processeurs TSMC *(Taiwan Semiconductor Manufacturing Company),* lui, a été contraint de fermer ses usines pendant un jour entier[61].

3.3. Les services publics, une situation inquiétante qui s'améliore lentement

Les services publics couvrent un panel divers de secteurs d'activités et peuvent comprendre les ministères, les institutions, les collectivités territoriales, les secteurs de la santé ou encore les forces de l'ordre. En dehors des services publics identifiés comme OIV, la culture du risque cyber y est faible alors que les impacts en cas d'attaques destructrices peuvent être graves, comme en témoignent les cyberattaques qui ont visé l'hôpital *Hollywood Presbyterian Medical Center* à Los Angeles en 2016[62] et le système de santé public britannique *National Health Services* (NHS) en 2017[63]. Dans les deux cas, l'organisation s'en est retrouvée ébranlée et dans le cas du NHS, certains soins n'ont pas pu être dispensés. Du côté des services de l'État, il faut aller un peu plus loin pour constater des cas avérés de

[59] « Renault touché par la cyberattaque de niveau mondial, des sites de production à l'arrêt », *Le Monde,* 2017.

[60] « Cyber Attack At Honda Stops Production After WannaCry Worm Strikes », *Forbes,* 2017.

[61] « TSMC Chip Maker Blames WannaCry Malware for Production Halt », *The Hacker News,* 2018.

[62] « Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers », *The Guardian,* 2016.

[63] « Cyberattaques : les hôpitaux britanniques, principales cibles atteintes », *Les Echos,* 2017.

cyberattaques : Bercy en 2011[64] et l'Elysée en 2012[65], tous deux victimes d'espionnages informatiques. Ces incidents emblématiques ont toutefois fait progresser la situation sur les périmètres les plus sensibles.

Les services publics sont caractérisés par des structures complexes et difficiles à transformer : des procédures d'appels d'offres lourdes, des organisations de grande taille souvent réparties sur de nombreuses zones, une réglementation qui lui est propre… En matière de cybersécurité, la situation est donc très variable mais en retard en moyenne par rapport aux autres secteurs de l'économie. Dans les collectivités territoriales, la situation est pire, mais des initiatives voient le jour comme le programme DcANT 2018-2020[66], programme de développement concerté de l'administration numérique territoriale qui inclut des actions de cybersécurité en plus d'œuvrer à la transformation numérique des territoires.

Les services publics touchent par nature un nombre important de citoyens. En cas de « cyber ouragan », les impacts peuvent être particulièrement graves et il sera attendu de l'État qu'il soit en mesure d'assurer les éventuels secours. En particulier, les forces de sécurité et les services de secours sont fortement dépendants des radios mobiles professionnelles pour réaliser leurs actions. Or, à l'heure du tout numérique, ces radios évoluent pour inclure des fonctions désormais essentielles : flux vidéo, données de géolocalisation, accès aux applications métier… Elles sont donc plus exposées et poten-

[64] « Bercy, l'Élysée et le Quai d'Orsay visés par une cyberattaque », *Le Point,* 2011.

[65] « NSA: les Américains étaient-ils à l'origine de l'espionnage de l'Elysée en 2012 ? », *L'Express,* 2012.

[66] Le portail de la modernisation de l'action publique, *Programme dcant 2018-2020 : l'État et les collectivités territoriales transforment ensemble le service public,* 2017.

tiellement vulnérables. La revue stratégique de cyberdéfense a identifié ce sujet stratégique et le ministère de l'Intérieur a déjà enclenché des actions en ce sens[67]. Naturellement, cette numérisation des moyens de communication introduira de nouveaux risques qu'il s'agira de couvrir dans le but d'assurer la résilience des services de secours : sans connectivité, ils peuvent se retrouver dans l'incapacité de réagir. À titre d'illustration, en août 2018, la brigade de pompiers du Comté de Santa Clara en plein combat contre le « *Mendocino Complex* », l'incendie qui a ravagé plus de 117 000 hectares en Californie, s'est retrouvée dans l'incapacité de suivre et d'organiser la réponse car ses moyens de communication ont été fortement bridés par son opérateur de télécommunications[68].

3.4. Les TPE/PME/ETI au centre des préoccupations

À l'occasion de l'édition 2018 du Forum International de la Cybersécurité à Lille, le secrétaire d'État au numérique, Mounir Mahjoubi, s'exprimait sur la nécessité d'améliorer la protection des TPE/PME françaises[69]. Cet ensemble du tissu économique français présente un faible niveau de protection aujourd'hui. Il y a peu de compétences au sein de ces structures, peu de moyens et les réglementations et mesures entreprises par l'État dans le domaine de la cybersécurité ne les concernent pas.

---

[67] « Le Ministère de l'Intérieur choisit Orange Business Services pour son réseau de communications mobiles critiques dédié aux forces de sécurité », *Global Security Mag,* 2018.

[68] « Verizon throttled fire department's "unlimited" data during Calif. wildfire », *Ars Technica,* 2018.

[69] « Mounir Mahjoubi, FIC : il faut trouver les moyens d'améliorer la protection de nos TPE/PME », *Global Security Mag,* 2018.

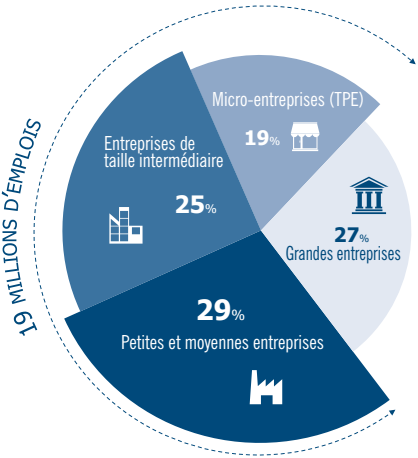
Le secrétaire d'État au numérique soulignait pourtant : « Si demain ce sont 25 000 TPE/PME qui tombent le même jour, c'est l'État français qui sera menacé », avant de rappeler encore une fois l'importance de sensibiliser les PME au risque de cyberattaque, à l'occasion du mois européen de la cybersécurité[70]. Selon les chiffres de l'Insee, en 2015, les TPE (MIC) et les PME représentent près de 54 % des emplois français (soit plus de 12,4 millions d'emplois) et les TPE/PME/ETI représentent ensemble près de 73 % des emplois français (soit plus de 19 millions d'emplois)[71]. Si les TPE/PME/ETI sont touchées simultanément par un scénario de type « cyber ouragan », cela pourrait donc devenir un véritable sujet sociétal, aggravé par le fait que ces structures présentent une certaine fragilité financière. Par exemple, en 2017, une TPE de Clermont-Ferrand spécialisée dans l'électroménager a été contrainte de mettre la clef sous la porte après avoir été victime d'un rançongiciel[72]. Cette situation isolée pourrait être généralisée en cas d'attaques majeures.

[70] « Comment l'État veut sensibiliser les PME au risque de cyberattaque », *L'Usine Nouvelle,* 2018.

[71] Insee, *Caractéristiques des entreprises par catégorie en 2015,* 2017.

[72] « Clermont-Ferrand : victime de pirates informatiques, un chef d'entreprise met la clef sous la porte », *France Info,* 2017.

Figure 6 - Répartition des emplois en France par taille d'entreprise



La principale problématique se situe au niveau des produits et services informatiques achetés et utilisés par les TPE/PME/ETI, car ils n'intègrent souvent pas la cybersécurité par défaut. Des compétences en cybersécurité sont alors nécessaires pour sécuriser leur usage. Des efforts de simplification et une signalétique claire doivent être entrepris pour aider à baliser simplement la marche à suivre pour ces structures. Des démarches ont déjà été lancées pour améliorer cette situation :

- Le GIP ACYMA est un groupement d'intérêt public qui « assume un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de la population française ». Il propose notamment une assistance et une mise en relation

entre des victimes de cybermalveillance et des prestataires de confiance.

- Les initiatives de labellisation comme le Visa de sécurité[73] délivré par l'ANSSI permettent de mettre en lumière les solutions de cybersécurité de confiance. Un label à l'échelle européenne en matière de cybersécurité est aussi à l'étude comme affiché dans la revue stratégique de cyberdéfense.

- L'ANSSI mène aussi des actions de proximité en région dans le but d'assister les collectivités territoriales et les entreprises locales[74]. L'ANSSI édite également des guides à destination des TPE et des PME notamment en partenariat avec la Direction Générale des Entreprises (DGE)[75] et avec la Confédération des petites et moyennes entreprises (CPME)[76].

3.5. Un marché dynamique des offreurs de cybersécurité en manque de compétences humaines

Le marché des offreurs de cybersécurité est particulièrement dynamique et comporte de très nombreux acteurs. Si les États-Unis et Israël présentent l'écrasante majorité des offreurs de produits de cybersécurité, la France et plus largement l'Europe ont une carte à jouer sur les services en cybersécurité. Tous les offreurs sont toutefois marqués

[73] « Pourquoi les visas de sécurité ANSSI ? » site ANSSI.

[74] « Action territoriale » site ANSSI.

[75] « Référentiel pédagogique de formation à la cybersécurité des TPE et des PME », site ANSSI, 2017.

[76] « Guide des bonnes pratiques de l'informatique », site ANSSI.

par la même difficulté globalisée de manque de compétences. Les technologies existent mais il manque des femmes et des hommes avec les bonnes compétences pour les manipuler. En France, le label SecNumedu délivré par l'ANSSI à 50 formations dans les écoles et universités a délivré 901 diplômes l'an passé. Cette année, ce sont 1 365 places qui sont ouvertes dans ces formations[77]. Il est néanmoins probable que le manque de compétences ne se résorbera pas à court terme. Seulement aux États-Unis, il est estimé qu'il y a encore en 2018 près de 5 000 postes non pourvus en cybersécurité[78]. Certaines écoles éprouvent même parfois des difficultés à trouver des professeurs.

Au-delà du manque de compétences, une autre grande difficulté frappe le secteur : les offreurs de cybersécurité ciblent en majorité les grandes entreprises. Pour les TPE/PME/ETI, il n'existe aujourd'hui que très peu d'offres et certaines offres existantes n'ont pas trouvé leur marché d'une part dû à la complexité de mise en œuvre et d'autre part à cause du manque d'appétence de ces structures pour les sujets cybersécurité. Les efforts doivent donc être double :

- des investissements et une prise de conscience à enclencher chez les TPE/PME/ETI ;

- des efforts de simplification des produits de cybersécurité, comme par exemple intégrer par défaut la cybersécurité de façon packagée aux produits à destination des entreprises de taille réduite.

L'analyse du marché de la cybersécurité ne saurait être exhaustive sans traiter le sujet de la souveraineté. Une véritable prise de conscience s'opère aujourd'hui au sein des États. En France, la revue stratégique

[77] « Formations labelisées SecNumEdu » site ANSSI.
[78] https://www.cyberseek.org/

de cyberdéfense présente trois technologies « dont la maîtrise est nécessaire à l'exercice de notre souveraineté numérique » :

- Le chiffrement des communications.
- La détection d'attaques informatiques.
- Les radios mobiles professionnelles.

Dans l'optique de maintenir la souveraineté numérique, miser sur le développement des *startups* cybersécurité françaises peut être une bonne approche. L'écosystème français de *startups* cybersécurité est d'ailleurs florissant et dynamique, on constate une augmentation en nombre de près de 30 % entre 2017 et 2018[79]. Toutefois, il est marqué par des difficultés de croissance flagrantes. En effet, en dehors des quelques levées de fonds emblématiques, les *startups* cybersécurité françaises peinent à trouver des investissements à hauteur de plusieurs millions d'euros qui leur permettraient de passer à l'échelle et de pousser les portes de l'international[80]. Cependant, le financement n'est pas le seul moyen de soutenir les *startups,* les grandes entreprises peuvent aussi participer à la croissance des jeunes pousses françaises en adaptant leurs processus d'achat pour inclure les *startups* dans les critères d'éligibilité et en les rémunérant lors des phases pilote de *Proof of Concept.*

[79] « Cybersécurité et *startup* : la France en croissance », *Les Echos,* 2018.

[80] Selon les points de vue, la réussite des *startups* françaises à l'étranger et l'export peut participer à la souveraineté numérique. Dans ce cas-là, souveraineté et protectionnisme économique ne sont pas synonymes.

3.6. Les autorités et les acteurs de la recherche mobilisés pour augmenter les compétences en cybersécurité

À l'échelle européenne, le président de la Commission européenne Jean-Claude Juncker annonçait en septembre 2017 renforcer le champ d'action de l'ENISA, en la transformant en une véritable agence de cybersécurité européenne[81] pour notamment promouvoir les produits et services de cybersécurité en Europe. La Commission européenne est motrice sur la recherche et le développement des compétences avec la création d'un réseau de centres de compétences et de recherche en cybersécurité[82]. La Commission a aussi annoncé en juin 2018 son intention d'investir deux milliards d'euros dans la cybersécurité et la confiance numérique au sein de l'Union[83].

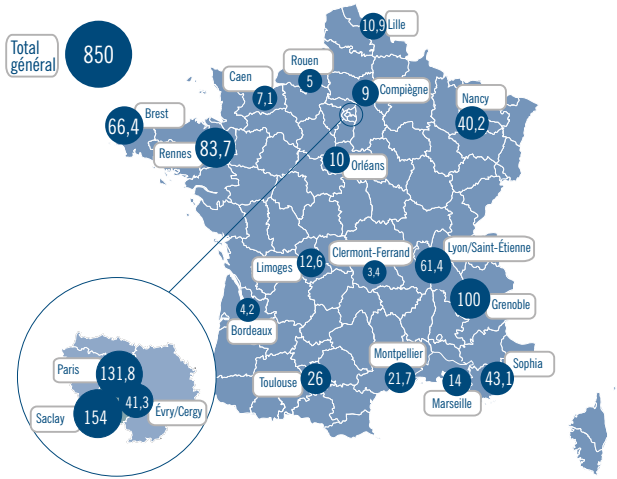
La recherche académique bénéficie d'une dynamique positive dans le domaine de la cybersécurité. Les compétences cyber sont bien présentes au sein des équipes de recherche. Selon une analyse menée par ALLISTENE (Alliance des sciences et technologies du numérique) auprès des établissements de recherche français, on estime à 1 100 le nombre de personnes qui travaillent en recherche dans le domaine de la cybersécurité – des chercheurs, enseignants-chercheurs, ingénieurs, doctorants – en France. Au sein de l'INRIA, près de 200 ETP (équivalents temps plein) sont dédiés à la cybersécurité, et il y en a 850 au total en France.

[81] « State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks », Commission Européenne, 2017.

[82] « Reminder: Call for proposals for a €50 million pilot to support the creation of a network of cybersecurity competence centres across the EU », Commission européenne, 2018.

[83] « Budget de l'Union : La Commission propose d'investir un montant de 9,2 milliards d'euros dans le tout premier programme numérique », Commission européenne, 2018.

Cartographie de la recherche française en cybersécurité[84]



Source : Allistene, 2017.

Il est important de noter que la recherche académique suit également une logique de recrutement des talents. Les instituts de recherche se livrent une bataille pour attirer les meilleurs chercheurs et la concurrence étrangère est forte. L'Allemagne a fortement investi récemment dans la recherche en cybersécurité : le gouvernement allemand a en effet lancé une politique ambitieuse de créer une *Silicon Valley* européenne et a créé à ce titre l'Institut Helmholtz CISPA i.G. *(Center for IT Security, Privacy and Accountability)* à Sarrebruck qui est doté d'un budget annuel de 50 millions d'euros et ambitionne d'attirer 800 chercheurs.

[84] « Cartographie de la recherche académique française en cybersécurité », Allistene, 2017.

La mobilisation de la recherche est importante dans un domaine technologiquement complexe où beaucoup reste à construire.

3.7. La cyberassurance, un mécanisme assurantiel au potentiel vertueux mais qui navigue à vue

Aujourd'hui, l'offre de cyberassurance permet de couvrir les entreprises sur plusieurs volets :

- sensibiliser et alerter les entreprises sur le risque cyber ;
- évaluer l'exposition aux risques cyber ;
- accompagner les entreprises victimes de cyberattaques ;
- couvrir les dégâts financiers (matériel, immatériel, sanctions…) potentiels en cas de sinistres.

Les politiques d'assurance cyber peuvent donc apporter leur lot de bienfaits pour couvrir les risques résiduels, toutefois le marché de la cyberassurance n'affiche pas encore une maturité et un déploiement suffisants face à un risque de cyber ouragan.

Le marché de la cyberassurance pourrait doubler d'ici 2020, à 10 milliards de dollars et atteindre jusqu'à 20 milliards de dollars d'ici 2030[85]. Ces projections traduisent une dynamique forte du secteur et le fait que le sujet devient une préoccupation croissante

[85] « Growing threat from cyber risks. Munich Re offers more than just insurance », Munich RE, 2018.

des chefs d'entreprise[86] et donc un enjeu stratégique pour les cyberassureurs et ré-assureurs.

Le marché croît mais il navigue à vue, car les données de sinistre ne sont pas en nombre suffisants pour pouvoir évaluer finement l'exposition aux risques et toutes les réactions en chaîne que pourrait engendrer un scénario systémique. Cette croissance se fait donc en demi-teinte : la couverture du marché n'est pas suffisante et les assureurs sont précautionneux de se prémunir contre le risque d'accumulation qui grandit avec le caractère systémique des scénarios mis en avant dans ce rapport. En particulier, contrairement aux catastrophes naturelles, les cyberattaques ne sont pas circonscrites à une région donnée et sont moins prédictibles.

Par ailleurs, le marché n'est pas encore suffisamment mature non plus en matière de jurisprudence concernant l'activation ou la non-activation des clauses d'exclusion. Comme, par exemple, les exclusions liées aux actes de guerre, qui ne sauraient trouver la base juridique solide suffisante pour se faire valoir, en particulier face à la difficulté de caractériser une cyberattaque en acte de cyberguerre.

[86] Marsh, *Les principales préoccupations des dirigeants d'entreprises en 2017,* 2017.

IV

PROPOSITIONS POUR AUGMENTER LA CYBERRÉSILIENCE DU TISSU ÉCONOMIQUE FRANÇAIS

Si le numérique apparaît aujourd'hui comme un catalyseur de l'innovation et du progrès, il est toutefois nécessaire que tous les acteurs concernés prennent la mesure des risques inhérents au cyberespace pour être en mesure de prévenir et contenir les effets systémiques pouvant découler d'une cyberattaque destructrice d'ampleur. Le chapitre suivant expose les propositions de ce rapport pour augmenter la cyberrésilience du tissu économique français face à des scénarios de type « cyber ouragan ».

Menées entre mars et octobre 2018, les auditions et les travaux du groupe de travail ont permis d'identifier trois enjeux majeurs pour atteindre cet objectif :

- mobiliser l'ensemble du tissu économique pour anticiper un cyber ouragan ;

- démultiplier les compétences et être solidaire en cas de crise majeure ;

- pouvoir répondre à des attaques larges et rapides de manière efficace.

Les recommandations du groupe de travail ont donc été axées autour de ces trois piliers.

Mobiliser l'ensemble du tissu économique

Pour les entreprises cotées d'une certaine taille :

1. Encourager la rédaction d'un rapport sur les risques cyber à disposition des administrateurs, voire une intégration partielle dans les rapports annuels.

Constat :

Les entreprises du CAC 40 ont beaucoup communiqué ces dernières années sur leurs plans de transformation numérique. Mais cette numérisation accrue s'accompagne évidemment de risques de cybersécurité, dont les mentions se font plus rares. Elles forment pourtant un bon indicateur du niveau d'attention apporté par les instances dirigeantes à ces risques.

Pour évaluer la prise en compte de la cybersécurité dans les entreprises du CAC 40, le cabinet Wavestone a ainsi récemment[87] analysé l'ensemble de leurs documents de référence à la recherche de mentions sur la cybersécurité ou sur leurs plans d'action de couverture du risque. Publiés par les entreprises cotées à Euronext, les documents de référence sont un moyen pour elles de communiquer aux analystes financiers et aux investisseurs la nature de leurs activités mais aussi de leurs risques et perspectives de manière à faciliter les opérations sur le marché.

On note que si 73 % des entreprises communiquaient sur la cybersécurité dans leur document de référence en 2010, elles sont

[87] « Quel bilan de maturité cybersécurité dans les rapports annuels du CAC 40 ? », Wavestone, 2018.

100 % en 2017, marquant une mobilisation accrue des grands groupes français sur ces sujets, et ce au plus haut niveau.

Ce constat est toutefois à nuancer. 25 % des groupes du CAC 40 uniquement abordent directement la problématique de la cybersécurité au niveau des comités exécutifs. Les investissements réalisés et les plans d'actions mis en œuvre pour couvrir ces risques sont encore peu mentionnés par les groupes français. Les investissements restent morcelés et à des niveaux hétérogènes : seules 12,5 % des entreprises du CAC 40 annoncent avoir lancé un programme de cybersécurité contre 75 % qui ne mentionnent que des plans d'action unitaire morcelés. Plus surprenant, seulement 58 % des entreprises du CAC 40 faisaient mention du RGPD dans leurs documents de référence en 2017.

La vigilance concrète et opérationnelle des risques de cybersécurité par le plus haut niveau reste donc à atteindre : la communication des groupes doit être complétée d'une analyse de risques et de plans d'action plus détaillés. Cette vigilance est d'autant plus essentielle dans un contexte où les groupes communiquent beaucoup sur leur numérisation. Il est important que ces deux stratégies soient liées.

Recommandation :

Le manque de communication au plus haut niveau en matière de cybersécurité est à la fois le témoin du manque de sensibilisation des équipes dirigeantes et la marque du manque d'intégration de la cybersécurité à la stratégie d'entreprise.

Pour répondre à ces carences, nous proposons d'encourager la rédaction d'un rapport sur les risques cyber à disposition des administrateurs

et d'intégrer partiellement ces risques et les contre-mesures au rapport annuel.

Cette proposition vise deux objectifs :

- Le premier est de sensibiliser les dirigeants à l'étendue de leurs risques cyber. La documentation destinée aux administrateurs est bien sûr suivie attentivement par la direction générale ; y inclure un résumé des risques cyber de l'entreprise et les actions prévues pour y répondre assurerait donc une implication accrue de toute l'équipe dirigeante.

- Le second est d'obtenir la validation par les administrateurs, dont c'est l'une des missions, de la stratégie de l'entreprise pour répondre à ces risques.

Ce document pourra inclure des volets sur les sujets de : la menace contextualisée à l'entreprise ; l'implication des instances dirigeantes ; la gouvernance de la cybersécurité et les plans d'action de couverture des risques ou programmes de cybersécurité ; l'intégration de la cybersécurité dans la stratégie numérique ; la protection des données personnelles ; la cyberassurance ; la sensibilisation…

Ce rapport, non public, serait seulement destiné aux administrateurs de manière à éviter toute exploitation par des acteurs mal intentionnés et pour éviter de porter atteinte à l'attractivité de l'entreprise. En cas de publication intégrée dans le rapport annuel, le volet sur les risques cyber pourrait exposer les incidents répertoriés plutôt que le détail des risques qui doit rester à la discrétion de l'entreprise.

Pour les ETI/PME/TPE

2. Mobiliser les réseaux des métiers du chiffre (experts-comptables et commissaires aux comptes) pour réaliser un diagnostic cybersécurité annuel avec un cahier des charges minimum (construit avec les autorités nationales). Il serait communiqué aux dirigeants à titre d'information avec les recommandations de base pour couvrir les risques.

Constat :

L'institut de recherche technologique SystemX évalue à 50 000 le nombre de PME victimes d'une cyberattaque en 2017 avec des dégâts financiers significatifs pour leur trésorerie[88]. Trop peu sensibilisées au risque cyber, des attaques courantes comme le rançongiciel ou les fraudes au président ont touché de nombreuses PME l'année dernière.

Face à cela, leur niveau d'investissement en matière de cybersécurité reste décevant : un premier indicateur de ce manque d'investissement est leur faible recours aux offres d'assurance cyber. Évidentes quand il s'agit du risque d'incendie ou de vol, elles le sont beaucoup moins en matière de cybersécurité. L'audition réalisée par l'Institut Montaigne auprès d'une responsable cyber dans une grande société d'assurance nous apprend ainsi que si 100 % des entreprises du CAC 40 ont souscrit des assurances cyber (elles étaient 80 % en 2016 avant les attaques Wannacry et NotPetya), seulement 30 % des ETI en France sont couvertes. Ce taux est encore plus faible pour les TPE/PME, signe de la sensibilisation qu'il reste encore à faire.

[88] IRT SystemX, *Les cyberattaques et leurs préjudices sur les entreprises : quantification et qualification,* 2017.

Or, les PME sont régulièrement les cibles d'attaques, notamment car ce sont des points d'entrée privilégiés des attaquants dans la chaîne d'approvisionnement des grands groupes. Jean-Michel Denys, membre du groupe de travail audit informatique à la Compagnie régionale des commissaires aux comptes de Paris écrit ainsi que « dans la région de Toulouse, par exemple, [ils ont] vu des PME se faire attaquer parce qu'elles travaillent pour des grandes entreprises des secteurs aéronautique ou pharmaceutique ».

Dans certains secteurs, l'investissement en cybersécurité pourrait parfois être également une opportunité pour les PME : un système informatique sécurisé est un argument commercial qui leur permet de gagner des contrats.

Malgré cela, et le fait que les offres de cybersécurité à destination des PME se développent, le nombre de PME préparées au risque cyber reste faible. Il manque donc un accompagnement spécifique à ces entreprises pour les sensibiliser, les aider à évaluer les risques cyber auxquels elles sont confrontées et les diriger vers les solutions les plus adaptées.

Recommandation :

Notre proposition s'appuie sur un constat simple : l'individu auquel le chef d'entreprise pense naturellement quand il s'agit d'évaluer ses risques, qu'ils soient financiers ou d'une autre nature est l'expert-comptable ou le commissaire aux comptes. Ces métiers du chiffre sont très bien connectés aux PME et se positionnent comme des tiers de confiance pour l'entreprise et son environnement. D'après un expert auditionné par l'Institut Montaigne, le nombre d'entreprises touchées par ces professions s'élève à 2 150 000 (2 000 000 pour les experts-comptables et 150 000 pour les commissaires aux comptes).

Nous proposons donc de les mobiliser pour intégrer des diagnostics cybersécurité et rendre ces diagnostics obligatoires dans un second temps. Ces évaluations pourraient reposer sur un document préétabli en partenariat avec des experts en matière de cybersécurité. Des recommandations seraient alors adressées, sous forme informatives, par l'expert-comptable ou le commissaire aux comptes, pour poser les fondements d'un plan de réponse.

L'ordre des experts-comptables y est d'ailleurs favorable puisqu'il a fait paraître en mars 2018 un communiqué où il s'engage à accompagner les PME et TPE dans la lutte contre la cybercriminalité. L'ordre a ainsi formulé dix « commandements »[89] pour se prémunir de la cybercriminalité. Il en va de même pour la Compagnie des commissaires aux comptes, qui a partagé avec nous leur ambition de mettre en place une plateforme d'évaluation des risques de leurs clients : leur exposition ; leur maturité face à cette exposition ; la construction de scénarios de cyberattaques ; l'impact financier en cas de réalisation du scénario.

Les experts-comptables sont déjà sensibilisés aux questions de sécurité puisqu'ils peuvent être convoqués par la police nationale et être amenés à répondre à toute question portant sur des problèmes de technique comptable, financière ou fiscale (dans le respect du secret professionnel). Cependant, il est indispensable de continuer d'augmenter le niveau de compétence des métiers du chiffre sur ces questions, en incluant des journées de formation dans les programmes de formation auxquels les experts-comptables et commissaires aux comptes doivent participer, afin qu'ils puissent réaliser ces évaluations et avoir un dialogue efficace avec les chefs d'entreprise.

[89] « Dix commandements pour se prémunir de la cybercriminalité », *SIC, Le magazine de l'Ordre des experts-comptables,* 2018.

Au-delà d'alerter et de sensibiliser les chefs d'entreprise sur le sujet, cette recommandation pourrait, dans un temps plus long, participer à mettre en place un dispositif vertueux *via* un système de notation (profil de risque A/B/C/D…). Par exemple, la notation Banque de France permet d'apprécier la situation financière des entreprises par rapport à un ensemble de règles méthodologiques et communes : les chefs d'entreprise sont naturellement incités à rechercher une note maximale pour rassurer leurs investisseurs sur leur capacité à respecter les engagements et de résistance face aux évolutions de l'environnement. La notation cyber issue de l'évaluation par les experts-comptables et les commissaires aux comptes pourrait, par exemple, servir aux cyberassureurs : les chefs d'entreprise pourraient alors être incités à rechercher une note élevée pour bénéficier de bonus sur leur prime de cyberassurance.

3. Inciter et mobiliser les grands groupes sur leur responsabilité pour augmenter le niveau de cybersécurité de leur chaîne d'approvisionnement et de leurs fournisseurs.

Constat :

Pour rendre plus efficace leur logistique, la plupart des grands groupes ont fortement intégré leurs procédures et leurs systèmes avec ceux de leurs fournisseurs : il existe par exemple des systèmes de suivi des stocks partagés ; de nouvelles commandes peuvent ainsi être directement envoyées au sous-traitant en cas de besoin.

La chaîne d'approvisionnement des grands groupes intègre donc de plus en plus de systèmes numériques. Cette interconnexion, si elle facilite la production, introduit bien sûr de nouveaux risques cyber. Il peut maintenant suffire aux cybercriminels d'attaquer un fournisseur de taille moyenne pour avoir accès aux données de plusieurs entreprises,

voire du groupe directement. Dans certains cas, ils peuvent également interrompre le fonctionnement des services des entreprises.

Les liens numériques entre entreprises d'une même chaîne d'approvisionnement sont donc le reflet d'une nouvelle chaîne de risques, dans laquelle l'élément le plus faible peut mettre en danger l'ensemble du groupe.

Il est dans l'intérêt des grands acteurs d'assurer la sécurité de leur écosystème. Attention, la solution ne peut-être uniquement juridique. Les grands groupes incluent de plus en plus régulièrement des clauses cyber dans les contrats de prestation. Mais là encore, cela ne peut être un substitut à une démarche plus responsable de mobilisation et de formation des acteurs locaux, en manque de compétences cyber.

En outre, la notion de chaîne d'approvisionnement ne se cantonne pas uniquement à celles du cœur de métier. Ainsi, les entreprises qui externalisent l'infogérance de leurs systèmes d'information doivent prendre la mesure du risque et s'assurer que leurs sous-traitants prennent en compte effectivement le sujet cybersécurité.

Recommandation :

Nous proposons donc que les grands groupes forment et sensibilisent les petites entreprises et les fournisseurs dont ils dépendent à la cybersécurité, en rendant disponible une partie de leurs experts. La multiplication de ces échanges pourrait se matérialiser au sein de « centres d'accélération » tel que préconisé dans le rapport de l'Institut Montaigne « Industrie du futur, prêts, partez ! », mesure reprise par Edouard Philippe dans son plan pour transformer l'industrie par le numérique[90].

[90] « Discours à l'occasion de la présentation du plan d'action pour transformer notre industrie par le numérique », Gouvernement.fr, 2018.

Ces centres d'accélération s'inscrivent dans une démarche plus large[91] visant à mettre à disposition des structures de petites tailles des ressources matérielles et humaines leur permettant de se développer et monter en compétences. La forte mutation actuelle des métiers traditionnels signifie en effet que la capacité d'adaptation des entreprises est devenue une condition de leur survie. En s'assurant que leur chaîne d'approvisionnement reste robuste à ces changements, les grands acteurs stabilisent donc leur production.

Et la cybersécurité est bien un de ces enjeux : nous proposons donc qu'un pôle cyber voit systématiquement le jour au sein de ces centres d'accélération. Ce pôle serait animé par les experts des grandes entreprises clientes. L'objectif est ici celui de la prévention : il faut sensibiliser les TPE/PME/ETI, qui sont les plus touchées par les cyberattaques, aux risques qu'elles courent. Les formations qu'ils prodiguent à leur écosystème sont une première manière d'apporter aux TPE/PME des compétences qu'elles ont encore du mal à trouver sur le marché du travail.

4. Inciter à la création et à la souscription d'offres cybersécurité pour les TPE/PME/ETI, en particulier des offres de connectivité réseau intégrant par défaut des mesures de sécurité de base (nettoyage du trafic), des offres d'applications métier (ex. ERP) sécurisées par défaut et des offres de cyberassurance, incluant des services en cas d'incidents.

Constat :

Les PME et ETI, *a fortiori* les TPE, n'ont pas accès aux mêmes compétences en cybersécurité que les grands groupes. Ainsi, l'exis-

[91] Institut Montaigne, *Industrie du futur, prêts, partez !,* 2018.

tence de solutions sur étagère destinées aux TPE/PME/ETI de manière à ne pas avoir besoin de développer ou acquérir de nombreuses compétences en cybersécurité est crucial.

D'autres pays ont déjà lancé cette démarche : le Centre national de cybersécurité britannique (NCSC), à travers son programme *active cyber defense,* et la ville de New York, par le biais de la *startup* Quad9, fournissent respectivement des services de sécurisation de sites *web* et du réseau Internet gratuitement pour certains usages. Pour ce faire, les opérateurs et les fournisseurs de service doivent être mobilisés.

Autre exemple d'offre de cybersécurité immédiatement utilisable par les PME : l'*Enterprise Resource Planning* (ERP) dans le nuage par des fournisseurs labellisés à l'échelle européenne. Une offre packagée et sécurisée « *by design* » répondrait à un besoin des entreprises au secteur d'activité traditionnel, c'est-à-dire sans informatique en dehors de la comptabilité. Dans cet exemple, il est aussi nécessaire de veiller à ce que le marché se structure et se développe pour ne pas créer de nouveaux acteurs systémiques.

Comme évoqué plus tôt, la cyberassurance est un autre levier générique à disposition des PME, d'autant plus qu'au-delà du support financier, l'assureur accompagne quasi-systématiquement l'offre de services de gestion de crise, très précieux pour les petites organisations aux compétences en cybersécurité limitées.

Recommandation :

Pour répondre au besoin des PME/TPE/ETI, il faut donc favoriser la création d'offres sur étagère, simples, transparentes et ne requérant pas de compétences fortes.

Il n'est pas nécessaire que toutes ces mesures soient à l'initiative de l'État. Certaines initiatives pourront être lancées dans le cadre d'un travail en commun entre l'État et les opérateurs, mais il semble nécessaire que le développement de ces offres intégrant la sécurité par défaut soit une évolution naturelle des services des fournisseurs de manière à développer ou maintenir un avantage concurrentiel. L'alternative coercitive, qui imposerait cette évolution par la réglementation, ne saurait se justifier ici et pourrait être contre-productive. La réglementation peut se justifier lorsque les autorités demandent des actions que les organisations n'entreprendraient pas naturellement. Si l'on reprend l'exemple des opérateurs télécoms travaillant avec l'État pour nettoyer les flux de données transitant sur leurs réseaux, il s'agit bien d'une évolution naturelle de leur métier ; l'imposition par la contrainte n'a donc pas été jugée nécessaire.

L'État peut en revanche rendre plus visible ces offres de cybersécurité en les structurant par la labellisation (les Visas de sécurité ont vu le jour en France et l'action est en cours au niveau européen) ou par le lancement d'appels d'offres de l'État sur des services sécurisés.

Pour les secteurs critiques

5. Faire évoluer le corpus réglementaire, en particulier les textes liés à la loi de programmation militaire (LPM) 2014-2019, pour y ajouter des exigences précises de cyberrésilience (réalisation annuelle d'un exercice de crise, existence d'un système d'information de crise indépendant du système d'information nominal, introduction de diversité technologique sur les systèmes d'information d'importance vitale, etc.).

Constat :

L'article 22[92] de la loi de programmation militaire (LPM) de 2014 -2019 et la transposition de la directive *Network and Information Security* (NIS) en droit français apportent déjà beaucoup d'éléments sur la protection des infrastructures d'importance vitale et de services essentiels. En particulier, la LPM 2018 permet désormais aux opérateurs télécoms de mettre en œuvre des mesures de détection d'activités malveillantes sur leurs réseaux. Ces mesures, ciblant initialement les opérateurs d'importance vitale (OIV) sont élargies aux opérateurs de services essentiels (OSE).

Bien que l'arrêté[93] fixant les règles de sécurité, qui va s'appliquer aux OSE, relatives à la directive NIS introduise la notion de résilience, les règles LPM et NIS sont en très grande partie centrées sur la protection des systèmes d'information (SI) et la détection d'attaques. Elles ne couvrent pas encore complètement la résilience des systèmes, c'est-à-dire la capacité à rapidement endiguer une attaque, en limiter les effets et reprendre l'activité au plus vite (gestion de crise, reconstruction du SI en cas de destruction, continuité des métiers sans SI…).

En effet, lorsque des cyberattaques majeures et destructrices touchent une entreprise, leur premier réflexe est d'activer un plan de continuité d'activité (PCA) pour redémarrer l'activité le plus vite possible après l'incident. Or, les cyberattaques majeures provoquant une perte de

[92] Plus précisément, les arrêtés sectoriels, publiés dès 2016, fixant les règles relatives à la sécurité des systèmes d'information des OIV prévue par l'article 22 de la LPM 2014-2019.

[93] « Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique », Legifrance, 2018.

confiance dans les infrastructures (réseau, gestion des accès, gestion du parc…) n'ont pas été prises en compte lors de l'élaboration de la majorité des PCA. En particulier car ces plans s'appuient sur des principes de redondance et de synchronisation en temps réel qui propagent l'attaque sur les systèmes de secours dès qu'elle touche le système principal.

Les dispositifs de continuité et les procédures de gestion de crise des entreprises doivent évoluer pour s'adapter aux menaces cyber et être en mesure d'anticiper et limiter les effets d'une attaque. C'est donc un changement de mentalité qui s'opère : la question n'est pas de savoir seulement comment éviter une attaque mais aussi comment y résister en cas d'incident et reconstruire rapidement.

Recommandation :

Nous proposons de faire évoluer le corpus réglementaire, en particulier les arrêtés sectoriels fixant les règles relatives à la sécurité des systèmes d'information des OIV prévues par l'article 22 de la LPM 2014 et des OSE, pour y introduire des exigences de cyberrésilience ; les règles suivantes pourraient être rendues obligatoires :

- réalisation annuelle d'un exercice de crise cyber ;
- existence d'un système d'information de crise indépendant du SI nominal ;
- mise à disposition de capacités de reconstruction après un sinistre majeur.

Et pour des secteurs ciblés, il pourrait être demandé l'introduction d'une diversité technologique sur les SI d'importance vitale.

Cette recommandation va dans le sens des premières règles établies pour protéger les OIV qui se voulaient ambitieuses mais atteignables rapidement et sans donc être exhaustives. Il a toujours été dans la philosophie du texte, dont les premières règles ont été publiées par arrêtés, de laisser la possibilité de réaliser des mises à jour ultérieurement.

La première règle – la réalisation annuelle d'un exercice de crise cyber – est une simple adaptation au monde numérique d'exigences établies dans les grandes entreprises depuis longtemps. Il s'agit donc de généraliser ces exercices au sujet cyber et à l'ensemble des secteurs critiques.

L'existence d'un système d'information (SI) de crise indépendant du SI nominal permet d'assurer la capacité à réagir et à coordonner les actions même en cas de cyberattaque qui se propage très rapidement de façon large et indiscriminée.

En cas de sinistre majeur, la reconstruction nécessite tant des ressources humaines que matérielles, si bien que les collaborateurs de l'entreprise peuvent être mis à contribution pour passer à l'échelle rapidement, par exemple pour reconstruire leur propre poste de travail. Par ailleurs, il est nécessaire d'anticiper pour être en mesure d'automatiser la reconstruction.

L'introduction d'une diversité technologique sur les SI d'importance vitale vise à limiter les effets d'amplification d'une attaque en utilisant, par exemple, des systèmes d'exploitation différents (Windows, Linux, macOS…). Cette diversité ne concernerait que les systèmes les plus critiques pour commencer du fait des coûts importants engendrés et de problématiques d'acceptabilité. La mise en place d'une telle diversité

technologique doit bien sûr s'accompagner d'une formation adaptée aux experts chargés de veiller sur ces systèmes.

Démultiplier les compétences et être solidaire en cas de crise

6. Créer un parcours de formation financé par l'État en contrepartie d'un engagement dans la réserve de cyberdéfense pour un nombre minimum d'années afin de réaliser un appui opérationnel en cas de crise et de maintenir les compétences (entraînement, action de prévention…).

Constat :

Les nombreuses cyberattaques de ces dernières années en sont le témoin : le niveau général de la menace augmente et les organisations peinent à combler le retard en matière de sécurisation des systèmes alors même que l'innovation suit son cours et que de nouvelles solutions technologiques voient le jour. Le marché de la cybersécurité est ainsi aujourd'hui en forte croissance.

Selon le cabinet d'études Xerfi, la hausse des besoins en cybersécurité constatée en 2017 (+ 10 % sur le marché français) devrait se poursuivre au rythme moyen de 10 % par an à l'horizon 2020, soit un peu plus vite que le marché mondial (+ 9,5 % par an).

Mais cette activité connaît aujourd'hui une limite majeure : la disponibilité de professionnels compétents dans le domaine. Le recrutement d'ingénieurs et techniciens formés à la cybersécurité est donc un facteur limitant de la montée en régime du marché français et international.

Face à ce constat, l'ANSSI a lancé un programme de labellisation nommé SecNumEdu qui vise à qualifier les formations initiales en cybersécurité de l'enseignement supérieur pour apporter une assurance aux étudiants et employeurs concernés que la formation répond aux critères retenus par l'ANSSI avec les acteurs du domaine.

Les écoles et organismes de formation réagissent également avec l'apparition de nouvelles formations à tous les niveaux, notamment avec la création de nombreux masters spécialisés. Parallèlement, le recrutement de profils différents, plus expérimentés ou issus d'autres métiers, pour combler ces carences est une alternative suivie avec attention. La bonne transition de ces profils suppose donc une formation de qualité… Or, le coût des études longues (Bac + 5) ou de formations de reconversion constituent une barrière financière.

Recommandation :

Nous proposons la création d'un parcours de formation, incitatif, financé par l'État. Cet appui de la puissance publique exigerait un engagement de l'étudiant pour un nombre minimal d'années auprès de l'État. La réserve de cyberdéfense, rattachée au commandement de cyberdéfense, et constituée de 400 réservistes opérationnels, pourrait ainsi bénéficier de leur soutien en cas d'attaque d'envergure. L'une de leurs missions principales est la restauration des capacités opérationnelles des systèmes impactés. La réserve de cyberdéfense est actuellement en cours de refonte par le COMCYBER et l'ANSSI.

Ces formations pourraient être assurées dans des écoles disposant de cursus spécialisés ou dans les centres de formation de l'ANSSI (en identifiant des moyens spécifiques à sa montée en puissance).

Toutefois, la contrepartie ne doit pas se limiter à des sujets de cyberdéfense mais aussi s'ouvrir à des sujets civils, de manière à mobiliser les diplômés dans le temps en dehors de situation de crise (pour des formations, des actions de prévention ou de sensibilisation). Les réservistes pourraient à ce titre constituer un tissu de formateurs capables d'intervenir dans ces circuits de formation.

Les bénéfices attendus à court terme seraient l'augmentation des effectifs formés et disponibles pour la nation ; à moyen terme, ces parcours de formation amorceraient le renforcement du tissu cyber entre acteurs publics et privés, une partie des ressources évoluant naturellement vers le privé à l'issue de leur formation. Un tel dispositif pourrait aussi nourrir un sentiment d'appartenance et de patriotisme non négligeable.

Cette démarche pourrait d'ailleurs s'inscrire dans le Grand Plan d'Investissement engagé par le gouvernement. Le Plan d'Investissement dans les Compétences (PIC) en est l'un des quatre volets : 15 milliards d'euros sont ainsi prévus sur la période 2018-2022 pour renforcer les compétences et l'emploi. Le gouvernement a précisé que ce dispositif serait utilisé pour accompagner les transformations du premier cycle universitaire afin d'améliorer la formation initiale des jeunes.

C'est là un financement possible pour amorcer des parcours de formation en cybersécurité en lien avec la puissance publique.

7. Étendre le rôle de la réserve de cyberdéfense à la résolution de crises touchant les acteurs privés et augmenter le nombre et les compétences des réservistes en en faisant la promotion auprès des acteurs du secteur privé et de la recherche académique.

Constat :

Plusieurs réserves destinées au risque cyber ont été créées récemment. En mars 2018, le réseau de référents cybermenace de la Police Nationale a vu le jour. Rattaché à la sous-direction de la lutte contre la cybercriminalité (SDLC), il vise à sensibiliser les acteurs privés partenaires et à les alerter en cas de cyberattaque. De son côté, la réserve opérationnelle de cyberdéfense, lancée en mai 2016, est un réservoir de forces mobilisables en cas de crise majeure sur le territoire national. Elle comprendra 4 440 personnes en 2019, dont 40 postes permanents et 400 réservistes opérationnels composant le cœur du dispositif (dont 200 en région et outre-mer). Cette réserve a pour vocation d'intervenir principalement non seulement sur les réseaux du ministère de la Défense mais également au profit des OIV (opérateurs d'importance vitale), des administrations et de leurs sous-traitants. Elle a par exemple récemment été mobilisée dans le cadre de l'exercice interarmées de cyberdéfense (DEFNET). D'autre part, 4 000 réservistes citoyens sont mobilisables sur l'ensemble du territoire national.

Les recrutements pour la réserve opérationnelle ont débuté il y a deux ans et vont se poursuivre dans un contexte de montée en puissance humaine et de montée en puissance des capacités de formation. Une réflexion est en cours pour en augmenter le nombre tout en restant certain de leur expertise et de la confiance à leur accorder. L'objectif est de recruter des profils variés offrant à la réserve un large panel de compétences aussi bien en ingénierie, qu'en droit, management, R&D. Rappelons à ce propos que la Loi de programmation a consacré au domaine cyber, de 2014 à 2019, une enveloppe d'un milliard d'euros. La moitié de cette somme était alors consacrée aux investissements, en particulier de R&D, qui ont été multipliés par trois.

Ceci nous pousse naturellement à considérer le milieu de la recherche académique comme un réservoir de talents éventuel pour la réserve. L'ensemble des entités de recherche ainsi que les partenaires de recherche académique doivent être davantage impliqués dans l'écosystème cybersécurité national ; et la réserve de cyberdéfense est une structure existante, en besoin, qui pourrait les accueillir. Ceci est d'autant plus important que si la recherche en cybersécurité n'est pas maîtrisée à l'échelle de la France, alors la souveraineté risque de ne plus être assurée dans le temps long.

Recommandation :

Inclure les chercheurs volontaires au sein de la réserve de cyberdéfense aurait le double avantage de répondre au besoin humain grandissant de la réserve, et de nouer des collaborations entre la recherche académique et l'ensemble de l'écosystème cybersécurité (institutionnels, DGA, ANSSI…). Il faut donc communiquer directement auprès du monde académique pour mettre davantage en lumière la réserve de cyberdéfense.

Leur intégration ne nécessite d'ailleurs pas de statut particulier : leur entrée dans la réserve doit rester sur la base d'un volontariat. Une formation en amont serait un prérequis pour être opérationnel en cas de mobilisation. Dans cette hypothèse, les chercheurs peuvent être mobilisés en cas d'urgence, mais ils peuvent aussi être mis à contribution sur des aspects de recherche pour constituer des scénarios d'attaque et préparer la réaction. L'INRIA s'est ainsi dotée de laboratoires à haute sécurité informatique (LHS) à Nantes et Rennes afin d'accueillir des travaux de recherche destinés à sécuriser le réseau.

Au-delà du monde académique, nous proposons que des employés du secteur privé puissent eux aussi rejoindre plus généralement la réserve de cyberdéfense. Ceci suppose un soutien et un aménagement minimal de leurs ressources humaines et une communication accrue dans les entreprises. Mais les avantages sont nombreux : à la fois pour la réserve, qui bénéficierait de nouvelles passerelles avec les acteurs privés, d'ingénieurs et techniciens rompus à la gestion cyber en entreprise, mais aussi pour les entreprises. Celles-ci profiteraient de formations aux modes d'action et de planification valables en cas de crise pour des opérations militaires, et transposables au secteur privé.

En cas de crise, il faut néanmoins rester vigilant à la chaîne de commandement de ces réservistes issus du privé ; il n'est pas impossible qu'ils aient à intervenir chez des entreprises de leur secteur. L'ANSSI, relais accepté des entreprises, pourrait coordonner leur action. A défaut, c'est le RSSI de l'entreprise touchée, responsable opérationnel, qui pourrait être le point central de contact.

Au-delà du défi de la montée en capacité des compétences cyber, cette recommandation vise aussi à étendre le périmètre d'intervention de la réserve de cyberdéfense à la résolution de crise touchant les acteurs privés. Dans le cas très précis d'un « cyber ouragan » incapacitant des pans entiers de l'économie française, la réserve de cyberdéfense pourrait constituer un vivier de compétences pour déployer les actions de résolution de crise sur le territoire national. Agissant en tant qu'intermédiaire et organe coordonateur, l'ANSSI pourrait occuper un rôle de passerelle entre le monde de la cyberdéfense et celui des entreprises privées en cas de crise d'ampleur.

8. Proposer un cadre permettant aux acteurs privés de partager le personnel et leurs compétences avec leurs pairs en cas d'attaque.

Constat :

S'il existe aujourd'hui un manque de compétences cyber, celui-ci va s'amplifier dans les prochaines années. Les grands groupes, confrontés à de graves attaques l'année passée, ont déjà pu faire l'expérience des limites actuelles de leur effectif et des prestataires compétents lorsqu'une attaque généralisée se propage.

Pour contenir ces carences, nous avons proposé plus tôt dans ce rapport de mettre en place des formations initiales ciblées ; c'est là une mesure dont les bénéfices verront jour à moyen terme. Plus immédiatement, il faut considérer des manières nouvelles de trouver, lorsque la situation l'exige, des professionnels compétents.

La comparaison entre les ouragans cyber auxquels les entreprises seront de plus en plus confrontées et les états de catastrophe naturelle est ici légitime : lorsque la tempête Xynthia a touché l'Ouest de la France, des circuits de solidarité se sont naturellement mis en place pour répondre ponctuellement à la crise. Des entreprises, certaines ayant des missions de service public, ont mis à disposition une partie de leurs ressources.

C'est cet état d'esprit, fondé sur la solidarité, en particulier sectorielle, qui doit également primer dans le domaine de la cybersécurité. Il existe déjà des échanges réguliers entre RSSI de groupes différents, voire concurrents, mais trop souvent cette collaboration se cantonne au niveau d'échanges de bons procédés avec des refus de principe de la part des instances dirigeantes d'aller plus loin, même en situation critique.

Cette posture est défavorable à l'ensemble des secteurs et des entreprises susceptibles d'être attaqués, et il convient de la transformer.

Recommandation :

Nous proposons donc de mener ce changement de paradigme en mettant en place un cadre permettant aux acteurs privés de partager leur personnel en cas de grave attaque cyber, ingérable par leurs seules ressources.

Pour permettre une telle intervention, les conventions de mise à disposition et les dispositifs de détachement semblent être les plus appropriés. Contrairement au contrat de prestation, ceux-ci permettent le transfert de compétences vers une entreprise disposant déjà de la compétence requise, mais en quantité insuffisante, comme ce serait le cas lors d'une attaque majeure.

Évidemment, l'initiative viendrait de l'entreprise victime, en s'assurant que l'action de ces ressources supplémentaires reste coordonnée par le RSSI de l'entreprise touchée afin d'intervenir en accord avec les processus de l'entreprise et en limitant les problèmes de confidentialité. C'est bien ce que permet la convention de mise à disposition, qui prévoit un transfert du lien de subordination vers l'entreprise accueillante pour des motifs d'instruction et de contrôle uniquement.

Afin de souligner l'importance du respect de la confidentialité, un engagement de confidentialité pourra être signé entre les parties, en complément de la convention. À noter qu'une clause relative à la sous-traitance des données, précisant que les données à caractère personnel devront être supprimées après usage, devra être incluse afin de respecter le Règlement général sur la protection des données (RGPD).

La mise en œuvre de tels dispositifs s'anticipe : il faut définir une « force d'intervention rapide » préparée lors d'exercices de simulation afin de clarifier le partage des responsabilités et la chaîne de commandement. Ces passerelles, préparées et répétées, tracent le chemin pour des circuits de solidarité bien définis lorsqu'une crise cyber affectera ces entreprises. Il faut également rédiger ces contrats en amont. Deux options existent :

- un contrat tripartite, entre les deux entreprises et l'employé volontaire, à signer lorsque la crise survient ;

- une convention entre les deux entreprises, complétée d'un avenant entre la société mettant ses compétences à disposition et son employé.

Le principal enjeu de cette proposition réside donc plus dans le changement de posture qu'elle suppose que sur des difficultés juridiques, et le défi est de favoriser les conditions d'un environnement de confiance entre acteurs du secteur privé. Afin de sensibiliser les acteurs en amont, une charte pourrait être signée par les entreprises participantes, sur le modèle de la Charte de solidarité en situation d'exception signée entre les acteurs privés et le ministère de l'Intérieur[94].

Notre recommandation pourrait, lorsque les entreprises seront matures, s'élargir au partage de certaines données métier indispensables pour assurer la continuité de l'activité de la société en cas d'attaque. Elle peut sembler surprenante dans le cadre de la cyber-

[94] Ministère de l'Intérieur, « Charte de solidarité et d'exception » disponible sur ce lien : https://www.cics-org.fr/wp-content/uploads/2017/01/2016-12-05-Charte-task-force.pdf

sécurité mais des dispositifs qui s'en rapprochent peuvent exister dans d'autres secteurs. Dans les télécommunications, un parallèle pourrait être tiré avec le cas de l'itinérance à l'étranger du téléphone portable. L'appareil peut en effet se raccrocher à des réseaux maintenus par des opérateurs différents sans problème, mais en France lorsque l'opérateur auquel l'utilisateur est abonné est en panne, l'appareil ne bascule pas sur un autre réseau fonctionnel. Le secteur bancaire, aux États-Unis, est en avance avec l'existence d'un projet de mise en commun *(US Sheltered Harbor)* qui permettra à certaines banques américaines de partager leurs données et de pouvoir assurer une reprise sur les systèmes d'une autre banque sur des activités vitales (registre des comptes, distribution d'argent liquide…).

9. Renforcer la capacité d'échange opérationnelle de signatures d'attaques et d'informations sur les menaces *a minima* entre les entreprises stratégiques pour la nation, *via* une plateforme sécurisée d'échange opérée soit par l'État, soit par un ou des acteurs français majeurs de la cybersécurité et de confiance (avec une possible segmentation sectorielle).

Constat :

Des entreprises ne sont parfois prévenues de l'existence d'une menace que longtemps après le début d'une attaque, entraînant des conséquences potentiellement beaucoup plus importantes pour ces dernières. Des circuits d'échange d'information existent, notamment avec l'État, mais ils ne sont pour l'instant pas suffisamment efficaces et organisés.

Au sein de l'ANSSI, le CERT-FR *(« Computer Emergency Response Team »)* est le point de contact international privilégié pour tout incident de nature cyber touchant la France. Il apporte son soutien

aux institutionnels, aux collectivités et aux OIV (« Opérateur d'Importance Vitale ») en matière de gestion de crise.

Les moyens de détection d'attaques reposent essentiellement sur la disponibilité de « signatures » techniques caractérisant le mode opératoire des attaquants. Les entreprises et les administrations concernées opèrent donc actuellement le partage de ces informations par le truchement de l'ANSSI et d'acteurs privés spécialisés. Opérationnellement, des limites existent, en particulier pour assurer une circulation et une exploitation rapide de ces informations.

Certains groupes français ont créé des CERT locaux mobilisant leur écosystème : c'est le cas d'Airbus qui participe activement à un groupe de partage d'informations sensibles prolifique avec Boeing au sein de l'A-ISAC *(« Aviation – Information Sharing and Analysis Center »)* ou encore de la Société Générale ou de la BNP Paribas dans le monde bancaire.

Recommandation :

Nous proposons donc de renforcer la capacité d'échange opérationnelle de signatures d'attaques et d'informations sur les menaces entre les entreprises françaises stratégiques pour la nation, *via* une plateforme sécurisée d'échange opérée soit par l'État, soit par un ou des acteurs français majeurs de la cybersécurité et de confiance (avec une segmentation sectorielle). Cette structure pour échanger de l'information comblerait un manque flagrant aujourd'hui. L'ensemble des entreprises consultées s'accordent sur ce constat ; elles ne sont néanmoins pas encore parvenues à structurer cette piste, ne sachant pas si un pilotage par l'État est nécessaire.

C'est une recommandation qui présente un gain important à court terme tout en présentant un coût maîtrisé. Elle présente évidemment des difficultés, notamment celle de définir le groupe de confiance auquel le partage de l'information serait limité. Un découpage en termes de nationalité n'est par exemple pas toujours pertinent : l'A-ISAC cité précédemment rassemble ainsi Airbus et Boeing aux États-Unis pour limiter au maximum le risque à l'échelle internationale. Un cercle de confiance pourrait ainsi fonctionner par un système d'approbation exclusivement accordée par des participants déjà approuvés. La question technologique du choix de la plateforme arrive alors dans un second temps et n'est pas un frein ; plusieurs solutions existent.

Sur le modèle des organismes ISAC *(Information Sharing and Analysis Center),* sans but lucratif, cette plateforme pourrait être opérée par un organisme ou une association professionnelle dont l'adhésion serait payante pour professionnaliser le partage d'informations et le rendre opérationnel.

Insistons sur le fait qu'il n'y a pas lieu d'opposer les échanges entre l'ANSSI et les entreprises, qui restent indispensables, et ceux entre les entreprises. Des canaux de communication verticaux peuvent coexister avec des canaux plus horizontaux entre acteurs du même secteur d'activité. Encourager le multiplateforme pour multiplier les échanges peut introduire une dynamique positive qui se structurera à moyen terme.

Le principal enjeu est là encore culturel : il faut, par ces échanges, enclencher une dynamique de confiance, profitable à l'ensemble d'un secteur d'activité, pour que les cyberattaques, inévitables, ne soient plus vues comme des « maladies honteuses » qu'il s'agirait

de couvrir. Par nature sensible, les données échangées possèdent une valeur inhérente, l'un des défis de la structure opérant la plateforme sera de prévenir les dérives potentielles des individus souhaitant monétiser ces données.

Pouvoir répondre à des attaques larges et rapides

10. Mobiliser le tissu économique et l'État autour de l'intelligence artificielle pour détecter les attaques et réagir à la bonne vitesse (et sécuriser l'intelligence artificielle pour prévenir les dérives).

Constat :

Le rapport Villani fait état d'un important retard français dans l'utilisation de l'intelligence artificielle (IA) dans le domaine de la cybersécurité[95].

Pourtant les systèmes intégrant de l'IA se multiplient et ils ne sont pas toujours conçus pour prendre en compte les tentatives de détournement. Les attaques réussies se multiplient : trois grandes familles d'attaques sont aujourd'hui capables de détourner l'IA.

Les attaques par empoisonnement sont les premières : il s'agit de nourrir l'IA d'échantillons biaisés alors qu'elle est encore en période d'apprentissage pour en orienter les résultats. On peut citer en illustration la malheureuse expérience du chatbot « Tay » de Microsoft : la société avait créé un compte Twitter dont l'ensemble des messages reposait sur des algorithmes d'apprentissage automa-

[95] « Intelligence artificielle et cybersécurité : le retard français », LeMagIT, 2018.

tique. Celui-ci fut tellement surchargé de messages haineux de la part de comptes malintentionnés qu'il finit par reproduire leur comportement, générant ainsi des messages à connotation raciste.

Les attaques par illusion consistent à alimenter l'IA avec une image biaisée de la réalité sans que cela ne soit détectable à l'œil nu. Les attaques par inférence permettent de solliciter l'IA non pas pour en détourner l'usage mais pour en révéler le fonctionnement interne.

Si l'IA nécessite donc une vigilance particulière, il faut néanmoins noter qu'elle est aussi en capacité d'apporter des solutions pour sécuriser les systèmes et réseaux informatiques. Face à des attaques en mesure de faire tomber des milliers d'entreprises en quelques minutes, l'IA devient nécessaire pour détecter suffisamment tôt ces menaces et y réagir de manière automatique.

Recommandation :

Nous proposons donc de promouvoir l'utilisation de l'IA dans le domaine de la cybersécurité pour détecter les attaques suffisamment vite et rester en mesure de réagir avant que l'attaque ne se propage trop fortement.

Le rapport Villani souligne que la France compte parmi les quatre premiers pays au monde pour la production mondiale d'articles sur l'IA ; l'expertise est donc là. Cependant, le monde académique se divise encore entre les chercheurs spécialisés en IA et ceux focalisés sur la cybersécurité. Ces silos freinent l'avancée de technologies de détection avancées et automatisées, et il convient de les supprimer.

Il faut donc accélérer les investissements dans les technologies

d'apprentissage automatique associées à la cybersécurité pour être en mesure de répondre à des attaques larges et rapides.

Parallèlement, il faut anticiper les problèmes de sécurité que le développement de l'IA fera naître. Le rapport Villani mentionne d'ailleurs très clairement ces enjeux et propose même de confier une mission de veille et d'anticipation de ces menaces à l'ANSSI, l'agence nationale dédiée à la cybersécurité.

11. Définir une doctrine opérationnelle spécifique à l'échelle de l'État pour faire face à une attaque large (actions opérationnelles pour mobiliser les acteurs de l'écosystème cybersécurité dans le tissu économique privé, anticiper des actions pour isoler le pays d'Internet, pour communiquer auprès du grand public en cas de destruction des moyens de communication classiques, etc.).

Constat :

La définition d'une stratégie de communication et de réponse opérationnelle en cas d'attaque majeure est essentielle : le risque serait d'avoir des canaux d'actions et de communication strictement limités à l'ANSSI et aux OIV affectés. Mais le grand public ou la multitude d'entreprises touchées feraient également partie des victimes avec qui il faudrait communiquer. Dans cette situation, l'absence d'une stratégie de réponse et de communication solide pourrait mener à des conséquences plus graves en cas de panique générale.

En termes de communication, l'ANSSI participe déjà régulièrement aux exercices de crise du plan PIRANET, plan gouvernemental. Durant ces exercices, les scénarios joués présentent toujours des niveaux d'impacts très forts au niveau national, comme le secteur

de l'énergie paralysé, des transports inopérants, des émeutes généralisées… Ces exercices incluent systématiquement des volets de communication vers le grand public. Aussi, le scénario d'une cyberattaque fortement impactante nécessite une communication vers la population. Dans la revue stratégique de cyberdéfense, il est prévu de préparer ces questions dans les différentes instances de l'État à la fois au niveau du message à communiquer et au niveau du canal de communication.

Recommandation :

En cas de crise, la bonne coordination des acteurs locaux, l'endiguement des zones touchées et la communication auprès du public sont autant de volets qui doivent être adressés par l'État dans une doctrine opérationnelle qui permette de faire face à une attaque large.

La première priorité opérationnelle est d'identifier des relais au sein des entreprises qui soient des points privilégiés pour l'État sous toutes ses formes (pour l'ANSSI mais aussi pour les forces de l'ordre par exemple). Dans les grandes entreprises, identifier les RSSI comme acteurs de confiance pour créer un réseau immédiatement mobilisable en cas d'attaque majeure. Dans les petites et moyennes entreprises, un équivalent reste à inventer.

Une fois ces acteurs mobilisés, la deuxième priorité consiste à endiguer la menace. Nous recommandons la mise en place de procédures d'urgence pour isoler un site industriel, une entreprise ou certains territoires du réseau le temps que l'attaque soit contenue. L'existence d'un véritable « bouton rouge » est une solution d'urgence pour activer un fonctionnement en mode dégradé et protéger la population sans disséminer la menace.

Enfin, la communication auprès du grand public, prérogative de l'État, est indispensable en temps de crise pour rassurer la population et éviter la perte de confiance en les institutions, effet parfois spécifiquement recherché par les attaquants. Toujours dans la logique de fonctionnement en mode dégradé, des plans de communication de crise en cas de défaillance des moyens usuels doivent donc être préparés : TV, radio, Internet…

12. Inciter et donner un cadre aux entreprises sur la mise en place d'une stratégie de défense active mais sans sortir du cadre législatif en vigueur.

Constat :

La nature des attaques informatiques évolue et se complexifie : elles ne se contentent plus toujours de contourner les défenses en place mais s'efforcent parfois de se maintenir dans le système informatique visé sans déclencher immédiatement l'attaque. L'attaquant améliore ainsi sa connaissance de la victime pour préparer une seconde attaque plus large (vols de données etc.).

Face à des attaques qui s'adaptent, un nouveau concept émerge : la défense active. Elle vise à mettre en place une stratégie de défense dont le but est de réduire la menace ou de ralentir la progression de l'attaquant sans se limiter à son propre système informatique (en collectant de l'information sur l'attaquant par exemple) ou en agissant, dans le cadre légal, sur les outils utilisés par les attaquants.

Cette stratégie n'est pas à confondre avec la riposte directe (*hack back* en anglais) à laquelle la France s'oppose publiquement sur la scène internationale. Il existe en effet différents types de réponses possibles à une cyberattaque pour les entreprises s'inscrivant bien

dans un cadre légal : la saisie de serveurs ou noms de domaine utilisés de façon malveillante par exemple.

Recommandation :

Nous recommandons donc de cadrer l'usage de stratégies de défense active avec, par exemple, la parution d'un guide de réponse à incidents incluant des principes de défense active.

Ceci suppose un changement de posture des entreprises pour que les forces de l'ordre, par exemple, soient plus fréquemment sollicitées pour travailler avec les entreprises touchées. En situation de crise, les entreprises cherchent d'abord à se relever ou à s'isoler et non à rassembler des preuves et porter plainte. Or, les enquêtes numériques menées actuellement par la police restent trop souvent superficielles par manque d'éléments concrets provenant des victimes.

13. Imposer un label de cyberrésilience pour les équipements les plus à risque pour pouvoir continuer à agir en cas de crise et préserver les vies humaines. Cela doit s'inscrire dans un mouvement de responsabilisation des éditeurs et des fabricants en imposant des mesures de fonctionnement garanti même en cas de cyberattaque pour les équipements les plus sensibles (médicaux, industrie à risque, véhicule, radio des services de secours…) et ce malgré la compromission des réseaux IT/OT/IoT.

Constat :

Les équipements sensibles intègrent rarement des mesures de sécurité assurant leur fonctionnement même en cas de défaillance ou d'attaque sur leurs composants informatiques, en particulier pour ceux qui assurent des fonctions de sûreté. En parallèle, la présence de plus en plus forte des objets connectés va augmenter l'exposition aux risques.

Les attaques récentes ont prouvé qu'un danger sérieux pesait sur les systèmes embarqués et les équipements industriels. En réponse, certains groupes industriels consultés ont ainsi classifié chacun de ces équipements en fonction du risque de cyberattaque et du niveau de sensibilité dont il était l'objet. Ils ont partagé cette classification avec leurs sous-traitants et exigent maintenant un certain niveau de résilience adapté à chaque catégorie d'équipements. C'est en substance un label de mesure de la résilience des équipements partagés par la chaîne d'approvisionnement.

Parmi les critères retenus pour obtenir ce label figure l'existence d'un mode dégradé, c'est-à-dire un fonctionnement de survie, afin que l'équipement puisse continuer de fonctionner a minima malgré la compromission des systèmes ou des réseaux.

Recommandation :

Nous proposons de mettre en œuvre une démarche de labellisation des équipements les plus sensibles (médicaux, embarqués…) à l'échelle européenne, à l'instar du marquage CE, en imposant un fonctionnement de « survie » en cas de cyberattaques. C'est ce fonctionnement de sûreté, dans certains cas non-numérique (prenons l'exemple de la pédale de frein d'une voiture autonome), qui limite le danger en cas de défaillance des systèmes.

Notons que l'ANSSI analyse et certifie déjà de nombreux produits. Les entreprises initiant ce processus le font donc aujourd'hui pour entrer sur des marchés réglementés exigeant ces labels. Ces labels pourraient intégrer une notion de résilience.

Bien que cette recommandation se focalise spécifiquement sur les équipements sensibles, elle a pour vocation de se généraliser à tous

les fabricants et éditeurs de solutions dans l'optique de lancer une dynamique de fond de responsabilisation du marché. Ainsi, l'introduction d'une notion de responsabilité des sociétés mettant en circulation des équipements ou des logiciels non-sécurisés permettrait de niveler le marché par le haut en matière de cybersécurité et de sûreté de fonctionnement.

Une telle perspective ne peut se réaliser que sur le temps long compte tenu de la complexité du sujet à adresser et de la multitude d'acteurs, en particulier internationaux. Bien que ce rapport préconise un label de résilience à l'échelle européenne comme premier jalon, il est certain que pour appliquer cette dynamique de fond, il faudra mettre en œuvre un label à l'échelle internationale.

CONCLUSION

La cybersécurité est l'affaire de tous. Parce que la plupart de l'information des entreprises françaises et mondiales, petites et grandes, circule *via* des systèmes à la dépendance technologique forte (monopole de Microsoft sur les systèmes d'exploitation des postes de travail, prédominance des microprocesseurs Intel sur le marché…). Parce que l'interconnexion entre les systèmes d'information croît à mesure que les organisations externalisent leurs services, stockent leurs données sur des serveurs délocalisés *via* le *cloud*, ou intègrent de plus en plus d'objets connectés sur leurs réseaux. Parce que la mondialisation renforce ces deux mouvements d'uniformisation et d'interconnexion. Pour toutes ces raisons, la menace cyber est une menace systémique.

Dans ce contexte, il est nécessaire d'inciter les acteurs français à la solidarité et à la coopération afin d'augmenter la cyberrésilience de l'ensemble du tissu économique et des administrations. Or, si les grandes entreprises commencent à mieux réagir face à cette menace (même s'il reste une grande partie du chemin à parcourir), les plus petites, elles, peinent à se préparer aux enjeux qui se présentent à elles. Une partie de nos recommandations vise donc à permettre aux grands comptes et à une série d'acteurs (métiers du chiffre, éditeurs de logiciels et fournisseurs de services) de les aider à bénéficier des outils digitaux en toute sécurité (recommandations 2, 3, 4, 7 et 10).

La coopération doit également être mise en œuvre entre grands acteurs économiques. Il ne s'agit pas ici d'imaginer un monde utopique dans lequel les entreprises compromettraient leur avantage

compétitif. Notre objectif est plutôt d'appuyer un constat : les responsables de cybersécurité des entreprises ne peuvent pas opérer efficacement de manière isolée. Aujourd'hui, ils partagent l'information informellement. Nous pensons qu'encourager ces échanges en leur donnant un cadre augmentera la cyberrésilience des systèmes d'information de tous (recommandation 9). Par ailleurs, en situation de crise majeure, ce sont bien les intérêts économiques de la nation qui sont en jeu. Nous espérons que les acteurs économiques prennent la mesure de leur responsabilité pour soutenir les organisations touchées (recommandation 8). Bien sûr, ces propositions ne sont réellement efficaces que dans un contexte où les dirigeants et les conseils d'administration sont hautement sensibilisés à ces enjeux (recommandations 1, 5 et 12).

Enfin, la coopération et la solidarité sont également les affaires de l'État. Par exemple, la France manque cruellement de compétences dans le domaine numérique au sens large, et donc dans la cybersécurité. Nous pensons que l'État doit servir d'exemple en créant des parcours de formation en cybersécurité prestigieux qui permettent d'attirer et de former nos talents (recommandation 6). Dans l'ensemble, l'État doit être mieux préparé pour réagir à une attaque cyber sur le territoire national. Cela est d'autant plus vrai lorsque nous évoquons un scénario de « cyber ouragan » qui puisse avoir des conséquences graves sur la vie des citoyens (recommandations 11 et 13).

APT

Advanced Persistent Threat, désigne des acteurs menaçants ou des techniques de piratage employées par des acteurs menaçants pour s'introduire de manière discrète et furtive dans des systèmes hautement ciblés. Compte tenu de leur haut degré de sophistication, les APT sont souvent associés à des acteurs étatiques.

BGP

Border Gateway Protocol[96] est un protocole de routage qui permet à des systèmes autonomes d'échanger des informations sur les routes à emprunter pour établir une communication entre eux. Le BGP permet en quelque sorte de relier entre eux les systèmes qui assurent le fonctionnement d'Internet de façon globale. Un dysfonctionnement du BGP pourrait engendrer une coupure d'une partie de l'Internet.

Botnet

Issu de l'anglais « *robot* » et « *network* », un *botnet* désigne littéralement un réseau de robots informatiques. Le terme est usuellement employé pour désigner des réseaux de machines compromises, dites « machines zombies », qui sont à leur tour utilisées à des fins malveillantes. Les *botnets* sont par exemple utilisés pour réaliser des attaques DDoS.

Cloud

Le *cloud* ou l'informatique en nuage désigne la pratique de mettre en commun des « fermes » de serveurs informatiques et de les mettre à disposition à distance, *via* Internet par exemple, sous formes de services. Ces services peuvent prendre la forme de SaaS *(Software*

[96] Pour aller plus loin : https://tools.ietf.org/html/rfc4271

as a Service), de PaaS *(Platform as a Service)* ou de IaaS *(Infrastructure as a Service).* Ces services mis à disposition par un fournisseur varient selon le degré de responsabilité du fournisseur et du client. En SaaS, le fournisseur a la responsabilité de l'infrastructure, des systèmes d'exploitation et des logiciels applicatifs. Dans ce cas, les clients n'ont plus qu'à se connecter et utiliser les applications qui sont hébergées et entretenues à distance. A l'inverse, en IaaS, le fournisseur a la responsabilité du matériel, l'infrastructure et les couches basses uniquement.

Dark web

Souvent appelé « la face cachée d'Internet » ou encore « l'Internet parallèle », le *dark web* désigne l'ensemble des réseaux *(darknets)* qui s'appuient sur l'infrastructure d'Internet mais qui ne sont accessibles qu'à l'aide de logiciels spécifiques. Les utilisateurs du *dark web* y recherchent souvent la discrétion et l'anonymat. L'un des *darknets* les plus célèbres est sans nul doute le réseau Tor[97].

DDoS

Distributed Denial of Service est une attaque informatique par déni de service distribué, où le principe est de rendre indisponible un service à l'aide de nombreuses machines situées à des endroits différents. Les attaques DDoS les plus répandues consistent à inonder un service de requêtes, au-delà de la capacité de traitement de ce dernier afin de le rendre inopérant.

DNS

Domain Name System[98] est le service qui permet de traduire un nom de domaine, simple à manipuler par l'humain, en adresse IP, facile

[97] https://www.torproject.org/

[98] Pour aller plus loin : https://tools.ietf.org/html/rfc6895

à traiter par les machines. Les adresses IP peuvent ensuite être utilisées pour identifier les machines désignés.

Ethical hacker

Un hacker éthique, en français, ou parfois aussi désigné « *white hat* », désigne un professionnel de la sécurité informatique qui réalise des tests d'intrusion sur les systèmes d'information des organisations pour s'assurer de la sécurité et alerter en cas de découverte de vulnérabilités. Par opposition, un « *black hat* » désigne un hacker malintentionné. Il subsiste aussi une notion de moralité, si le hacker éthique agit dans la légalité et en toute moralité, le « *black hat* » ne suit pas de morale pour atteindre son objectif.

Faille « *zero-day* »

Une faille de type « *zero-day* » désigne une vulnérabilité sur un système qui n'est pas encore connue, ni de l'éditeur ni du public. Par définition, il n'existe donc pas de protection face à une faille de type « *zero-day* ».

Infogérance

L'infogérance désigne la gestion et l'exploitation de tout ou partie d'un système d'information par un prestataire informatique externalisé.

Microprocesseurs d'architecture x86

Les microprocesseurs d'architecture x86 désignent une famille de microprocesseurs utilisés dans la grande majorité des ordinateurs de bureau modernes et permettant de faire fonctionner les systèmes d'exploitation Windows, GNU/Linux ou encore Mac OS (depuis 2005).

Multi-tenant

Le *multi-tenant* ou multi-entité désigne un principe d'architecture informatique permettant à un système de servir plusieurs organisations clientes à partir d'une infrastructure commune. Le *multi-tenant* permet aux clients de bénéficier de sa propre instance tout en mutualisant les coûts de maintenance. Le degré de cloisonnement entre clients est toutefois différent selon la technologie employée.

SIS

Un système instrumenté de sécurité est un dispositif externe de réduction de risque, prévu pour assurer ou maintenir un état de sécurité de l'équipement industriel commandé par rapport à un événement dangereux spécifié (atteinte aux personnes, à l'environnement ou aux biens par exemple).

REMERCIEMENTS

L'Institut Montaigne remercie particulièrement les personnes suivantes pour leur contribution.

Président du groupe de travail

- **Marwan Lahoud,** associé, Tikehau Capital

Membres du groupe de travail

- **Pascal Andrei,** Chief Product Security Officer, Airbus
- **Alain Bernard,** directeur de la cybersécurité, L'Oréal
- **Laurent Collet-Billon,** chef de la direction générale de l'Armement de 2008 à 2017
- **Michael Fiey,** Chief Information Security Officer, ArcelorMittal Europe
- **Philippe Got,** senior business advisor, Wavestone
- **Eric Le Grand,** directeur de la prévention et de la protection du groupe, Renault
- **Jean-Philippe Naquet,** Group Chief Information Security Officer / responsable de la sécurité des systèmes d'information du Groupe, Total
- **Benoît Lemaire,** Head of Cybersecurity, SGS France
- **Olivier Nautet,** Head of IT Risk Management and Cybersecurity – Group Chief Information Security Officer, BNP Paribas
- **Emile Pérez,** directeur de la sécurité et de l'intelligence économique, Groupe EDF

- **Jean-Yves Poichotte,** directeur de la cybersécurité du groupe, Sanofi
- **Thierry Rouquet,** président et co-fondateur, Sentryo

Rapporteurs

- **Bilale Ahmimache,** ingénieur, Corps des Mines
- **Gérôme Billois,** partner cybersécurité et confiance numérique, Wavestone (rapporteur général)
- **Dominique Yang,** consultant cybersécurité et confiance numérique, Wavestone

Ainsi que :

- **Arthur Corbel,** assistant chargé d'études, Institut Montaigne
- **François Jolys,** assistant chargé d'études, Institut Montaigne
- **Théophile Lenoir,** chargé d'études, Institut Montaigne

Les personnes auditionnées ou rencontrées dans l'élaboration de ce travail :

- **Jean-Philippe Authier,** expert cybersécurité, Systemis
- **Florian Bachelier,** député LREM, co-président du groupe d'études sur la sécurité et la souveraineté numérique à l'Assemblée Nationale
- **Côme Berbain,** conseiller transformation numérique de l'État
- **Dominique Bolignano,** président fondateur, Prove&Run
- **Olivier Bonnet de Paillerets,** commandant de la Cyberdéfense (ComCyber), Ministère des Armées
- **Pierre-Olivier Brial,** directeur général délégué de Manutan et administrateur, METI

- **Agathe Cagé,** présidente de Compass Label, co-rapporteur de la Revue stratégique de cyberdéfense
- **Patrick Calvar,** directeur général de la sécurité intérieure de 2012 à 2017 et conseiller spécial de l'Institut Montaigne
- **Hélène Chauveau,** directrice des risques émergents, AXA
- **Gilles Daguet,** directeur général, ACE Management
- **Christian Daviot,** conseiller stratégie auprès du directeur général, ANSSI
- **Thierry Delville,** délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces, Ministère de l'Intérieur
- **Frédérick Douzet,** professeure à l'Institut français de géopolitique, Université Paris 8
- **Christiane Féral-Schuhl,** avocat associé, Feral-Schuhl / Sainte-Marie Associés
- **Eric Freyssinet, colonel,** chef de la mission numérique, Gendarmerie nationale
- **Aude Gery,** chercheure associée, GEODE
- **Jérôme Gossé,** Cyber Manager Continental Europe, Chubb
- **Patrick Guyonneau,** directeur technique, Direction générale de la sécurité intérieure
- **Estelle Hascoet,** analyste risques émergents, AXA
- **Claude Kirchner,** directeur de recherche émérite, Inria
- **Eric Lavertu,** directeur adjoint, Centre de crise et de soutien, Ministère de l'Europe et des Affaires Étrangères
- **Laurence Lemerle,** directrice risques techniques et cyber, AXA France
- **Valérie Levacque,** Chief Information Security Officer, Ariane Group

- **Ulrike Leyherr,** Head of PC Centre of Competence, Allianz
- **Georges Lotigier,** président, Vade Secure
- **Christophe Madec,** chargé de clientèle, expert Cyber, Bessé
- **Hugo Madeux,** directeur de l'unité sécurité, IBM
- **Cyril Magliano,** président-directeur général, Systemis
- **Nathalie Malicet,** expert-comptable commissaire aux comptes, vice-présidente de la Commission Numérique et Innovation, Compagnie Nationale des Commissaires aux Comptes (CNCC)
- **Sandy Matthews,** avocat senior, August Debouzy
- **Jean-Paul Mazoyer,** directeur général, Crédit Agricole Pyrénées Gascogne
- **Jean-Philippe Pages,** membre du comité de direction, Bessé
- **Dominique Perier,** expert-comptable commissaire aux comptes, président du comité technologique, Conseil Supérieur des Experts-Comptables
- **Guillaume Poupard,** directeur général, ANSSI
- **Christophe Quentel,** chef de la mission pour l'anticipation et les partenariats, Centre de crise et de soutien, Ministère de l'Europe et des Affaires étrangères
- **Henri Verdier,** directeur de 2015 à 2018, Direction interministérielle du numérique et du système d'information et de communication de l'État
- **Luc Vignancour,** Cyber and Crime Practice Leader, Marsh S.A.S.
- **Thomas Wilson,** Chief Risk Officer, Allianz

Les opinions exprimées dans ce rapport n'engagent ni les personnes précédemment citées ni les institutions qu'elles représentent.

LES PUBLICATIONS DE L'INSTITUT MONTAIGNE

- Partenariat franco-britannique de défense et de sécurité : améliorer notre coopération (novembre 2018)
- Sauver le droit d'asile (octobre 2018)
- Industrie du futur, prêts, partez ! (septembre 2018)
- La fabrique de l'islamisme (septembre 2018)
- Protection sociale : une mise à jour vitale (mars 2018)
- Innovation en santé : soignons nos talents (mars 2018)
- Travail en prison : préparer (vraiment) l'après (février 2018)
- ETI : taille intermédiaire, gros potentiel (janvier 2018)
- Réforme de la formation professionnelle : allons jusqu'au bout ! (janvier 2018)
- Espace : l'Europe contre-attaque ? (décembre 2017)
- Justice : faites entrer le numérique (novembre 2017)
- Apprentissage : les trois clés d'une véritable transformation (octobre 2017)
- Prêts pour l'Afrique d'aujourd'hui ? (septembre 2017)
- Nouveau monde arabe, nouvelle « politique arabe » pour la France (août 2017)
- Enseignement supérieur et numérique : connectez-vous ! (juin 2017)
- Syrie : en finir avec une guerre sans fin (juin 2017)
- Énergie : priorité au climat ! (juin 2017)
- Quelle place pour la voiture demain ? (juin 2017)
- Sécurité nationale : quels moyens pour quelles priorités ? (avril 2017)
- L'Europe dont nous avons besoin (mars 2017)
- Tourisme en France : cliquez ici pour rafraîchir (mars 2017)
- Dernière chance pour le paritarisme de gestion (mars 2017)
- L'impossible État actionnaire ? (janvier 2017)
- Un capital emploi formation pour tous (janvier 2017)
- Économie circulaire, réconcilier croissance et environnement (novembre 2016)
- Traité transatlantique : pourquoi persévérer (octobre 2016)
- Un islam français est possible (septembre 2016)
- Refonder la sécurité nationale (septembre 2016)
- Bremain ou Brexit : Europe, prépare ton avenir ! (juin 2016)
- Réanimer le système de santé - Propositions pour 2017 (juin 2016)
- Nucléaire : l'heure des choix (juin 2016)

- Un autre droit du travail est possible (mai 2016)
- Les primaires pour les Nuls (avril 2016)
- Le numérique pour réussir dès l'école primaire (mars 2016)
- Retraites : pour une réforme durable (février 2016)
- Décentralisation : sortons de la confusion / Repenser l'action publique dans les territoires (janvier 2016)
- Terreur dans l'Hexagone (décembre 2015)
- Climat et entreprises : de la mobilisation à l'action / Sept propositions pour préparer l'après-COP21 (novembre 2015)
- Discriminations religieuses à l'embauche : une réalité (octobre 2015)
- Pour en finir avec le chômage (septembre 2015)
- Sauver le dialogue social (septembre 2015)
- Politique du logement : faire sauter les verrous (juillet 2015)
- Faire du bien vieillir un projet de société (juin 2015)
- Dépense publique : le temps de l'action (mai 2015)
- Apprentissage : un vaccin contre le chômage des jeunes (mai 2015)
- Big Data et objets connectés. Faire de la France un champion de la révolution numérique (avril 2015)
- Université : pour une nouvelle ambition (avril 2015)
- Rallumer la télévision : 10 propositions pour faire rayonner l'audiovisuel français (février 2015)
- Marché du travail : la grande fracture (février 2015)
- Concilier efficacité économique et démocratie : l'exemple mutualiste (décembre 2014)
- Résidences Seniors : une alternative à développer (décembre 2014)
- Business schools : rester des champions dans la compétition internationale (novembre 2014)
- Prévention des maladies psychiatriques : pour en finir avec le retard français (octobre 2014)
- Temps de travail : mettre fin aux blocages (octobre 2014)
- Réforme de la formation professionnelle : entre avancées, occasions manquées et pari financier (septembre 2014)
- Dix ans de politiques de diversité : quel bilan ? (septembre 2014)
- Et la confiance, bordel ? (août 2014)
- Gaz de schiste : comment avancer (juillet 2014)
- Pour une véritable politique publique du renseignement (juillet 2014)

- Rester le *leader* mondial du tourisme, un enjeu vital pour la France (juin 2014)
- 1 151 milliards d'euros de dépenses publiques : quels résultats ? (février 2014)
- Comment renforcer l'Europe politique (janvier 2014)
- Améliorer l'équité et l'efficacité de l'assurance-chômage (décembre 2013)
- Santé : faire le pari de l'innovation (décembre 2013)
- Afrique-France : mettre en œuvre le co-développement Contribution au XXVI[e] sommet Afrique-France (décembre 2013)
- Chômage : inverser la courbe (octobre 2013)
- Mettre la fiscalité au service de la croissance (septembre 2013)
- Vive le long terme ! Les entreprises familiales au service de la croissance et de l'emploi (septembre 2013)
- Habitat : pour une transition énergétique ambitieuse (septembre 2013)
- Commerce extérieur : refuser le déclin Propositions pour renforcer notre présence dans les échanges internationaux (juillet 2013)
- Pour des logements sobres en consommation d'énergie (juillet 2013)
- 10 propositions pour refonder le patronat (juin 2013)
- Accès aux soins : en finir avec la fracture territoriale (mai 2013)
- Nouvelle réglementation européenne des agences de notation : quels bénéfices attendre ? (avril 2013)
- Remettre la formation professionnelle au service de l'emploi et de la compétitivité (mars 2013)
- Faire vivre la promesse laïque (mars 2013)
- Pour un « New Deal » numérique (février 2013)
- Intérêt général : que peut l'entreprise ? (janvier 2013)
- Redonner sens et efficacité à la dépense publique 15 propositions pour 60 milliards d'économies (décembre 2012)
- Les juges et l'économie : une défiance française ? (décembre 2012)
- Restaurer la compétitivité de l'économie française (novembre 2012)
- Faire de la transition énergétique un levier de compétitivité (novembre 2012)
- Réformer la mise en examen Un impératif pour renforcer l'État de droit (novembre 2012)
- Transport de voyageurs : comment réformer un modèle à bout de souffle ? (novembre 2012)

- Comment concilier régulation financière et croissance : 20 propositions (novembre 2012)
- Taxe professionnelle et finances locales : premier pas vers une réforme globale ? (septembre 2012)
- Remettre la notation financière à sa juste place (juillet 2012)
- Réformer par temps de crise (mai 2012)
- Insatisfaction au travail : sortir de l'exception française (avril 2012)
- Vademecum 2007 – 2012 : Objectif Croissance (mars 2012)
- Financement des entreprises : propositions pour la présidentielle (mars 2012)
- Une fiscalité au service de la « social compétitivité » (mars 2012)
- La France au miroir de l'Italie (février 2012)
- Pour des réseaux électriques intelligents (février 2012)
- Un CDI pour tous (novembre 2011)
- Repenser la politique familiale (octobre 2011)
- Formation professionnelle : pour en finir avec les réformes inabouties (octobre 2011)
- Banlieue de la République (septembre 2011)
- De la naissance à la croissance : comment développer nos PME (juin 2011)
- Reconstruire le dialogue social (juin 2011)
- Adapter la formation des ingénieurs à la mondialisation (février 2011)
- « Vous avez le droit de garder le silence… » Comment réformer la garde à vue (décembre 2010)
- Gone for Good? Partis pour de bon ? Les expatriés de l'enseignement supérieur français aux États-Unis (novembre 2010)
- 15 propositions pour l'emploi des jeunes et des seniors (septembre 2010)
- Afrique - France. Réinventer le co-développement (juin 2010)
- Vaincre l'échec à l'école primaire (avril 2010)
- Pour un Eurobond. Une stratégie coordonnée pour sortir de la crise (février 2010)
- Réforme des retraites : vers un big-bang ? (mai 2009)
- Mesurer la qualité des soins (février 2009)
- Ouvrir la politique à la diversité (janvier 2009)
- Engager le citoyen dans la vie associative (novembre 2008)
- Comment rendre la prison (enfin) utile (septembre 2008)

- Infrastructures de transport : lesquelles bâtir, comment les choisir ? (juillet 2008)
- HLM, parc privé
  Deux pistes pour que tous aient un toit (juin 2008)
- Comment communiquer la réforme (mai 2008)
- Après le Japon, la France…
  Faire du vieillissement un moteur de croissance (décembre 2007)
- Au nom de l'Islam… Quel dialogue avec les minorités musulmanes en Europe ? (septembre 2007)
- L'exemple inattendu des Vets
  Comment ressusciter un système public de santé (juin 2007)
- Vademecum 2007-2012
  Moderniser la France (mai 2007)
- Après Erasmus, Amicus
  Pour un service civique universel européen (avril 2007)
- Quelle politique de l'énergie pour l'Union européenne ? (mars 2007)
- Sortir de l'immobilité sociale à la française (novembre 2006)
- Avoir des *leader*s dans la compétition universitaire mondiale (octobre 2006)
- Comment sauver la presse quotidienne d'information (août 2006)
- Pourquoi nos PME ne grandissent pas (juillet 2006)
- Mondialisation : réconcilier la France avec la compétitivité (juin 2006)
- TVA, CSG, IR, cotisations…
  Comment financer la protection sociale (mai 2006)
- Pauvreté, exclusion : ce que peut faire l'entreprise (février 2006)
- Ouvrir les grandes écoles à la diversité (janvier 2006)
- Immobilier de l'État : quoi vendre, pourquoi, comment (décembre 2005)
- 15 pistes (parmi d'autres…) pour moderniser la sphère publique (novembre 2005)
- Ambition pour l'agriculture, libertés pour les agriculteurs (juillet 2005)
- Hôpital : le modèle invisible (juin 2005)
- Un Contrôleur général pour les Finances publiques (février 2005)
- Les oubliés de l'égalité des chances
  (janvier 2004 - Réédition septembre 2005)

Pour les publications antérieures se référer à notre site internet :
www.institutmontaigne.org

INSTITUT
MONTAIGNE

ABB FRANCE
ACCURACY
ADIT
AIR FRANCE - KLM
AIRBUS GROUP
ALLEN & OVERY
ALLIANZ
ALVAREZ & MARSAL FRANCE
ARCHERY STRATEGY CONSULTING
ARCHIMED
ARDIAN
ASTRAZENECA
A.T. KEARNEY
AUGUST DEBOUZY
AXA
BAKER & MCKENZIE
BANK OF AMERICA MERRILL LYNCH
BEARINGPOINT
BESSÉ
BNI FRANCE ET BELGIQUE
BNP PARIBAS
BOLLORÉ
BOUYGUES
BPCE
BRUNSWICK
CAISSE DES DÉPÔTS
CAPGEMINI
CAPITAL GROUP
CARBONNIER LAMAZE RASLE & ASSOCIÉS
CAREIT
CARREFOUR
CASINO
CGI FRANCE
CHAÎNE THERMALE DU SOLEIL
CHUBB
CIS
CISCO SYSTEMS FRANCE
CMA CGM
CNP ASSURANCES
COHEN AMIR-ASLANI
COMPAGNIE PLASTIC OMNIUM
CONSEIL SUPÉRIEUR DU NOTARIAT
CRÉDIT AGRICOLE
CRÉDIT FONCIER DE FRANCE
D'ANGELIN & CO. LTD
DENTSU AEGIS NETWORK
DE PARDIEU BROCAS MAFFEI
DRIVE INNOVATION INSIGHTS - DII
EDF
ELSAN
ENGIE
EQUANCY
EURAZEO
EUROGROUP CONSULTING
EURODISNEY
EUROSTAR
FONCIÈRE INEA
GALILEO GLOBAL EDUCATION FRANCE
GIDE LOYRETTE NOUEL
GOOGLE
GRAS SAVOYE
GROUPAMA
GROUPE EDMOND DE ROTHSCHILD
GROUPE M6
GROUPE ORANGE
HAMEUR ET CIE
HENNER
HSBC FRANCE
IBM FRANCE
IFPASS
ING BANK FRANCE
INSEEC
INTERNATIONAL SOS
IONIS EDUCATION GROUP
ISRP
JEANTET ASSOCIÉS
KANTAR
KPMG S.A.
LA BANQUE POSTALE
LA PARISIENNE ASSURANCES

SOUTIENNENT L'INSTITUT MONTAIGNE

INSTITUT
MONTAIGNE

LAZARD FRÈRES
LINEDATA SERVICES
LIR
LIVANOVA
LVMH - MOËT-HENNESSY - LOUIS VUITTON
MACSF
MALAKOFF MÉDÉRIC
MAREMMA
MAZARS
MCKINSEY & COMPANY FRANCE
MÉDIA-PARTICIPATIONS
MEDIOBANCA
MERCER
MERIDIAM
MICHELIN
MICROSOFT FRANCE
MNH GROUP
NATIXIS
NESTLÉ
OBEA
ODDO BHF
ONDRA PARTNERS
OPTIGESTION
ORANO
ORTEC GROUP
PAI PARTNERS
PIERRE ET VACANCES
PRICEWATERHOUSECOOPERS
PRUDENTIA CAPITAL
RADIALL
RAISE
RAMSAY GÉNÉRALE DE SANTÉ
RANDSTAD
RATP
RENAULT
REXEL
RICOL, LASTEYRIE CORPORATE FINANCE
RIVOLIER
ROCHE
ROLAND BERGER
ROTHSCHILD MARTIN MAREUL
SAFRAN
SANTÉCLAIR
SCHNEIDER ELECTRIC
SERVIER
SGS
SIA PARTNERS
SIACI SAINT HONORÉ
SIEMENS
SIER CONSTRUCTEUR
SNCF
SNCF RÉSEAU
SODEXO
SOLVAY
SPRINKLR
SUEZ
SYSTEMIS
TECNET PARTICIPATIONS SARL
TEREGA
THE BOSTON CONSULTING GROUP
TILDER
TOTAL
UBS FRANCE
VEOLIA
VINCI
VIVENDI
VOYAGEURS DU MONDE
WAVESTONE
WENDEL
WILLIS TOWERS WATSON
WORDAPPEAL

SOUTIENNENT L'INSTITUT MONTAIGNE

Imprimé en France
Dépôt légal : novembre 2018
ISSN : 1771-6756
Achevé d'imprimer en novembre 2018

INSTITUT
MONTAIGNE

INSTITUT
MONTAIGNE

IL N'EST DÉSIR PLUS NATUREL QUE LE DÉSIR DE CONNAISSANCE

Cybermenace : avis de tempête

Comme tous les pays, la France est aujourd'hui susceptible d'être frappée par une cyberattaque majeure. L'interconnexion des technologies et des entreprises, la numérisation de l'économie, ou encore le fait que les systèmes d'information dépendent d'un petit nombre d'acteurs laissent planer le risque d'un « cyber ouragan ».

Afin de faire face à ce défi inédit, l'Institut Montaigne a travaillé avec les grands groupes industriels, les PME et ETI ainsi que les universités, pour comprendre la nature du risque et identifier les solutions qui s'offrent à nous.

De ces réflexions découle un besoin vital de coopération et de solidarité entre acteurs privés d'une part, et entre acteurs privés et publics d'autre part, afin d'anticiper et d'identifier ces attaques ainsi que de limiter leurs effets sur les systèmes d'information français.

Institut Montaigne
59, rue La Boétie - 75008 Paris
Tél. +33 (0)1 53 89 05 60 – www.institutmontaigne.org

10 €
ISSN 1771-6764
Novembre 2018