CYBER : UNE QUESTION DE SOUVERAINETÉ

LA QUATRIÈME DIMENSION DE L'ESPACE NATIONAL

Un Livre blanc avec 30 propositions et le Projet CYBUNIH

OUVRAGE COLLECTIF DE LA COMMISSION CYBER-STRATÉGIE

UNION DES ASSOCIATIONS D'AUDITEURS DE L'INSTITUT DES HAUTES ÉTUDES DE DÉFENSE NATIONALE

Note pour les lecteurs

Ce texte est mis en page de manière à permettre à ceux qui le souhaitreraient de faire une impression recto-verso de tout ou partie de ce document, d'où quelques pages paires (verso) blanches, précédant des débuts de chapitre.

Avertissement lexical

L'élément lexical cyber est naturellement omniprésent dans ce document (il figure 700 fois). Il est utilisé nominativement « le cyber » pour désigner l'ensemble du domaine. Il a aussi souvent le rôle d'un adjectif qualificatif « le risque cyber ». Mais on trouve le plus fréquemment ce groupe comme préfixe dans une multitude de néologismes. La graphie de ces néologismes n'est pas encore fixée par l'usage, on trouve indifféremment dans la littérature et selon les termes l'usage du trait-d'union ou la forme agglutinative, plus aboutie (cyber-risque, cyberattaque). Nous avons pris le parti dans ce document d'utiliser systématiquement le trait-d'union, seule solution qui convienne à l'ensemble des cas rencontrés. L'usage permettra progressivement de sélectionner pour chaque néologisme une graphie. Naturellement, ceci ne s'applique pas au terme cybernétique, fréquemment utilisé, mot dans lequel cyber n'est pas un préfixe mais le cœur du mot.

École Militaire, 1 place Joffre, case courrier 41, 75700 Paris SP 07
delegation.union.ihedn@gmail.com

Ouvrage collectif sous la direction de Julien ROITMAN

Pilotes des groupes de travail de la Commission cyber-stratégie

Sébastien BOURDON, Pierre-Guillaume GOURIO-JEWELL, Guillaume JEUNOT, Ali MLALA, Didier SPELLA, Patrick VABRE, Julien VALIENTE

Autres rédacteurs ayant participé à l'élaboration de ce Livre blanc

Élise ACQUIN, Céline BOYARD, Gabriel BREIT, Marius CAMPOS, Laurent CHABAUD, Thierry COLOMBIER, Julien ESTEBANEZ, Véronique GUEVEL, François GUYOT, Christine HAGET, Emmanuelle HERVE, Olivier LASMOLES, Vincent LE DILASSER Jean-Claude LEBRESNE, Patrick LHEUREUX, Olivier LYS, Jean- Paul MATTEI, Cédrick MORMANN, Marie-Hélène PEBAYLE, Pierre UZAN, Justine VAN MINDEN, Marc WELTMANN

Mise en page finalisée par François GUYOT et François LEFAUDEUX

Remerciements

Jamal BASRIRE, Marguerite BILALIAN, CYB-RI (ILERI), CINOV Numérique (Olivier LYS), Fanny DEMASSIEUX, Thomas ESTÈVE, Sophie FUCHS, Simond de GALBERT, Caroline GORSE-COMBALAT, Pierre GUYOT, Philippe LAVAULT, Pauline LOURADOUR, Jean-François MOREL, Maxime OLIVA, Jacqueline PASDELOUP, Mohand RAMTANI, Jacques ROUDIER, Philippe TELEP, Philippe TROUCHAUD

Préface

Une part croissante de nos vies se joue désormais dans le cyber-espace. Dans tous les domaines, cette nouvelle donne technologique est porteuse d'opportunités inédites, mais aussi de menaces nouvelles. Au cours des dernières années, on a vu des acteurs mal intentionnés, parfois des États, se livrer à des actes d'espionnage et de déstabilisation qui, pour être cyber, n'en étaient pas moins caractérisés. Les préoccupations que de tels actes n'ont pas manqué de susciter n'avaient, à juste titre, rien de virtuel.

Demain, les technologies du quotidien pourraient s'avérer aussi préjudiciables à la bonne marche de nos entreprises, de nos services publics et de nos institutions démocratiques que les plus spectaculaires de ces cyber-attaques. Si nous n'y prenons garde, le déploiement de la 5G, l'essor de l'informatique en cloud (nuage) et le développement de l'intelligence artificielle risquent, en effet, d'ouvrir de véritables brèches dans notre sécurité numérique et d'inscrire, dans le plus banal de nos gestes, la menace d'une vulnérabilité nouvelle.

Face à cette rupture stratégique majeure, la France s'emploie à construire, à tous les niveaux pertinents et avec l'ensemble de ses partenaires européens et internationaux, une réponse globale capable de parer à toute la gamme des atteintes de sécurité et de souveraineté auxquelles nous sommes exposés.

Une politique nationale ambitieuse pour garantir notre cyber-sécurité

L'enjeu n'est pas seulement d'appuyer les efforts mis en œuvre par l'Agence nationale de la sécurité des systèmes d'information pour garantir la sécurité des Français et l'intégrité de nos infrastructures. Il s'agit aussi de préserver, dans la durée, notre liberté de faire nos propres choix et notre capacité à agir conformément à ces choix. Car, au XXIe siècle, la souveraineté est aussi numérique, ou elle n'est pas.

Tout en poursuivant le renforcement des capacités cyber de nos armées préconisé par la Revue stratégique de cyberdéfense de 2018 et acté par la dernière loi de programmation militaire, nous avons fixé une doctrine claire en matière de lutte informatique défensive et offensive, dans le respect du droit international.

Une souveraineté numérique européenne

Dans un monde cyber-structuré par la compétition que se livrent quelques grandes puissances, et notamment les États-Unis, la Russie et la Chine, nous ne saurions vraiment défendre

la souveraineté de notre pays qu'en bâtissant, avec nos partenaires et avec les institutions européennes, une souveraineté commune des Européens. Face à ceux qui voudraient faire de notre continent leur terrain de jeu numérique, nous devons parler d'une même voix et, surtout, agir ensemble. Si nous voulons rester acteurs de notre propre destin, un sursaut de souveraineté est indispensable. Dans bien des domaines, l'Europe commence à sortir de la naïveté et de l'innocence. Il est temps qu'elle s'y emploie aussi sur les questions numériques, forte du modèle singulier dont elle a commencé à jeter les bases, pour échapper au double écueil de l'autoritarisme et du laisser-faire.

Tout en travaillant à renforcer notre niveau global de cyber-sécurité, il est urgent que nous nous donnions les moyens de consolider notre rôle de puissance normative et de puissance d'innovation. Au sein de l'Union comme sur la scène internationale, nous devons travailler à donner corps à ce principe fondamental : le numérique est un bien commun, qu'il est indispensable de mettre à l'abri de toute tentative de confiscation et dont la régulation est l'affaire de tous.

La France et l'Europe à l'initiative pour la régulation multilatérale du numérique

C'est pourquoi les défis numériques sont au cœur du nouveau multilatéralisme que nous défendons, à titre national et entre Européens, aux Nations unies, à l'OCDE, au G7, au G20 et dans le cadre de l'Alliance pour le multilatéralisme, en veillant à donner voix au chapitre à l'ensemble des acteurs concernés – des organisations de la société civile aux entreprises du secteur privé. Car la gouvernance numérique mondiale ne saurait se mettre en place sans eux.

Le succès rencontré par ces initiatives, en particulier l'Appel de Paris pour la confiance et la sécurité dans le cyber-espace, en témoigne : nous sommes une majorité, sur la scène internationale, à refuser de vivre dans une jungle 2.0 régie par la loi du plus fort. À nous, maintenant, d'en tirer toutes les conséquences pour inventer, en commun, les règles du vivre-ensemble numérique.

Je forme le vœu que ce Livre blanc puisse nourrir la réflexion de tous ceux qui, chacun dans ses fonctions, veillent à la sécurité et à la souveraineté de notre pays et je salue la Commission cyber-stratégie de l'Union-IHEDN, qui a mené à bien ce projet dont j'espère qu'il pourra également éclairer nos concitoyens sur un sujet si important pour leur avenir.

Jean-Yves LE DRIAN
Ministre de l'Europe et des affaires étrangères

Avant-propos

« La dimension cyber de la sécurité de la France est de première importance. Si son aspect global relève de la responsabilité de l'État, elle intéresse également la défense des intérêts des citoyens comme ceux des entreprises : préservation de la vie privée, protection des données et de leur accès dans un contexte de compétition économique et médiatique mondiale, mise en place de parades à la vulnérabilité des infrastructures, développement d'une résilience permettant la continuité des opérations et une reprise rapide, élaboration d'une capacité de riposte »[1].

Il pourra sembler téméraire que d'anciens auditeurs du CHEAr (aujourd'hui 3AED) et de l'IHEDN osent s'attaquer à la rédaction d'un Livre blanc sur la souveraineté cyber, alors que des organismes publics, autrement plus compétents et mieux pourvus, traitent déjà ce domaine au titre de leur mission. Il faut toutefois se souvenir que la vocation de l'Union-IHEDN qui regroupe ces auditeurs et leurs associations, est de contribuer au renforcement de la cohésion nationale par la promotion au sein de la Nation d'une culture de défense et de sécurité. Il nous a donc semblé pertinent d'apporter au débat le point de vue de la commission cyber-stratégie, tout particulièrement à une époque où il est de bon ton de consulter le citoyen de base sur les réponses à donner aux grands défis du moment.

Constituée d'une quarantaine d'auditeurs délibérément recrutés dans toutes les régions et issus des horizons professionnels les plus divers, la commission s'est donné comme objectif de *« stimuler et fédérer des initiatives dans le domaine cyber, d'en identifier les grands thèmes et les axes de progrès, de dégager des recommandations à faire connaître et appliquer »*[2]. S'en est suivi un important travail de réflexion dont les premières conclusions et propositions sont regroupées dans cet ouvrage, qui devrait en principe se prolonger par une mobilisation nationale sur le terrain d'anciens auditeurs, en vue d'aider à titre bénévole à sensibiliser au cyber dans toutes les Régions les segments les plus vulnérables de la population.

Afin d'apporter une réelle valeur ajoutée, nous avons choisi de jouer les Candide en essayant d'aborder sous un angle nouveau, voire naïf, différents aspects de la stratégie cyber, et d'y contribuer en apportant une vision originale avec un accent mis plutôt sur l'économique, le culturel, le sociétal et le politique que sur le militaire ou la technologie, domaines très spécifiques et déjà largement couverts. De même, convaincus que la richesse des contenus résulte de la diversité des participants, nous avons souhaité réunir un nombre important de contributeurs

1 Lettre de mission du président Mario Faure 22 décembre 2017

2 idem note

ayant des analyses et des points de vue différents, et donné sans doute ainsi un petit côté patchwork à ce Livre blanc qui a vocation à éclairer et à proposer, plutôt qu'à édifier un monument universitaire.

L'ouvrage s'articule autour des éléments de réponse que nous avons tenté d'apporter à plusieurs questions : Qu'est vraiment le cyber ? Quelle est sa problématique ? Qui en sont les protagonistes en France et à l'international ? Qu'en est-il de l'entreprise ? Qu'en est-il de l'Administration ? Où en est la France ? Où en sera-t-on dans quinze ans ? Que faire à court terme ? Que faire à moyen terme ? Regroupées sous le titre « *Cyber : une question de souveraineté — La quatrième dimension de l'espace national* », nos observations débouchent sur trente propositions à l'intention des pouvoirs publics et des décideurs privés. Ce Livre blanc n'est sans doute d'ailleurs que le début d'une longue série, dans la mesure où l'évolution permanente de la donne cyber et des moyens nécessaires pour la maîtriser imposera de toute évidence des mises à jour périodiques.

En matière de numérique comme ailleurs, la souveraineté est la capacité à exercer une autorité et à défendre un espace sur lequel on revendique des droits. Le cyber, quatrième dimension de l'espace national, ne fait pas exception à la règle — avec une différence toutefois : par-delà les responsables à qui sont habituellement confiées les missions régaliennes de l'État, chacun des 67 millions d'habitants de la France est un acteur de la sécurité cyber. Comme il en constitue le maillon faible, c'est clairement l'homme et son éducation à cette discipline qui doivent être au cœur de la réflexion et de l'action future : l'ampleur du défi impose de faire évoluer l'ADN français pour le rendre cyber-résistant sans attendre d'y être contraint par les circonstances. C'est l'affaire d'une génération, vingt ans d'efforts au moins, mais c'est réalisable et il faut commencer sans attendre, en s'attachant en priorité aux jeunes, aux PME/PMI/TPE et aux petits organismes territoriaux, segments de population dont notre travail de réflexion et de recherche a mis en lumière la vulnérabilité cyber.

La crise sanitaire, politique, sociale et économique dans laquelle la pandémie de Covid-19 vient de plonger la planète n'a fait que renforcer la dépendance au numérique de chacun, organisations comme individus, avec les MOOC, visio-conférences, télétravail… et accentué notre fragilité en la matière. Selon certains d'ailleurs[3] « le prochain virus sera cyber » et il faut s'y préparer.

D'où notre proposition de capitaliser à travers leurs associations sur les 10 000 anciens auditeurs que leur passage par l'IHEDN ou le CHEAr (AED) a sensibilisés aux questions de défense, et dont l'activité s'exerce au meilleur niveau dans les domaines les plus variés comme dans toutes les géographies. L'idée est de leur proposer, sur une base de volontariat, de restituer à

3 Alain Bauer – 24 avril 2020

la Nation un peu de ce qu'ils en ont reçu : on les ferait participer à un déploiement terrain de sensibilisation cyber de ces populations, en complète coordination avec les entités publiques en charge de la couverture sécurité cyber du territoire : triptyques régionaux gendarmerie-ANSSI-Comcyber, mais aussi ACYMA et CNIL, et en appui de leurs opérations.

Le cyber est à l'armement classique ce que le smartphone est au tam-tam. Comment mieux garantir la souveraineté de la France qu'en faisant du développement et de la sécurité cyber sous tous ses aspects une priorité nationale dans la durée ? Cette volonté politique que nous appelons de nos vœux pourrait se traduire par la création d'un ministère d'État chargé, comme c'est déjà le cas au niveau européen, de la politique industrielle, de l'innovation et du numérique. Demain se prépare aujourd'hui.

Julien ROITMAN
Président de la commission cyber-stratégie de l'Union-IHEDN

Sommaire

Chapitre I

qu'est-ce que le Cyber ?

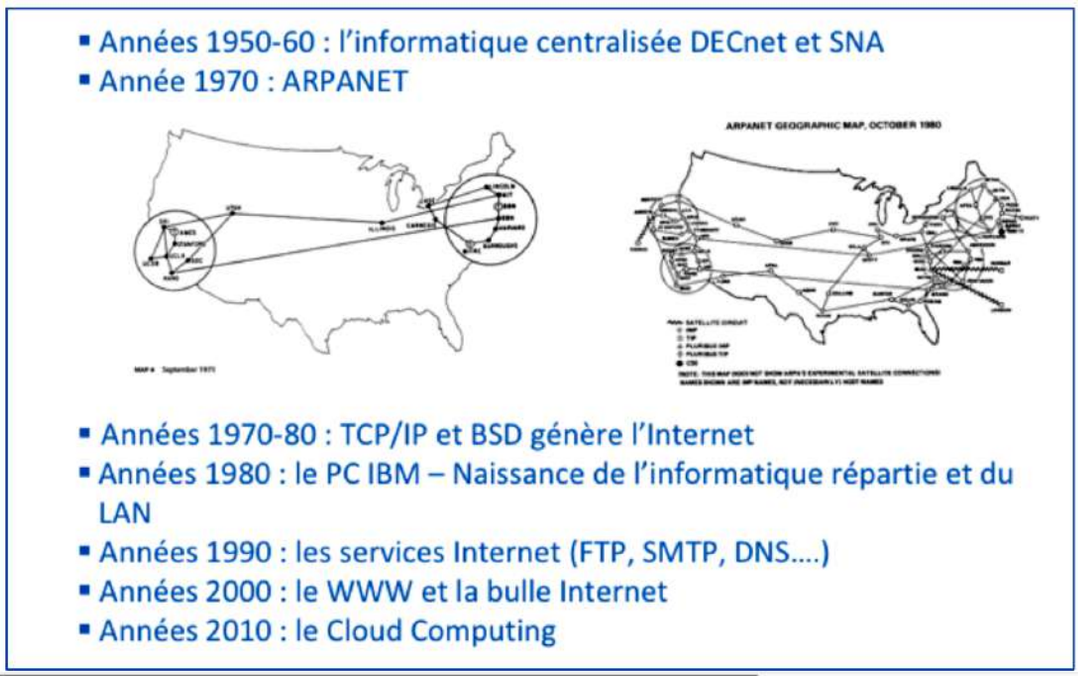
Le préfixe cyber vient du mot grec *kubernêtikê* signifiant « gouvernail ». Transposé dans la sphère informatique et réseaux par le terme cybernétique : il désigne la science des commandes et du contrôle. Le terme de cyber-espace désigne, d'après le Petit Robert, un « ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs. » Il est traduit de l'anglais cyberspace (contraction des termes Cybernetics et Space), néologisme et buzzword, apparu au début des années 1980 dans une nouvelle de William Gibson.

On retrouve ce préfixe dans la littérature et le cinéma, notamment en science-fiction. La cybernétique (terme inventé en 1948 par le mathématicien Norbert Wiener) nourrit tout un univers imaginaire et fantastique de guerre entre des hommes et des machines. Le cyberpunk, genre littéraire qui aborde les thématiques du hacker, de l'intelligence artificielle et des multinationales. Il se déroule la plupart du temps sur Terre dans un futur proche. Aujourd'hui entre réalité et science-fiction le fil s'amenuise…

Actuellement, il est courant de parler de cyber-attaques, de cyber-sécurité, de cyber-criminalité. Mais le cyber apparaît aussi dans notre quotidien au travers de lieux physiques comme les cyber-cafés ou les cyber-espaces (espaces qui donnent accès à des formations à l'Internet et aux nouvelles technologies).

Les origines : Internet

Plongeons dans l'histoire et retrouvons-nous en pleine guerre froide. Les militaires américains se voient poser une question cruciale dans le conflit qui les oppose à l'URSS : comment garantir les moyens de communication si jamais plusieurs de leurs bases étaient détruites, comment assurer la coordination des déclenchements des armes nucléaires en cas de guerre atomique ? La réponse apparaît au début des années mille neuf cent soixante avec le premier réseau de communication distribué, baptisé ARPANET. Il est opérationnel en 1969 : les ordinateurs peuvent enfin communiquer entre eux malgré de longues distances.



Source : Edition ENI - support de cours

Ensuite, tout s'accélère. Le civil, à travers les universités, développe également son réseau, et en 1989 Tim Berners-Lee conçoit la base de ce qui va devenir le *World Wide Web*. Le terme « d'Internet », dérivé du concept d'internetting ou « interconnexion des réseaux » se vulgarise. Internet est aujourd'hui un réseau informatique mondial accessible au public. Il est composé de millions de réseaux distribués aussi bien publics que privés, universitaires, commerciaux ou gouvernementaux, qui peuvent être eux-mêmes regroupés en réseaux autonomes. Le socle d'infrastructures et de protocoles propice au cyber-espace est né.

LE CYBER-ESPACE, UN ENSEMBLE DE SERVICES

Si Internet a connu un tel essor, c'est que les services qu'il a rendu possibles ont trouvé leur application dans notre quotidien. Le réseau Internet est basé sur des architectures comme OSI *(Open Systems Interconnection)* défini par l'ISO *(International Organization for Standardization)*, et des protocoles comme TCP/IP[4] pour fonctionner. Mais pour les utilisateurs, Internet est avant tout un support pour de nombreux services qui permettent un large usage. Le plus connu peut-être, souvent confondu avec Internet, est le World Wide Web qui permet de naviguer de page en page en cliquant sur des liens grâce à un navigateur. Les messageries de type courriel ou instantanée, la téléphonie par Internet ou *Voice Over Internet Protocol* (VOIP), Telnet ou encore FTP[5] sont des services dont on ne saurait plus se passer aujourd'hui.

4 TCP/IP est l'ensemble des protocoles utilisés pour le transfert des données sur Internet.

5 *File Transfer Protocol* (protocole de transfert de fichier), ou FTP, est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP

Avec l'essor des nouvelles technologies, de la miniaturisation et l'augmentation de puissance des batteries, le cyber-espace est devenu bien plus qu'un monde d'ordinateurs et de routeurs. Montres connectées, smartphones et une infinité d'objets connectés, ont démultiplié les possibilités et les usages, créant des liens de plus en plus forts entre le monde cyber et le monde physique.

Une gouvernance mondiale

La technologie seule ne suffit pas. Pour fonctionner, ce système complexe doit respecter des règles et faire l'objet de consensus. Dès 1979, l'*Internet Configuration Control Board* est fondé aux États-Unis par la DARPA *(Defense Advanced Research Projects Agency)* pour superviser les développements du réseau. Aujourd'hui on ne peut pas parler d'une administration ou d'un e-gouvernement mondial pour l'Internet, mais plutôt d'une forme de gouvernance collégiale impliquant les États, le secteur privé, la société civile et les organisations internationales. Parmi lesquelles trois principales doivent être citées :

- *Internet Corporation for Assigned Names and Numbers* (ICANN) : attribution des adresses IP et des noms de domaines ;
- *Internet Engineering Task Force* (IETF) : développement et promotion des standards de communication ;
- *Internet Society* (ISOC) : promotion du développement, de l'évolution et de l'usage de l'Internet.

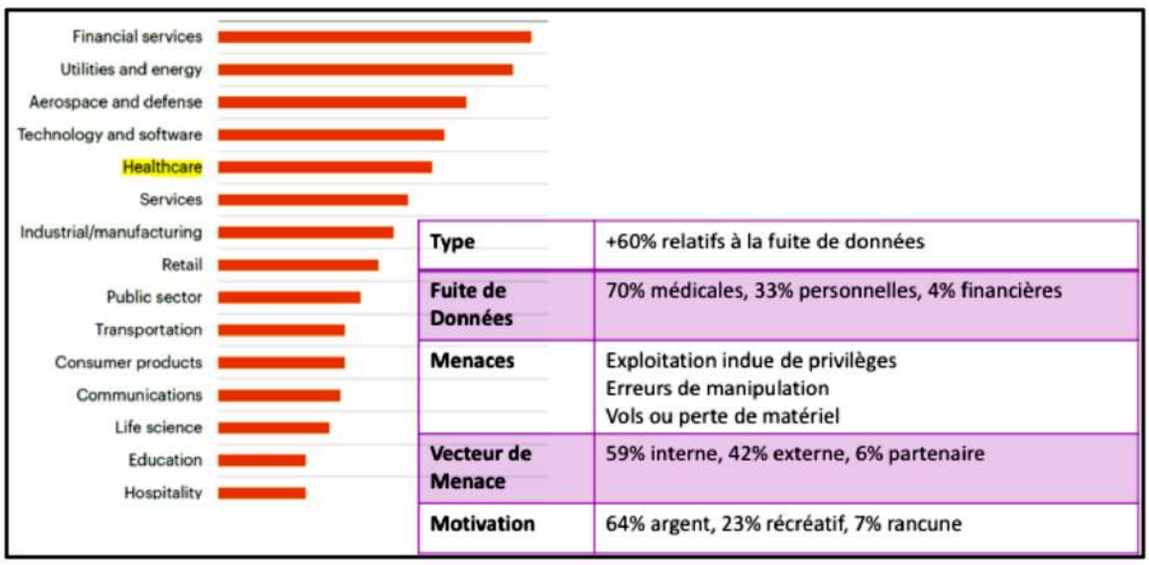
Des sujets comme la libre circulation de l'information, l'application du droit, ou le développement durable sont également débattus au niveau mondial, impliquant des organismes comme l'ONU (au travers de l'UIT, Union internationale des télécommunications, par exemple), l'OMC et des ONG.

Le « numérique » en quelques chiffres

L'UIT estimait fin 2018 que 51,2 % de la population mondiale, soit 3,9 milliards de personnes, utilisait Internet. Elle précisait également que le nombre d'abonnements à la téléphonie mobile cellulaire était devenu supérieur à celui de la population mondiale. L'arrivée prochaine de la 5G pourrait accentuer encore la progression du nombre d'objets connectés par habitant. En 2020, un foyer de quatre personnes vivant dans un pays développé ne devrait pas posséder moins de 50 appareils connectés (l'OCDE en annonce 14 milliards dans le monde pour 2022), faisant ainsi des IOT (Internet Of Things : Internet des objets) les premiers composants du cyber-espace.

Rançon de la gloire : tous ces usages dans notre quotidien attirent des convoitises et stimulent d'autres intérêts. En 2017, plus de 700 millions de cyber-attaques ont été enregistrées à travers le monde, soit une augmentation de 100 % depuis 2015 (étude ThreatMetrix).

Attaques selon les secteurs d'activité :



Type	+60% relatifs à la fuite de données
Fuite de Données	70% médicales, 33% personnelles, 4% financières
Menaces	Exploitation indue de privilèges Erreurs de manipulation Vols ou perte de matériel
Vecteur de Menace	59% interne, 42% externe, 6% partenaire
Motivation	64% argent, 23% récréatif, 7% rancune

Source : ACCENTURE - 2017 Cost of cyber-crime Study

Le Parlement européen nous alerte sur d'autres formes de risque. Dans son rapport sur l'informatique cloud (en nuage)[6] de mai 2016, il annonçait que la consommation énergétique totale des centres de traitement de données dans l'ensemble du monde (données gérées en cloud (nuage) et dans les centres informatiques internes) passerait de 95 milliards de kilowattheures en 2015 à plus de 140 milliards en 2020[7]. Dans un futur proche, Internet deviendra ainsi la première source mondiale de pollution[8].

6 En réalité le terme « cloud » est ambigu : Seul l'utilisateur est dans le « nuage », ne sachant pas où sont ses données et traitements. Les centres de stockage et de traitement des données sont eux parfaitement matériels.

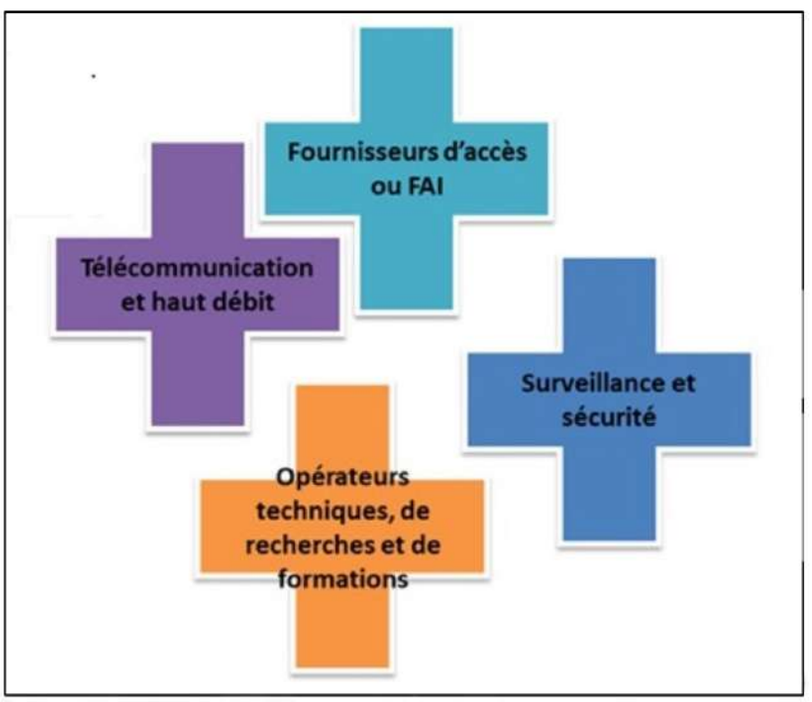
7 Et la consommation globale du réseau, inluant les appareils ds utilisateurs jusqu'à 650 milliards de kilowattheures (pour une consommation, elle aussi gobale, d'élctricité dans le monde un peu supérieure à 20 000 terawattheurs, soit environ 3,5 %).

8 Dans la mesure où l'électricité utilisée n'est pas suffisament « verte ».

Chapitre II

Les protagonistes

Vouloir décrire de manière exhaustive les protagonistes du cyber semble tenir de l'utopie. Il semble cependant pertinent de distinguer quelques grandes catégories d'acteurs.



Télécommunications Mobiles

Il existe en France trois types d'acteurs des télécommunications mobile.

Les quatre principaux opérateurs de réseau mobile sont Orange, SFR, Bouygues Télécom, et Free Mobile ; ils possèdent l'infrastructure et distribuent les services aux clients finaux et aux deux autres types d'opérateurs .

Les MVNO *(Mobile Virtual Network Operator)* sont des opérateurs qui ne disposent pas de

leur propre réseau radio[9] mais qui, pour offrir des services de communications mobiles à leurs abonnés s'appuient sur les services des opérateurs de réseau mobile en leur achetant des communications en gros. Bien que ne disposant pas d'un réseau radio en propre, les MVNO sont des opérateurs à part entière, maîtrisant la conception et le lancement de leurs offres commerciales, et pleinement responsables de la fourniture de services de communications mobiles à leurs clients. Les principaux MVNO sont le Groupe Euro-Information Telecom (EIT) et la Poste Mobile .

Les MVNE *(Mobile Virtual Network Enabler)* sont des entreprises proposant à des MVNO l'accès à un ensemble de services ou d'équipements nécessaires à l'activité d'opérateur mobile. Il peut s'agir, par ailleurs, d'opérateurs de communications électroniques.

Enfin, les accords de licence de marque signés entre un opérateur et une entreprise tierce permettent à l'opérateur de commercialiser une offre ou une gamme d'offres en exploitant la marque de l'entreprise partenaire. L'opérateur peut par la même occasion proposer des services spécifiques en lien avec l'activité de l'entreprise partenaire (accès à des contenus enrichis comme de la musique, à des services bancaires, etc.). Dans ce cas, l'opérateur de réseau reste responsable vis-à-vis des clients de la fourniture des services de communications mobiles.

La liste des MVNO fluctuant au rythme de l'évolution des stratégies commerciales, l'ARCEP publie régulièrement à titre indicatif une liste non exhaustive des MVNO présents sur le marché .

Télécommunication et haut débit

Parler de cyber-espace impose de parler de la fracture numérique et de l'accès au haut débit. L'accès au réseau implique quatre principaux types d'organisation : l'État, les opérateurs privés, les collectivités territoriales et l'Autorité de régulation des communications électroniques et des postes (ARCEP), Depuis la loi de modernisation du 18 octobre 2019 cette autorité administrative indépendante (AAI) régule également la distribution de la presse. Conscient des enjeux, le gouvernement a mis en place un Plan France très haut débit[10] qui vise à couvrir l'intégralité du territoire en très haut débit d'ici 2022. Il prévoit pour cela de mobiliser les acteurs privés et publics pour un investissement total de 20 milliards d'euros.

Accès Internet

Accéder à Internet nécessite de souscrire à des offres d'accès auprès de fournisseurs d'accès à Internet (FAI) dont les principaux en France sont : Orange, Free (groupe Iliad), SFR-Numéricable et Bouygues Telecom (groupe Bouygues). Les autres sont : Alsatis, Nordnet, OVH Télécom, Prixtel, Budget Telecom, Coriolis Télécom, Virgin Mobile, Vivéole, FDN, Nerim, Magic OnLine, etc.

9 Ce réseau d'antennes émettrices réceptrices, sur tours dédiées ou sur les toits d'immeubles qui a fait dans un passé récent polémique.

10 À titre indicatif, on parle de très haut débit quand la liaison est capable de transmettre tant dans le sens montant que descendant plus de 30 Mb/s.

Toujours en France, le contexte législatif permet à des associations de se constituer en fournisseur d'accès associatif. Il existe ainsi plus d'une dizaine de FAI associatifs en France dont les principaux sont French Data Network ainsi qu'une fédération de fournisseurs d'accès internet associatifs : la Fédération FDN.

Opérateurs techniques et de formation

L'Association française pour le nommage internet en coopération (AFNIC) est responsable des noms de domaines relevant de la France.

L'Agence pour le développement de l'administration électronique (ADAE), rattachée au ministre chargé du budget et de la réforme de l'État, assure la maîtrise d'ouvrage des services opérationnels d'interconnexion.

Le Centre de formation à la sécurité des systèmes d'information (CFSSI) forme les personnels de l'administration exerçant directement dans le domaine de l'informatique ou de la SSI.

L'Institut national de recherche en informatique et en automatique (INRIA) a été impliqué dans le réseau Cyclades, préfiguration d'Internet en France.

Gouvernance, administration et contrôle

Au sein du ***Secrétariat général de la défense et de la sécurité nationale*** (SGDSN), la direction centrale de la sécurité des systèmes d'information (DCSSI) est chargée d'organiser les travaux interministériels et de préparer les mesures que le secrétaire général de la défense et de la sécurité nationale propose au Premier ministre. Elle mène également des inspections dans les systèmes d'information des ministères. Au-dessus du Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA), elle a mis en place un Centre opérationnel de la sécurité des systèmes d'Information (COSSI), activé en permanence et chargé d'assurer la coordination interministérielle des actions de prévention et de protection face à des attaques sur les systèmes d'information.

L'***Agence nationale de la sécurité des systèmes d'information*** (ANSSI), à compétence nationale, est rattachée au secrétaire général de la défense et de la sécurité nationale (SGDSN). Elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées. Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. L'ANSSI décerne trois qualifications PDIS, PASSI et PRIS :

- la qualification PASSI (prestataire d'audit de la sécurité des systèmes d'information) de 2013-2015 a pour but d'accroître la qualité des prestations d'audit dans la cyber-sécurité.

Elle homologue les compétences des auditeurs, leur déontologie et leurs méthodes et porte sur six types d'audits relatifs ;
- la qualification PDIS (prestataires de détection d'incidents de sécurité) de 2019 est un label qui permet aux fournisseurs agréés d'accompagner les opérateurs d'importance vitale (OIV) dans la détection des cyber-attaques. Les strictes exigences en matière de cyber-sécurité imposées aux OIV proviennent de la loi de programmation militaire (LPM) de 2014-2019.
- Les dossiers PRIS[11] (prestataires de réponse aux incidents de sécurité) sont en cours de qualification auprès de dix prestataires nationaux.

« cybermalveillance.gouv.fr » porté par le Groupement d'Intérêt public ***ACYMA*** est un dispositif gouvernemental contre la cyber-malveillance, avec pour mission de prévenir et d'aider la population en matière de sécurité numérique. Il vise trois objectifs :
- via une plate-forme numérique, la mise en relation des victimes avec des prestataires de proximité susceptibles de restaurer leurs systèmes ;
- la mise en place de campagnes de prévention et de sensibilisation à la sécurité du numérique ;
- la création d'un observatoire du risque numérique permettant de l'anticiper.

Le ***ministère de l'Europe et des affaires étrangères*** coordonne les travaux de la France en matière de « cyber-diplomatie ». Cette action se décline dans un cadre européen et international.

Le ***ministère des armées*** est un acteur important pour les produits gouvernementaux de haut niveau de sécurité. Il est le maître d'œuvre des équipements ou moyens destinés à protéger ces systèmes d'information gouvernementaux. Il a également capacité à apporter son concours aux contrôles et mesures que peuvent nécessiter les systèmes d'information en service dans les départements civils. Enfin, il est chargé de doter l'État d'équipes et de laboratoires de mesures propres à satisfaire l'ensemble des besoins gouvernementaux. En outre, la direction générale de la sécurité extérieure (DGSE) est chargée de la lutte contre la cyber-criminalité à l'extérieur du territoire. Rattachée au ministère des armées, elle apporte sa connaissance des menaces étrangères sur les systèmes d'information. La direction du renseignement et de la sécurité de la défense (DRSD) assure de son côté une veille sur la sécurité des industries de défense. Enfin, le commandement de cyber-défense (Comcyber), placé sous les ordres du chef d'état-major des armées, consolide les actions du ministère dans ce domaine.

Le ***ministère de l'économie, des finances et de l'industrie*** a pour mission l'animation du développement industriel d'équipements de sécurité non-gouvernementaux. Le service des technologies et de la société de l'information (STSI) de la direction générale des entreprises (DGE) du ministère comporte un bureau du multimédia et de la sécurité, qui couvre le domaine SSI dont il finance des projets au travers d'appels à projet *Oppidum*. Enfin, comme pour les autres domaines technologiques, le Minefi contribue au financement de l'innovation dans les PME via divers mécanismes d'aide, en particulier le crédit impôt-recherche, et par le canal de BPI France dont il assure la tutelle.

11 https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/

L'agence du numérique a pour mission d'impulser et de soutenir des actions préparant la société française aux révolutions numériques. Créée en 2015, l'agence du numérique est un service à compétence nationale placé sous la responsabilité du ministère de l'économie et des finances, et pilote trois politiques publiques :

- Le ***Plan très haut débit*** qui vise à déployer les infrastructures nécessaires pour apporter un accès internet performant sur l'ensemble du territoire ;
- Le ***Pôle société numérique*** qui favorise l'autonomie et la capacité de tous à se saisir des opportunités du numérique ;
- L'initiative ***French Tech*** qui soutient la croissance des start-up en France et à l'international.

La ***direction générale de la modernisation de l'État*** au sein du ministère de l'économie, des finances et de l'industrie, regroupe plusieurs structures qui s'occupent de sujets liés à la réforme et la modernisation de l'État : direction de la réforme budgétaire, délégation aux usagers et aux simplifications administratives, délégation à la modernisation de la gestion publique et des structures de l'État, agence pour le développement de l'administration électronique. Elle succède à l'agence pour le développement de l'administration électronique (ADAE), créée dans le cadre du plan ADELE, dont la mission principale était de favoriser au sein des administrations publiques le développement de l'usage de systèmes d'information afin de faciliter l'accès du public.

Au ministère de l'Intérieur, la ***direction générale de la sécurité intérieure*** (DGSI) est chargée de la lutte contre la cyber-criminalité à l'intérieur du Territoire. L'**OCLCTIC**[12] est une structure à vocation interministérielle placée au sein de la direction centrale de la police judiciaire (DCPJ), qui lutte contre les auteurs d'infractions liées aux TIC. Elle enquête à la demande de l'autorité judiciaire, centralise et diffuse à l'ensemble des services répressifs l'information sur les infractions. La police parisienne dispose d'un service similaire, le BEFTI.

En matière de sécurité des systèmes d'information, la ***Commission nationale informatique et libertés*** (CNIL), s'intéresse essentiellement à la protection des données personnelles. La loi du le 6 août 2004 lui donne une mission de labellisation de produits et de procédures. La CNIL détient un pouvoir d'imposer que n'a pas la DCSSI.

Le ***Conseil national du numérique*** **(CNNum)** est un organisme consultatif en charge d'étudier les questions relatives au numérique et d'informer et conseiller le gouvernement quant aux enjeux et perspectives de la transition numérique. Constituée de personnalités civiles experts du numérique, cette instance est placée depuis décembre 2017 sous la tutelle du ministre chargé du numérique et défend une transition numérique citoyenne et inclusive.

Le **FIC** ***(forum international de la cyber-sécurité)*** connaît un succès grandissant confirmé par sa 12e édition, avec vingt-cinq fois plus de visiteurs et d'auditeurs qu'au départ, ce qui traduit une prise de conscience très forte à tous les niveaux de responsabilité des acteurs de la société

12 Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication..

civile et militaire. Grâce à l'appui initial et constant de la direction générale de la gendarmerie nationale (DGGN), le FIC s'est imposé comme l'événement de référence en Europe en matière de sécurité et de confiance numériques et 110 pays y sont représentés aujourd'hui. Le thème retenu pour l'édition 2020 : *« Replacer l'humain au cœur de la cyber-sécurité »*, traduit bien l'importance que l'on attache de plus en plus à la maille la plus fine de l'écosystème.

Les acteurs privés

Orange cyberdefense, Thales, CS group,, Airbus Defence & Space sont les quatre plus grands acteurs privés. Ils interviennent notamment pour l'État, les entités territoriales, les 600 opérateurs d'importance vitale (OIV) et les nouveaux opérateurs de service essentiels (OSE), ainsi qualifiés par l'ANSSI. À noter également l'importance de la Fédération des industries électriques, électroniques et de communication (FIEEC) ainsi que d'associations comme Alliance pour la confiance numérique (ACN), Tech in France ou Hexatrust.

Grandes entreprises

Il est clair que les grandes entreprises sont mieux protégées que les TPE et PME décrites dans d'autres chapitres, ne serait-ce que parce qu'elles entrent déjà dans les critères définis par l'ANSSI :

Opérateurs d'importance vitale : Face à l'augmentation en quantité et en sophistication des attaques informatiques, et à leur impact potentiellement destructeur, l'ANSSI a pour mission d'accompagner les OIV dans la sécurisation de leurs systèmes d'information sensibles. Ils sont environ 250 dans 12 secteurs d'activité, répartis en 4 dominantes :

- HUMAINE : alimentation, gestion de l'eau, santé ;
- RÉGALIENNE : activités civiles de l'État, activités judiciaires, activités militaires de l'État ;
- ÉCONOMIQUE : énergie, finances, transports ;
- TECHNOLOGIQUE : communications électroniques, audiovisuel et information, industrie, espace et recherche.

Fournisseurs de services numériques : La directive NIS définit les FSN comme *« Personnes morales qui fournissent tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services »*. Trois types de services numériques sont concernés par ce cadre réglementaire :

- les places de marché en ligne, qui permettent à des consommateurs ou à des professionnels de conclure des contrats de vente ou de service en ligne avec d'autres professionnels, soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne ;
- les moteurs de recherche en ligne, qui permettent aux utilisateurs d'effectuer des recherches sur tous les sites internet ou sur des sites internet dans une langue donnée, sur la base

d'une requête lancée sur n'importe quel sujet à partir d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoient sur des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé ;
— les services d'informatique en cloud (nuage), qui permettent l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées.

La définition de FSN couvre autant l'activité envers les particuliers (business to consumer — B to C) qu'envers les professionnels (business to business — B to B) et (business to administration — B to A).

O*pérateurs de service essentiel* : Un OSE est un opérateur, tributaire des réseaux ou systèmes d'information, qui fournit un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société. Un service essentiel correspond à trois critères :
— il est essentiel au maintien d'activités sociétales ou économiques critiques ;
— sa fourniture est tributaire de réseaux et de systèmes d'information ;
— un incident sur ces réseaux et systèmes aurait un *effet disruptif* majeur sur la fourniture dudit service, son importance étant déterminée en prenant en compte les facteurs trans-sectoriels suivants :
  - nombre d'utilisateurs tributaires du service fourni par l'entité concernée ;
  - dépendance des autres secteurs à l'égard du service fourni par cette entité,
  - conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur des fonctions économiques ou sociétales ou sur la sûreté publique,
  - part de marché de cette entité,
  - portée géographique, eu égard à la zone susceptible d'être touchée par l'incident,
  - importance que revêt l'entité pour garantir un niveau de service suffisant, en cas d'indisponibilité de solutions de rechange pour la fourniture de ce service.

Au-delà de ces catégories, les grandes entreprises et les grandes administrations sont plus sensibles au cyber-risque, mais présentent très souvent l'avantage de posséder bien plus de ressources dédiées que les TPE et PME. Leurs niveaux de risque sont également différents, car au-delà d'un simple impact de coûts dus à une cyber-attaque, elles peuvent aussi subir une très forte dégradation de leur image « économique ». On constate d'ailleurs que les entreprises ayant subi une cyber-attaque « réussie » peuvent perdre jusqu'à 10 % de leur valeur boursière.

Au-delà de ces catégories, les grandes entreprises et les grandes administrations sont plus sensibles au cyber-risque, mais présentent bien souvent l'avantage de posséder bien plus de ressources dédiées que les TPE et PME. Comparons la nouvelle volonté politique très forte en Chine envers son gigantesque tissu de TPME/PMI : 100 % des *« Network Operators »* NO (opérateurs de réseaux), soit 99 % des entreprises chinoises, doivent identifier et former à leur frais un référent cyber-sécurité. Nous sommes encore loin en Europe et en France de cette volonté politique… Les niveaux de risque des grandes organisations sont évidemment plus

élevés, car au-delà d'un simple impact de coût dû à une cyber-attaque, elles peuvent aussi subir une très forte dégradation de leur image « économique ». On constate d'ailleurs que les entreprises ayant subi une cyber-attaque « réussie » peuvent perdre jusqu'à 10 % de leur valeur boursière.

Administrations

Qu'elle s'incarne sous la forme d'un service d'État, de collectivité territoriale, d'une organisation ou d'une institution internationale, l'administration publique s'inscrit dans une dynamique plus ou moins rapide et intrusive dans le cyber-espace. Les motivations ne sont pas nouvelles. Dès 1966, le président Charles de Gaulle, sous l'impulsion de Michel Debré, d'un groupe de hauts fonctionnaires et d'industriels, lance Le Plan calcul dont l'objectif était d'assurer l'autonomie de la France dans les technologies de l'information et de développer une informatique européenne. Vision d'autant plus actuelle que des outils comme l'intelligence artificielle ou la blockchain[13] sont en plein essor et semblent pouvoir apporter une réponse aux problèmes de nos organisations. Malheureusement, aujourd'hui encore, les systèmes d'information sont trop souvent perçus comme un enjeu uniquement technologique, une question de techniciens, alors que toute technique, aussi performante et prometteuse qu'elle soit, reste dépendante de l'humain pour sa mise en œuvre.

Le Plan calcul a connu son premier échec avec le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus), la dimension sociétale ayant été sous-évaluée : la réminiscence des déportations rendues possibles via l'utilisation des fichiers dont disposait l'administration de Vichy et la suspicion envers l'administration ont provoqué un mouvement populaire qui a sabordé le projet. Adolphe Touffait, procureur général de la Cour de cassation, s'exprimait déjà en ce sens en 1973 devant l'Académie des sciences morales et politiques : « *La dynamique du système qui tend à la centralisation des fichiers risque de porter gravement atteinte aux libertés, et même à l'équilibre des pouvoirs politiques* ». Des plans successifs, nombreux et plus ou moins ambitieux, ont tracé le chemin vers une cible qui s'est précisée au fur et à mesure par la création successive de nouveaux services ayant entre eux une meilleure complémentarité et une bonne cohérence.

Sous-jacente à ces démarches, la recherche de performance économique liée à une réduction de la masse salariale et à la dématérialisation, a masqué l'objectif sociétal de l'administration numérique dans sa mission de service public. À titre d'exemple, le métier d'écrivain public est en plein essor car il se substitue aux agents des finances publiques dans l'assistance à des contribuables démunis face aux outils numériques, et qui représentent encore un pourcentage non négligeable de la population. Ainsi, même si France Connect[14], qui avec un seul et même identifiant permet d'accéder à un ensemble de services publics, annonce 13 millions

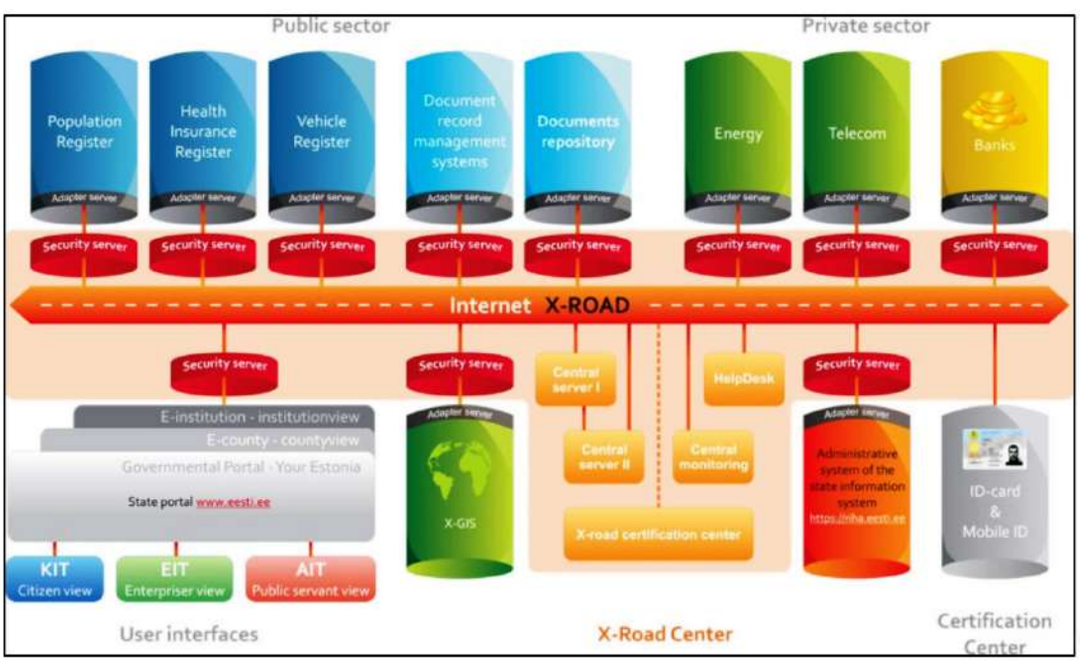
13 La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe central de contrôle (définition de Blockchain France).

14 (https://franceconnect.gouv.fr/),

d'utilisateurs, une description sans ambiguïté de l'objectif visé devrait être formulée, partagée et discutée.

La technologie moderne ne cesse d'offrir à l'homme de nouvelles possibilités, d'ouvrir le champ du possible, mais porte-t-elle en elle une morale, une finalité ? Comme l'évoque Lawrence Lessig avec sa célèbre formule « le code est Loi » : on place l'architecture technique au sein d'un ensemble d'éléments qui déterminent le mode de réglementation, i.e. comment, avec quoi et pourquoi ces éléments synthétisent-ils la volonté politique, les contraintes technologiques et la finalité du service public. La prétendue objectivité reflète en réalité la vision personnelle des codeurs… Or la confiance dans un système d'information réside avant tout dans l'usage que l'on veut et que l'on peut en faire.

Un modèle se développe actuellement en Europe. Il prend sa source en Estonie où plus de 98 % des démarches administratives se font en ligne. Elles s'appuient sur une identité numérique individuelle (chacun peut devenir erésident estonien !) et sur une plate-forme technologique appelée X-Road :



Source : Gouvernement estonien

À l'échelle d'un pays se pose la question de savoir qui décide réellement : celui qui fait la Loi ou bien celui qui code le système ? Lier l'administration à son avatar cyber pose la question fondamentale d'une nécessaire adaptation du droit. Exemple extrême de cette dichotomie du droit : vous risquerez une condamnation plus légère en piratant un pacemaker connecté plutôt qu'en poignardant la personne avec un couteau de cuisine !

Même si le cadre juridique se renforce pour protéger les individus dans l'usage qui est fait de leurs données et dont le règlement général sur la protection des données à caractère personnel (RGPD) est un exemple majeur, il n'en reste pas moins qu'un travail d'ampleur reste à faire sur l'ensemble des menaces qui pèsent sur notre modèle sociétal. Une vigilance s'impose à l'heure des « *Big Brother* » monitorant l'activité internet, des télé-réalités, des systèmes de notation en tous genres depuis les *like* Facebook jusqu'aux avis partagés sur les portails en ligne.

La fiction associée à cette imaginaire du Big Brother *(1984)* a été rattrapée par la réalité d'un système conçu pour veiller à la sensibilisation, à l'intégrité et à la crédibilité des individus au sein d'une société. Avec son système de « crédit social » combinant surveillance de masse, surveillance des individus par d'autres, voire par eux-mêmes, reconnaissance faciale et autres technologies, la Chine nous donne un exemple concret des lendemains que d'aucuns pourraient souhaiter voir dans nos démocraties.

Le marché français de la cyber-assurance

Au premier semestre 2019, la société de courtage AON a répertorié 3 718 cyber-incidents dans le monde, en croissance par rapport à 2015 (3 391) et 2016 (3 252). Devant la multiplication de ces attaques, le risque cyber prend de plus en plus d'ampleur en France comme ailleurs : en février dernier, la fédération française de l'assurance publiait la deuxième édition de son baromètre des risques émergents pour les assureurs et les réassureurs et, sans surprise, le risque cyber arrivait en première position.

Les exemples de sinistres cyber sont pléthoriques. L'évolution a été importante en France durant les trois dernières années, notamment avec l'arrivée des logiciels de rançonnage (ransomware) comme *WannaCry*, *Petya* et *NotPetya*. Les incidents provoqués par ces logiciels ont donné une immense résonnance au risque cyber et, en conséquence, au besoin d'assurance cyber en France. Les chiffres parlent en effet d'eux-mêmes : en 2018, le marché mondial de l'assurance cyber était estimé à 3,5 milliards de dollars, dont 85 à 90 % sur le marché américain. Sur la même période l'Europe ne représentait que 5 à 9 %, soit un maximum de 300 millions de dollars de prime, la France ne pesant, elle, que 40 millions d'euros. Ces chiffres montrent l'important décalage de maturité de la cyber-assurance entre la France et les États-Unis. Il y a néanmoins certaines évolutions notables ces deux dernières années : recrudescence des cyber-attaques contre tous types de secteurs et toutes tailles d'entreprises, publication de la directive européenne n° 2016/679 du 25 mai 2018. Ce règlement général sur la protection des données (RGPD) a permis une prise de conscience générale, tout au moins au niveau réglementaire : obligations de notification, de mise en place d'un *Data Privacy Officer* (DPO), etc.

Depuis lors, la menace cyber n'a jamais été aussi prégnante en France. Le type d'attaque qui a dépassé le traditionnel Ransomware, peu coûteux à mettre en place, mais très rémunérateur, est aujourd'hui le *Business Email Compromise*, l'attaque par e-mail d'imposteur. En 2018, près

du quart des incidents déclarés auprès des assureurs du marché français étaient en lien avec ce type d'attaque, en augmentation de 11 % par rapport à 2017.

Durant cette période, tous les secteurs du marché ont été impactés : agroalimentaire, médical, consulting, etc. Ceux des incidents qui ont été mis en lumière par la presse concernent, évidemment, surtout de grandes entreprises comme Altran, Eurofins ou Fleury Michon, mais les TPE et PME françaises ont été impactées elles aussi, de même que des collectivités territoriales et des hôpitaux publics.

Conséquence de ce phénomène, on observe depuis une nette augmentation de la souscription d'assurances cyber, reflétant à un an d'intervalle sur le marché une explosion de sinistres d'une sévérité en constante augmentation qui déclenchent notamment des types de garanties qui n'étaient pas activées auparavant : on constate aujourd'hui couramment des sinistres déclarés à plus d'un million d'euros là où il y a encore deux ans les grands sinistres se montaient à quelques milliers. Cette poussée a engendré *de facto* un durcissement des modalités de souscription et de négociation des primes.

En 2018, la fréquence des attaques a augmenté de 67 % en France, la proportion de PME touchées par une cyber-attaque ayant elle aussi augmenté : quatre PME sur dix ont déjà subi une ou plusieurs attaques ou tentatives d'attaque cyber, entraînant différents types de préjudices :
- paralysie des infrastructures : système d'information, serveurs…
- vol de données personnelles ou confidentielles : clients, fournisseurs, salariés ;
- atteinte à l'image et à la réputation ;
- impact économique et financier.

Ces agressions cyber font courir des risques de dommages et de responsabilité civile potentiellement importants à toutes les entreprises, quel que soit leur secteur d'activité. Le marché français reste encore un *soft market* sur la cyber-assurance, mais l'expérience de 2019 laisse à penser qu'il sera de plus en plus difficile de souscrire une assurance cyber. Les assureurs deviennent particulièrement regardants sur l'hygiène informatique des prospects et sur leur management des risques, et seront moins enclins à accepter sans contrepartie une exposition trop importante. Concernant les renouvellements, par exemple, nous voyons déjà (comme dans les autres domaines) des majorations tarifaires plus sévères appliquées suite à des sinistres intervenus.

L'international

Le monde est devenu tricéphale depuis l'entrée de la Chine au sein de l'OMC le 11 décembre 2001 : États-Unis, Europe, Chine et son homologue russe. . Il deviendra quadricéphale « quand l'Inde s'éveillera » à son tour. Encore trop peu de dirigeants, de décideurs de petites, moyennes et même de grandes organisations, qu'elles soient privées ou publiques, mesurent le contenu,

la portée, les conséquences induites et l'impact pour leur propre écosystème des arsenaux législatifs mis en place par ces trois blocs.

Certains ont bien compris que la loi fédérale américaine *« Clarifying Lawful Overseas Use of Data Act »*, dite *Cloud Act* (H.R. 4943), a été adoptée sans examen spécifique, i.e. votée *ipso facto* par les deux chambres dans le cadre de la loi de finances États-Unis, puis promulguée le 23 mars 2018. Ce *Cloud Act* permet en théorie une intrusion systémique partielle dans nos systèmes d'information par la puissance américaine. Mais encore trop peu de dirigeants et décideurs comprennent l'étendue de cette approche, les risques qui y sont attachés et, surtout, les conséquences pour le quotidien informatique de tous leurs salariés, de leurs *multi-devices*, et aussi de leurs sous-traitances en cascade, ni informés et ni « blindés » juridiquement par autant de contrats bipartites ou collectifs de droit français ou autre qu'il y a de donneurs d'ordres et de parties prenantes dans la chaîne de sous-traitance.

Très peu de non financiers et seuls quelques *risk managers* comprennent l'impact de directives qui ne sont pas directement relatives à l'informatique : à titre d'exemple, la trop faible prise en compte de l'impact de *« Purchase to Pay* (P2P) » et « *Order to Cash* (O2C) » sur tout le processus des chaînes d'approvisionnement de rang 1 à n, ou du paiement « SEPA » en application de la Directive des Services de paiement 2007/64/CE dite « DSP1 », autour par exemple de la LAB/LAT[15]. La DSP2 est entrée en vigueur le 13 janvier 2019, dans une indifférence quasi générale, même si les Français attendaient sa transposition avant la fin de l'année.

Face à cela, analysons le remarquable *Empire du Milieu*. Son arsenal législatif est une première dans l'histoire des civilisations par son ampleur (500 textes de loi), sa rapidité de création (cinq ans) et de mise en application, *de facto* au 1er janvier 2019, dans une indifférence totale de l'Europe hormis quelques services gouvernementaux. La *China Cybersecurity Law* (CSL) est entrée en vigueur 1er janvier 2017, en suite logique de la création de la *Cyberespace Administration of China* (CAC) en 2012 en vertu du principe : « Il n'y a pas de sécurité nationale sans cyber-sécurité ». Cette ANSSI locale dépend directement du Président, désormais à vie, de la République de Chine. Cette batterie de lois et règlements s'applique à deux niveaux d'organisations chinoises ou « assimilées » :

- *« Network Operators »* NO (opérateurs de réseaux), soit 99 % des TPE/PME/PMI, organisations privées comme publiques, en clair toute organisation qui possède un site internet ou cinq ordinateurs connectés, ou encore une adresse IP fixe ;
- *« Critical Infrastructure Operators »* (CIO), l'équivalent de nos 249 OIV, et de nos quelques centaines de nouvellement définies OSE et FSN.

Les dizaines de millions de « NO » doivent notamment identifier et former à leur frais un référent cyber-sécurité. Dans l'indifférence totale, une véritable « armée cyber » s'est donc mise en place, sans équivalent en Europe.

15 Lutte anti blanchiment et contre le financement de terrorisme.

La France, quant à elle, s'est dotée d'une Agence nationale de la sécurité des systèmes d'information (ANSSI) dont on pourrait résumer l'encadrement juridique comme suit :

- *description* : elle est « l'autorité nationale en matière de sécurité des systèmes d'information » ;
- *fondement légal* : créée par le décret n°2009-834 du 07 juillet 2009
- *Cadre institutionnel* : 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 dans l'exercice de ses responsabilités en matière de Défense et de Sécurité nationale ;
- *Compétences* : Elle « *Se prononce sur la sécurité des dispositifs et des services, offerts par les prestataires, nécessaires à la protection des systèmes d'information.* » À ce titre, elle intervient pour l'agrément « *Des centres d'évaluation et la certification de sécurité offerte par les produits et les systèmes des technologies de l'information* ». Elle est aussi, bien sûr, en charge de la certification (« autorité nationale de contrôle de la certification ») avec l'Agence européenne.

Qu'apporte l'Union européenne ? La France, en tant que membre de l'UE, est soumise à sa réglementation. Dans ce contexte, la construction du marché unique du numérique a conduit au règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019, créant l'ENISA (Agence de l'Union européenne pour la cyber-sécurité) et une nouvelle certification de cyber-sécurité pour les technologies de l'information et des communications. Entré en vigueur le 27 juin 2019, il abroge et remplace le Règlement UE n°526/2013 relatif à la cyber-sécurité. Aux termes dudit règlement, les axes majeurs de l'ENISA sont de :

- contribuer au développement du secteur de la cyber-sécurité dans l'Union, en particulier parmi les PME et les start-ups ;
- de s'efforcer d'établir une coopération plus étroite avec les universités et les entités de recherche afin de réduire la dépendance de l'UE à l'égard des produits et services de cyber-sécurité provenant de l'extérieur, et de renforcer les chaînes d'approvisionnement à l'intérieur de l'Union[16].

Cette agence européenne s'est aussi vue attribuer un rôle de coordination des politiques de cyber-sécurité et de conseil :

- préparation des « schémas européens de certification de cyber-sécurité » ;
- connaissance et information sur les menaces numériques ;
- éducation du public à la sécurité des systèmes d'information, de recherche et innovation ;
- coopération internationale avec les pays tiers dans le cadre de ses compétences ;
- maintien à jour d'un « site internet sur les schémas européens de certification de cyber-sécurité ».

Ce règlement prévoit aussi la mise en place d'un système européen de certification de cyber-sécurité instauré à l'échelle de l'Union, aux termes duquel :

16 https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32019R0881&from=FR

- toute certification obtenue dans un État membre est automatiquement reconnue dans les autres, sans aucune formalité supplémentaire ;
- trois niveaux de certification des systèmes de cyber-sécurité sont prévus (par ordre croissant de protection) : niveau d'assurance élémentaire, niveau d'assurance substantiel, niveau d'assurance élevé ;
- chaque État crée / met en place un guichet unique (l'ANSSI assure cette mission en France).

Outre la norme ISO 27000 sur la sécurité des systèmes d'information, les mécanismes permettant d'assurer un niveau élevé de sécurité de ces SI ont fait l'objet d'une harmonisation en vue de constituer un marché intérieur du numérique avec l'adoption de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016, concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite directive SRI, dont l'objectif général est d'assurer un rapprochement *a minima* des législations dans ce domaine. Ce texte assigne trois objectifs opérationnels :

- implémentation d'une cartographie des systèmes d'information sensibles : Principaux opérateurs de l'économie numérique, identification des entités vitales ;
- signalement des incidents informatiques intervenus sur ces systèmes d'information ;
- adoption par les États membres d'une stratégie nationale compatible avec l'intérêt général à terme.

Chapitre III

Zoom sur la cyber-criminalité

La cyber-criminalité est une notion floue, abstraite, qui a vu le jour à la fin des années 1990. Elle désigne *« Toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau* [17]*».* Selon l'OCDE, la cyber-criminalité s'assimile à *« Tout comportement illégal, ou contraire à l'éthique, ou non autorisé, qui concerne un traitement automatique de données et, ou de transmission de données »*. Ce terme renvoie à une nouvelle forme de délinquance qui se situe dans un espace virtuel communément appelé le « cyber-espace ». En effet, si Internet a permis à des millions de personnes d'accéder à d'innombrables informations, son développement a, par ailleurs, engendré la naissance d'un « cyber-crime ». Le terme cyber se voit ainsi associé à toutes sortes de délinquances : la « cyber-fraude », le « cyber-terrorisme », la « cyber-pédophilie », etc.

C'est pourquoi la France, mais aussi la communauté internationale, souhaitent se prémunir contre cette menace. Notons par exemple l'accent que mettent de plus en plus Interpol et Europol sur le cyber-crime. Au niveau national, le législateur, la doctrine et la jurisprudence se sont saisis du domaine d'Internet contribuant ainsi à l'émergence d'une nouvelle branche du droit : le « cyber-droit pénal ». L'internaute est un justiciable, et nul n'est censé ignorer la loi. En 2009, les sages du Conseil Constitutionnel ont estimé que l'accès à Internet était un droit fondamental pour les citoyens, ce qui limite, notamment, les moyens d'actions du législateur dans sa lutte contre la cyber-criminalité. C'est une des formes de délinquance qui connaît actuellement la croissance la plus forte. La rapidité et les fonctionnalités des technologies modernes, conjuguées à l'anonymat qu'elles permettent, facilitent la commission de nombreux crimes et délits.

En réalité, cet anonymat est une chimère : outre les hackers et autres virtuoses du web, chaque internaute est assez aisément identifiable. Le titulaire de l'accès à Internet par un abonnement est une personne physique ou morale, qui se voit attribuer temporairement, ou pour toute la durée de son abonnement, une adresse IP lui permettant de communiquer sur Internet. Celle-ci correspond à un numéro qui permet l'identification de chaque ordinateur connecté à Internet, et par conséquent l'identification de son utilisateur.

D'autre part, en matière d'investigation, les ordinateurs sont de véritables « réservoirs de preuves ». Ce qui autrefois était consigné sur du papier, a toutes les chances d'être aujourd'hui

17 https://fr.wikipedia.org/wiki/Cybercrime

consigné sous forme numérique. Tout informaticien armé des bons outils peut retrouver et exhumer tous fichiers et dossiers compromettants, pourtant soigneusement effacés. Il apparaît que la cyber-criminalité renvoie à trois types d'infractions :

- il y a tout d'abord les formes traditionnelles de criminalité, facilitées par les technologies de l'information et de la communication. La fraude ou l'escroquerie en sont de parfaits exemples. Arnaques, fraudes ou encore non-respect du copyright préexistent à Internet, mais on ne peut nier que la toile a favorisé leur développement ;
- sont visées ensuite les infractions dites « de contenu » telles que la pédophilie via Internet, le racisme ou la xénophobie. On ne peut pas tout faire et tout dire sur Internet, c'est pourquoi les blogueurs doivent faire preuve d'une certaine prudence car ils peuvent être poursuivis s'ils commettent des infractions (diffamation, etc.) via leurs blogs ;
- enfin, il y a les nouveaux crimes, qui ont vu le jour avec les réseaux numériques. Ce sont des infractions visant les systèmes d'information et de traitement de données. Le piratage en est sans doute l'exemple le plus connu.

Le point commun de toutes ces infractions est qu'elles peuvent être commises à grande échelle. De plus, la distance géographique entre le lieu où le délit est commis, et celui de ses effets peut être considérable : un hacker basé à Shanghaï pourra tout à fait pirater le système de sécurité d'une banque parisienne.

Hacking ou piratage

Le terme piratage désigne l'utilisation de connaissances informatiques à des fins illégales. L'*article 323-1* du Code pénal sanctionne « Le fait d'accéder ou de se maintenir frauduleusement, dans tout ou partie d'un système de traitement automatisé ». La peine encourue est deux ans d'emprisonnement et 30 000 € d'amende, et peut être portée à trois ans de prison et 45 000 € d'amende lorsqu'il en résulte « Soit la suppression, soit la modification de données contenues dans le système, soit une altération du fonctionnement de ce système ». Le hacker encourt également, au titre des peines complémentaires, la confiscation du matériel informatique qui a servi ou était destiné à commettre l'infraction. Il convient de préciser que le hacker engage sa responsabilité pénale, mais également sa responsabilité civile. Il devra ainsi verser des dommages-intérêts à la victime pour l'indemniser. L'extraterritorialité limite évidemment la portée de cet éventail de sanctions.

Spoofing

Le *spoofing* s'apparente au hacking. Il désigne le fait d'intervenir dans les communications entre plusieurs machines dans le but de se substituer frauduleusement à certaines d'entre elles. Cela permet d'intercepter des données, des correspondances ou, encore, d'envoyer des données en usurpant l'identité du titulaire de la machine « spoofée ». La répression est la même que pour le hacking, à savoir deux ans d'emprisonnement et 30 000 € d'amende. Le spoofer engage également sa *responsabilité civile*.

Le Carding

Le *carding* désigne la création virtuelle de cartes bancaires. C'est une « fraude à la carte bleue ». Sur certains sites, il est en effet possible d'acheter ou de vendre des accès à des comptes bancaires, des numéros de cartes volés, des copies de pistes magnétiques et des profils personnels complets.

Le Skimming

Le *skimming*, quant à lui, désigne une opération frauduleuse qui consiste à faire des copies magnétiques des cartes bancaires à l'aide d'un lecteur mémoire appelé *skimmer*. C'est également une fraude à la carte bancaire. Le code confidentiel peut ainsi être capté à l'aide d'une micro-caméra. Les données acquises sont alors inscrites sur les pistes magnétiques d'une carte contrefaite. Ces fausses cartes peuvent ensuite être utilisées dans les commerces ou pour des retraits de numéraire dans les distributeurs automatiques de billets.

L'article L163-4 du Code monétaire et financier punit de sept ans d'emprisonnement et de 750 000 € d'amende, *« Le fait de contrefaire ou de falsifier une carte de paiement ou de retrait ; de faire ou tenter de faire usage, en connaissance de cause, d'une carte de paiement ou de retrait contrefaisante ou falsifiée ; d'accepter, en connaissance de cause, de recevoir un paiement au moyen d'une carte de paiement contrefaisante ou falsifiée »*.

Scamming

Le *scamming* désigne toutes les arnaques faites par le biais d'Internet. Elles sont multiples, mais ont toutes en commun pour but d'obtenir de la victime qu'elle effectue un virement depuis son compte bancaire.

Par exemple, l'escroquerie « à la nigériane » se fait par l'intermédiaire de mails où « un soi-disant homme d'affaire, un orphelin ou une veuve sollicite de l'aide pour transférer des millions de dollars bloqués dans un pays « en raison de problèmes politiques », adaptés en fonction de l'actualité internationale. L'escroc sollicite une somme d'argent afin de corrompre les autorités locales ou de payer l'entreprise de gardiennage détenant un coffre. Un pourcentage de l'ordre de 10 à 15 % du montant total est généralement promis. Ces transferts d'argent en cash se font via des sociétés spécialisées comme Western Union.

Le *scammer* et ses complices peuvent être poursuivis pour fraude. L'article 313-1 du code pénal sanctionne, au titre de l'escroquerie, *« Le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge »*. L'auteur encourt une peine decinq ans d'emprisonnement et de 375 000 € d'amende, la manipulation informatique étant en effet considérée comme une manœuvre frauduleuse.

Spamming

Le *spamming* désigne l'envoi de courriers électroniques non sollicités. Tous les internautes ont déjà reçu des *spams*, ces courriers qui ont pour effet de « pourrir » les boîtes mail. En français, on parle d'ailleurs de « pourriels ». Cette pratique peut être sanctionnée sous diverses qualifications, en étant assimilée :

- à une entrave ou au fait de fausser le fonctionnement d'un système de traitement automatisé de données par déni de service, si l'envoi massif de courriers électroniques a eu pour effet de paralyser le serveur mail de la victime ;
- à des prospections directes au moyen de courrier électronique, utilisant les coordonnées d'une personne physique qui n'a pas donné son consentement préalable à recevoir des prospections directes par ce moyen ; ce qui est sanctionné par le code de la consommation.

Cryptologie

La *cryptologie* désigne la technique qui consiste à chiffrer un message afin de le rendre inintelligible à celui qui ne possède pas la clé de décodage. En France, l'usage de la cryptologie est libre depuis la loi pour la confiance dans l'économie numérique du 21 juin 2004. Toutefois, l'article 132-79 du code pénal sanctionne la cryptologie *« Lorsqu'un moyen de cryptologie a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission »*. Le maximum de la peine privative de liberté encourue est relevé lorsque l'auteur ou le complice de l'infraction, malgré la demande des autorités judiciaires ou administratives, refuse de remettre la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement.

Google Bombing

Le *google bombing* (bombardement google) désigne l'activité consistant à diffuser en masse une information. Cette technique n'est pas illégale en soi car elle ne relève ni du piratage ni d'une quelconque faille, mais exploite simplement la manière dont Google organise les résultats de recherche sur ses pages. Concrètement, le pirate crée une multitude de sites et procède à leur référencement dans différents annuaires. Lorsqu'un internaute cherchera une information sur la personne victime du *bombing*, elle tombera alors sur les faux sites.

Lorsque les informations faisant l'objet du « google bombing » sont fausses, voire diffamatoires, cela peut devenir fort préjudiciable pour la victime. Malgré son nom, la technique de « bombardement Google » est évidemment observable sur d'autres moteurs de recherche comme Yahoo! ou Live Search.

Cracking

Le *cracking* désigne en informatique, l'opération de faire un « crack » ou déverrouillage de logiciel. C'est l'activité consistant à contourner un système de protection d'un logiciel ou plus généralement d'une œuvre, puis éventuellement à mettre à la disposition du public la nouvelle version du logiciel ou de l'œuvre.

L'*article L335-3-1 du code de la propriété intellectuelle* punit de 3 750 € d'amende les modifications non autorisées des logiciels mais aussi « Le fait de porter atteinte sciemment, à des fins autres que la recherche, à une mesure technique afin d'altérer la protection d'une œuvre par un décodage, un décryptage, ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle ».

Le simple fait de procéder au cracking d'une œuvre est sanctionné, sans qu'il soit besoin de prouver que le « cracker » a mis à disposition du public le logiciel ou l'œuvre sans son logiciel de protection. L'article L335-3-1 du code de la propriété intellectuelle ajoute que le « cracker » qui met à disposition du public des logiciels de « cracking » encourt une peine d'emprisonnement de six mois et 30 000 € d'amende. Cela constitue également un acte de contrefaçon et peut être puni pour ce chef, l'auteur encourant alors cinq ans d'emprisonnement et 500 000 € d'amende.

Fraude aux sites aux enchères

Les fraudeurs sont souvent attirés par les sites de ventes aux enchères en ligne. Le fraudeur peut aussi bien être le vendeur que l'acheteur. La fraude peut consister, d'une part, à tromper l'acheteur sur les caractéristiques essentielles du bien vendu, ou plus simplement à ne pas livrer le bien. Il se peut également que le bien vendu soit en réalité un bien volé, voire contrefait. Dans ce cas, et à défaut de pouvoir établir sa bonne foi, l'acheteur peut encourir des peines relatives au recel ou à la contrefaçon. Le délit peut également consister à ne pas payer un bien acheté alors même qu'il a été livré, ou à le payer avec des moyens frauduleux.

Cyber-sexualité

La pédopornographie par Internet constitue une forme particulièrement grave d'exploitation sexuelle des enfants. À ce jour, on compte environ 100 000 sites consacrés à la pédopornographie. La pornographie infantile, est définie par les Nations unies comme *« Toute représentation, par quelque moyen que ce soit, d'un enfant s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou toute représentation des organes sexuels d'un enfant, à des fins principalement sexuelles »*.

Elle est illégale en France et dans la plupart des pays occidentaux. Le législateur français a d'ailleurs fait de la lutte contre la pédopornographie l'une des priorités de sa politique criminelle. Les affaires de pédophilie représentent chaque mois en France 20 à 40 % des affaires pénales touchant Internet. Qu'il s'agisse de producteurs, d'intermédiaires ou de simples consommateurs d'images de mineurs à caractère pornographique, tous peuvent faire l'objet de poursuites pénales sur différents fondements juridiques.

L'*article 227-23 du code pénal* sanctionne de cinq ans d'emprisonnement et de 75 000 € d'amende *« Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur, lorsque cette image présente un caractère pornographique »*.

Il en est de même du fait *« De diffuser une telle image ou représentation par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter »*. Les peines sont portées à sept ans d'emprisonnement et à 100 000 € d'amende lorsque la diffusion de ces images s'est faite sur un réseau de télécommunication comme Internet. Le simple fait de détenir une telle image ou représentation, est puni de deux ans d'emprisonnement et de 30 000 € d'amende. La représentation à caractère pédophile inclut les montages et dessins à caractère pédophile fabriqués à partir de photographies d'enfants, mais aussi des images totalement virtuelles à caractère pédophile. Ces dispositions sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée d'au moins dix-huit ans au jour de la fixation ou de l'enregistrement de son image. Il existe donc une présomption de minorité qui fait peser la charge de la preuve sur le détenteur des images.

Est également sanctionné le fait de faire des propositions sexuelles à un mineur par tout moyen de communication électronique. Ainsi, *« Le fait pour un majeur de faire des propositions sexuelles à un mineur de 15 ans ou à une personne se présentant comme telle, en utilisant un moyen de communication électronique est puni de deux ans d'emprisonnement et de 30 000 € d'amende »*. Ces peines sont d'ailleurs aggravées à cinq ans d'emprisonnement et 75 000 € d'amende lorsque les propositions aboutissent à une rencontre effective.

Cyber-proxénétisme

Comme tous les délinquants, les *proxénètes* ont de plus en plus recours à Internet pour développer leurs activités délictueuses. Ils encourent, dès lors, des peines aggravées. L'article 225-7 du code pénal dispose que « Le proxénétisme est puni de dix ans d'emprisonnement et de 1 500 000 € d'amende lorsqu'il est commis grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de télécommunication ». De nombreux sites de proxénètes se dissimulent sous des appellations anodines telles que « massages » ou « rencontres », ce qui rend leur identification plus délicate. Il convient de préciser qu'un site qui propose des services à caractère sexuel moyennant rémunération tombe également sous le coup du délit de racolage.

Téléchargement illégal

Le développement d'Internet est aussi au cœur du débat concernant le respect des *droits de propriété intellectuelle*. Des millions de fichiers de musique et de films sont téléchargés illégalement grâce à des logiciels « Peer to Peer » ou, plus récemment, via des sites de streaming, ce qui justifie la mobilisation des auteurs qui entendent protéger leurs créations. Il convenait de trouver un juste équilibre entre le droit fondamental que constitue l'accès à Internet, et la protection de la propriété intellectuelle. C'est maintenant chose faite depuis la promulgation de la loi HADOPI II.

L'infraction de téléchargement illégal vise *« Les manquements à l'obligation de surveillance de l'accès à Internet, pesant sur le titulaire d'un abonnement à un service en ligne, de veiller à ce*

que cet accès ne fasse pas l'objet d'une utilisation constituant une atteinte aux droits d'auteur ». La Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI) met en œuvre cette loi contre le téléchargement illégal via un dispositif de riposte graduée, qui prévoit deux niveaux d'avertissement. Dans un premier temps, l'internaute identifié recevra un avertissement par e-mail, puis en cas de récidive un second par lettre recommandée. En cas de troisième infraction, une suspension de son abonnement internet pour une durée maximale d'un an peut être prononcée par le juge, ainsi qu'une amende, voire une peine de prison. Le texte prévoit en effet une amende de 1 500 €, doublée en cas de récidive. Dans les cas les plus graves de contrefaçon, le délinquant peut se voir infliger une amende allant jusqu'à 300 000 € et une peine de trois ans de prison.

Chapitre IV

L'entreprise, acteur majeur du cyber

L'époque où les cyber-attaques étaient le lot de quelques PME malchanceuses est bel et bien révolue. Très rentables pour les cyber-criminels car plus faciles à attaquer que les grands groupes, elles sont devenues une cible de choix. Au cours des douze derniers mois, 21 % des PME ont été victimes d'une cyber-attaque. Si le coût de celles-ci dépasse rarement les 10 000 €, il peut arriver dans de rares cas que l'entreprise victime ne s'en relève pas, notamment quand l'affaire devient publique (01/02/2019 – Damien Bancal[18]). En 2017, 76 % des ETI en France avaient subi au moins un incident. Notre propos consistera ici à identifier et caractériser les risques et menaces pesant sur elles, et nous tenterons de proposer des solutions leur permettant de les prévenir et d'y réagir.

Constats sur le terrain

Sur une population française totale de 67 millions en 2019, les actifs représentaient environ 30 millions, dont 27 millions en entreprise.

Une enquête menée au niveau européen par PwC précise les différences entre :

— **Grandes entreprises** (CA > 1 Md$) qui ont les moyens de se protéger :
  - *a minima,* ont mis en place une stratégie → niveau acceptable : 57,1 % (moyenne globale France : 49 %),
  - *a minima* ont nommé un RSSI → prise de conscience : 53 % (moyenne globale France : 48 %),
  - pas de RSSI identifié ni prévu → faible prise en charge du sujet : 15 % (moyenne globale France : 13 %) ;
— **Petites entreprises** (CA < 100 M$), où l'on pourrait parler d'un dialogue de sourds entre sécurité informatique et management :
  - *a minima,* ont mis en place une stratégie → niveau acceptable : 52,6 % (moyenne globale France : 49 %),
  - *a minima* ont nommé un RSSI → prise de conscience : 46 % (moyenne globale

18 https://www.zataz.com/proteger-vos-donnees-personnelles-en-2019/

France : 49 %),
- pas de RSSI identifié ni prévu → faible prise en charge du sujet : 25 % (moyenne globale France : 13 %).

Bien que la cyber-sécurité soit omniprésente dans les médias et les discours politiques et que des termes comme *malware* ou *hacker* soient devenus familiers au grand public et aux entreprises, les études[19] montrent que la majorité des petites entreprises françaises restent peu ou mal sécurisées.

Un début d'explication

On évoque souvent les attaques ayant ciblé de grandes entreprises connues, une entreprise au rayonnement national ou international étant bien plus visible qu'une TPE locale. Malheureusement, cela ne sert pas à sensibiliser les petites entreprises qui font pourtant face à des attaques ciblées désormais quotidiennes. Ce que l'on constate en effet, c'est que les PME ne se reconnaissent pas dans le profil des sociétés ciblées par les cyber-criminels et ne se sentent pas concernées par les mêmes problématiques. Une entreprise de quinze personnes pense ne présenter aucun intérêt pour des cyber-criminels, contrairement à un groupe de 4 000 personnes. Il faut cependant rappeler que ce n'est pas un effet du hasard si la charte d'utilisation des moyens informatiques de l'ANSSI a été élaborée spécifiquement à l'attention des petites et moyennes organisations.

Il existe de très nombreux groupes de cyber-criminels et autant de variétés de types d'attaque, les objectifs divers n'ayant en commun que leur caractère malicieux, essentiellement *faire du profit illégal, ou attenter aux intérêts stratégiques de la cible*. Les attaquants ciblent les très petites entreprises car plus vulnérables elles leur permettent à moindres frais de réaliser un profit. Les PME sont également ciblées car elles constituent un point d'entrée vers de plus grands groupes dont elles sont clientes ou fournisseurs. Comme dit Pierre Curien, directeur de France Doctor Web : *« Si les attaques touchant les petites entreprises étaient plus souvent mises en lumière, les sociétés de cette typologie se sentiraient plus concernées. »*

19 PwC Digital Trust Insight, Baromètre IPSOS PwC, étude Bessé / PwC Mars 2018.

Une « belle commande »

Encore un de ces matins ensoleillés qui font le charme de la région. Il est temps de se rendre sur les parcs à huîtres car la marée n'attend pas. Ce matin, René, notre ostréiculteur, a une grosse commande à expédier. Hier soir, il a reçu par mail de son commanditaire habituel une demande un peu particulière, mais bon, il lui a répondu qu'il ferait tout son possible pour l'honorer.

Au retour des parcs, la mise en cagette des deux tonnes d'huîtres ne prend que quelques heures et le livreur est déjà prêt à faire la route jusqu'en Espagne. Cette fois ci, le lieu de livraison a changé, mais bon, ce sont des choses qui arrivent. La journée se poursuit, il reste à envoyer la facture…

Deux jours plus tard, le jeudi, nouvelle commande de son commanditaire. René en profite pour l'appeler…
« Alors, cette commande de mardi ? Ça vous a plu ? »
« Quelle commande ? Je ne vous ai rien commandé depuis trois semaines !
« Mais si, votre message de lundi, les deux tonnes d'huîtres ? »
« Je ne vous ai jamais envoyé de message lundi, j'étais au Maroc depuis samedi. Je suis rentré mardi soir. J'ai même mis des photos sur ma page Facebook ».
René commence à réaliser qu'il vient de se faire escroquer… Quelqu'un s'est fait passer pour son commanditaire. En reprenant l'adresse mail de sa commande, il s'aperçoit alors qu'elle est légèrement différente… Encore une usurpation d'identité. Le cyber-criminel a observé les échanges de l'ostréiculteur et a surveillé le commanditaire. Un cas assez classique d'infraction pénale commise à l'encontre d'une petite entreprise. Cette attaque aurait pu tout aussi bien prendre la forme d'un rançongiciel (ransomware) cryptant les données de son ordinateur.

Contexte

Qu'il s'agisse de petites et moyennes entreprises (PME) ou de très petites entreprises (TPE), leur caractéristique commune est une centralisation de la gestion de la société. Elles en font un véritable atout de compétitivité, car du fait de leurs ressources humaines réduites, ces sociétés sont bien plus réactives et flexibles que les structures des grands groupes. Pour contextualiser réellement les TPE et les PME, qu'on a souvent tendance à confondre, mais qui sont pourtant différentes, il convient de les définir avec précision.

Il est d'usage de qualifier de TPE toute structure entrepreneuriale dont le nombre de salariés est inférieur à dix et dont le chiffre d'affaires annuel HT (ou le total du bilan) ne dépasse pas un plafond de deux millions d'euros. Cette forme d'activité est dans la grande majorité des cas une entreprise sans salarié. Il s'agit alors d'une « micro-entreprise » (ou auto-entreprise). Cette forme d'organisation correspond au besoin de travailleurs non salariés comme les artisans, les commerçants ou les professions libérales. Ainsi, n'exigeant pas l'apport d'importantes ressources humaines ou financières, les TPE constituent l'essentiel des créations d'entreprises en France. Près de 93 % des sociétés créées en France seraient des micro-entreprises, qui bénéficient, en particulier, d'un régime fiscal spécifique, qui est semble-t-il en voie de normalisation notamment pour les auto-entrepreneurs.

Par comparaison avec la TPE, la PME se démarque par sa taille. À ce jour, il n'existe pas de définition précise pour ce type d'entreprise. La définition qui semble toutefois s'imposer est celle de la recommandation européenne n° 96/280/CE du 3 avril 1996 modifiée par la recommandation n° 2003/361/CE du 6 mai 2003. Textes qui organisent une classification des entreprises en fonction de leur taille et de leur chiffre d'affaires. Sont donc définies comme « petites entreprises », les sociétés dont l'effectif se situe entre 10 et 50 salariés et dont le chiffre d'affaires

(ou le bilan total) n'excède pas 10 millions d'euros HT par an. Entre 51 et 250 salariés, on peut définir des « moyennes entreprises » avec un chiffre d'affaires inférieur à 50 millions d'euros HT et un bilan total maximum de 43 millions d'euros HT. Au-delà de 250 salariés, on parlera d'entreprises de talle intermédiaire (ETI).

Selon une étude de PwC[20], la cyber-sécurité est aujourd'hui un enjeu pour moins d'un tiers des entreprises françaises, dont les ⅔ considèrent d'ailleurs que le risque d'une cyber-menace n'est pas important. Il en ressort aussi, et c'est peut-être le plus grave, que seules deux entreprises sur dix se sentent tout à fait capables de gérer une cyber-attaque. Pour compléter le tableau, moins d'une entreprise sur cinq a véritablement mis en œuvre les mesures de protection possibles, et 95 % des entreprises ne comptent pas engager de personne dédiée à la cyber-sécurité dans les douze prochains mois.

Les risques cyber sont de deux ordres :
- risques directs sur l'environnement technique des technologies de l'information et de la communication (TIC), comme par exemple une attaque par déni de service qui va bloquer l'utilisation des ordinateurs, ou l'inoculation d'un virus ;
- risques plus «classiques» qui concernent des environnements utilisant les TIC. Le plus connu est l'arnaque au président qui aura pour support un faux ordre de virement par mail.

On voit bien que la problématique de sécurité ne peut pas se résumer à un simple renforcement des TIC.

La meilleure définition de l'espace numérique est « *L'ensemble des paradigmes qui sont utilisés afin de fournir le service que l'on attend d'une machine numérique* ». Ces paradigmes, à partir desquels l'espace numérique s'est développé, sont au nombre de quatre :
- l'électricité, au sens « d'ions » positifs et négatifs, et de toutes les propriétés qui en découlent : transport d'énergie, mais aussi électromagnétisme, ondes radios, rayonnement, etc.
- la conception de toute machine numérique qui reprend tout ou partie de l'architecture type définie par von Neumann ;
- la communication, qui peut être schématisée de la manière suivante : la transmission d'un message nécessite le fait d'avoir un émetteur et un récepteur, qui codent et décodent un message transmis au moyen d'un canal de transmission ;
- la donnée avec ses trois propriétés souhaitables : disponibilité, confidentialité et, enfin, intégrité.

De la sécurité informatique… à la cyber-sécurité

À l'aube du monde numérique, on a des machines numériques imposantes qui nécessitent une installation dans des lieux dédiés. Elles sont chères, comme tous les périphériques qui s'y rattachent. Elles sont administrées par des personnels qualifiés et nécessitent une surveillance

20 PWC, Les entreprises face aux enjeux de la cyber-sécurité, 2018.

permanente. Leurs accès logiques sont réduits faute de potentiel d'accès, celui-ci étant très limité par les possibilités de débit. Il en résulte que seules des fonctions pouvant être numérisées sont développées et traitées sur ces machines à la ressource contrainte.

Les centres informatiques, véritables « bunkers » physiques, vont surtout offrir une protection physique assurant une bonne disponibilité. Un personnel nombreux et qualifié y est employé. Les utilisateurs du système sont au mieux connectés en filaire pour traiter quelques informations. Au pire, ils lancent des traitements « batch » qui leur sont restitués sous forme de documents imprimés (listings). Aucune ressource de traitement n'est délocalisée. Les protocoles réseau sont rigides et complexes, mais facilement traçables. Les débits sont limités. La disponibilité est la grande priorité. Cet environnement technique, lourd, nécessite des ressources importantes et spécialisées, avec une sécurité physique et technique. C'est un monde technique fermé, mis en œuvre par des spécialistes et dont les utilisateurs « attachés » à un centre de traitement doivent respecter les règles et les contraintes.

Dans les TPE et PME, l'investissement numérique est rare et spécifique. Les machines doivent être installées par des prestataires confirmés. L'ensemble de la gestion du système est en général confié à un spécialiste pour les structures suffisamment importantes ou totalement sous-traité à un prestataire de service.

Au cours des vingt dernières années, les quatre paradigmes ci-dessus ont subi des évolutions drastiques.

L'électricité a vu l'utilisation de ses propriétés développée , notamment en termes de consommation d'énergie, d'électromagnétisme, de rayonnement, d'ondulation…

La machine de von Neumann, a pu être réduite, miniaturisée et renforcée. Elle entre dans des appareils très petits, transportables, puis portatifs, de plus en plus robustes et ne nécessitant pas un environnement aseptisé. En outre, les systèmes peuvent maintenant être préconfigurés, leur coût devenant de plus en plus réduit, ils sont proposés au grand public par les canux commerciaux généralistes, et qsans soute le plus important, ils peuvent être mis en œuvre par des non-spécialistes.

Les communications aussi ont subi des évolutions phénoménales, en termes de support et d'appareillage. Les débits s'accroissent et les protocoles sont plus simples. L'ensemble combiné permet alors dans le « dernier kilomètre » une diffusion « sans fil » rendant obsolète toute forme de connexion physique : plus besoin d'une compétence réseau pour les mettre en œuvre.

En ce qui concerne la donnée, sa disponibilité est assurée par des médias de plus en plus performants, miniaturisés et peu chers, et sa confidentialité semble assez simple à assurer. De fait, son intégrité devient le nouvel enjeu de la sécurité.

Il ressort de ces évolutions une vulgarisation complète de la technologie numérique devenue simple et bon marché, accessible à tous. On peut tout numériser, donc tout est numérisé. Le pouvoir qui était autour du système informatique se déplace des experts et des spécialistes vers des utilisateurs finaux qui n'ont plus besoin de connaître les technologies, toute la gestion du monde numérique étant dévolue à l'utilisateur final. Mais si les technologies ont évolué pour lui rendre cette gestion transparente, elles ouvrent autant de voies à des activités frauduleuses friandes de sa fragilité. Exit les bunkers sécurisés où étaient gardées les machines de traitement. Exit les protocoles qui permettaient de suivre le cheminement des trames. Grâce à une discrète gestion en amont de la complexité par des spécialistes, l'utilisateur final vit maintenant dans un monde technologique ouvert, qui peut être mis en œuvre sans compétences particulières.

Confrontés à l'évolution de ces paradigmes, on peut comprendre le désarroi des patrons de TPE et de PME. Les quatre piliers du numérique leur sont devenus les quatre cavaliers de l'Apocalypse. D'où la nécessité d'une cyber-sécurité.

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

La transition

Après ces lourds constats, comment identifier quelques axes de progrès qui permettraient d'amener les chefs d'entreprises à mieux appréhender ces évolutions. La cyber-sécurité doit être abordée, non pas comme un problème technique, mais comme un problème sociétal et organisationnel. Le chef d'entreprise doit s'en daisir en y associant le responsable informatique, pour celles qui en ont un, ou leurs prestataires pour les autres. Ce sont les acteurs incontournables de cette démarche, mais pas les seuls.

Il revient dans un premier temps au chef d'entreprise de recenser l'intégralité de ses risques. Couvrant tous les domaines de l'entreprise, cette démarche nécessitera une analyse fine. En fonction de celle-ci, le dirigeant d'une entreprise devra commencer par améliorer sa sûreté puis sa sécurité[21], afin de réduire l'ensemble des risques initialement identifiés, voire même en transférer une partie vers un assureur spécialisé dans le domaine concerné, rendant alors son risque acceptable. À noter cependant que le secteur assurantiel est lui-même en proie à d'importantes interrogations en raison de la nouveauté de ce type de risque : la profession

21 https://surete.securitas.fr/questions-frequentes/difference-surete-securite

ne maîtrise pas encore la complexité des risques à couvrir et n'a pas encore conçu le modèle économique idoine. Les solutions que le chef d'entreprise va mettre en œuvre auront toutes un coût pour son entreprise. Pour le rendre acceptable, il devra le comparer à celui qu'entraînerait un sinistre dû aux risques identifiés et évalués lors de l'analyse.

Les moyens mis en œuvre pour la cyber-sécurité devront être acceptés par l'ensemble des acteurs de l'entreprise. Si une protection n'est pas acceptée par la globalité des collaborateurs, les moyens mis en œuvre peuvent s'avérer d'une inefficacité redoutable. La mauvaise appropriation des outils de protection peut être illustrée par le cas récent d'un établissement public qui avait équipé ses collaborateurs de téléphones sécurisés. Or, afin de simplifier leur relations professionnelles, ces collaborateurs communiquaient entre eux via leurs téléphones personnels, rendant inopérante la sécurisation des échanges…

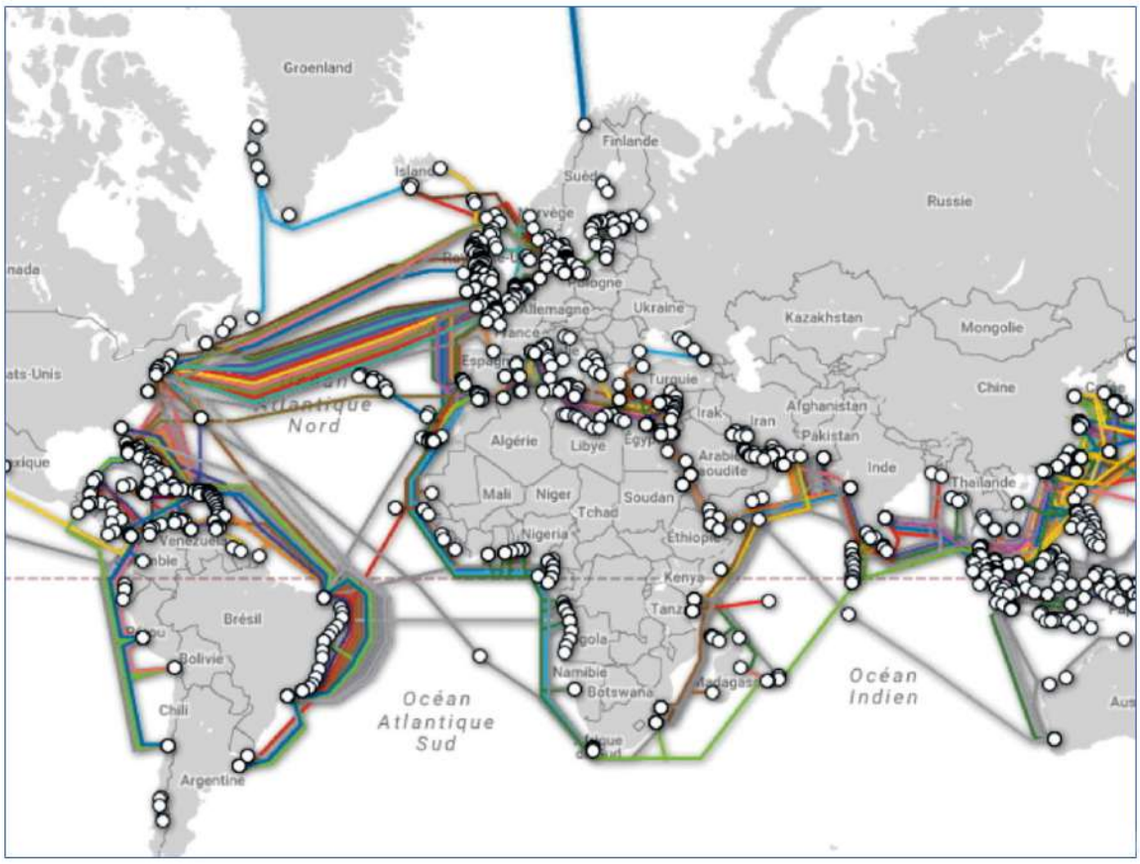
Les objectifs et leurs modalités ne peuvent être définis que par le chef d'entreprise, et c'est sans doute là que se pose le dilemme le plus difficile pour lui.

DE LA CYBER-SÉCURITÉ AU CYBER-MONDE

L'évolution des comportements et l'impact sociétal de la cyber-sécurité nous contraignent à envisager cette question dans un environnement élargi, et il faut donc faire appel à la notion de cyber-culture.

L'outil Internet ne peut être appréhendé que dans sa diversité. On peut considérer qu'il est constitué au minimum de quatre couches indépendantes : physique, logique, applicative et cognitive, et il faut appréhender la diversité des enjeux géopolitiques, économiques, environnementaux et juridiques liés à chacune de ces couches.

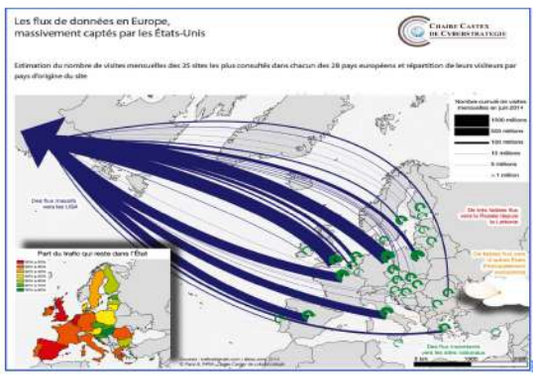
La couche physique : quel que soit le mode de transmission, Internet est tributaire des infrastructures réseau que sont (très majoritairement) les câbles sous-marins, les répétiteurs, etc., vulnérables par nature, et qui peuvent fournir des débits plus ou moins importants. Elles se trouvent par ailleurs très souvent dans des zones à fort enjeu géopolitique. Les usagers de l'Internet sont donc confrontés à une dilemme : avoir accès au plus grand nombre possible de données et ne pas être tributaires de crises politiques.

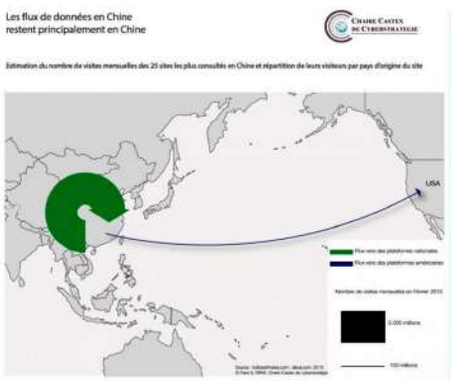


Eurafibre - Carte mondiale des câbles sous-marins

L'un des enjeux majeurs de cette couche physique est communément désigné sous l'expression de « principe de neutralité » et consiste à garantir une égalité de traitement quel que soit le flux de données. Il correspond au respect de l'exercice des deux libertés fondamentales que sont d'une part l'accès à l'Internet et d'autre part l'égalité à cet accès. Aboli par le Président Trump en 2018, il a été rétabli en 2019 par la Chambre des représentants au travers du *« Save the Internet Act »*, sous réserve de validation par le Sénat américain.

La couche logique : c'est la structure logique d'Internet, celle qui permet d'assurer la transmission des données et qui repose sur un langage commun à tous les ordinateurs (TCP/IP). Elle comprend, notamment, le routage (choix de la route des données), le nommage (nom des éléments réseau et des usagers) et l'adressage (transformation du binaire en mots intelligibles). Elle est actuellement sous domination des États-Unis et structurée en un maquis d'organes sous la tutelle de l'ICANN *(Internet Corporation for Assigned Names and Numbers)*. Cet organisme privé d'autorégulation est soumis au respect du droit américain, du fait de l'implantation de son siège social sur le territoire des États-Unis.





Source : Chaire Castex de cyber-stratégie

On ne peut qu'être interpellé par la différence de volume des échanges de données au sein du bloc occidental et de celui-ci avec la Chine (cartes Chaire Castex). Le contrôle des données de l'Europe ne devrait-il pas commencer par une inflexion sérieuse de notre dépendance majeure aux seuls États-Unis ?

La couche applicative : elle correspond aux outils permettant la mise en œuvre d'usages, indépendamment de toute connaissance informatique : web, emails, moteurs de recherche, réseaux sociaux… Elle fournit également des instruments puissants développant les possibilités du « *data mining* » grâce au « *big data* » dans le « C*loud* », permettant de répondre aux types de questions suivantes : *Qui je suis – Ce que je fais – Quand et comment je le fais – Où je le fais et avec qui …* On ne peut ici, que se poser une nouvelle fois la question de la dépendance durable de la France vis-à-vis d'outils gouvernés par des principes éthiques qui relèvent d'une conception sociétale ultra-libérale, bien différente de notre modèle national.

La couche cognitive : c'est la plus subtile, celle des usagers, des interactions sociales, des discussions et des échanges entre humains, la plus complexe à cartographier : celle de l'influence, « *fake news*[22] », des appels aux révolutions, du harcèlement, de la théorie du complot, de la manipulation de masse…

En synthèse, on observe que chaque couche de l'Internet introduit des questions juridiques nouvelles, avec des enjeux complexes et parfois contradictoires à concilier :

- liberté d'expression (principe fondamental du net) *versus* demande de sécurité ou contenus illégaux (pédophilie, réseaux terroristes, fake médicaments…),
- demande de protection de la vie privée *versus* sécurisation du commerce en ligne pour les consommateurs…

Ces enjeux nécessitent des réponses adaptées, notamment en droit de la concurrence comme en témoigne l'initiative du CNAC [Comité national anti contrefaçon] pour appréhender les

22 Le terme Fake news, pris au sens propre a le sens de fausses nouvelles, et sous-entend désinformation et propagande. Mais il a été détourné de son sens par la présidence américaine qui qualifie de fake news toutes les informations vraies qui le gêne et propose alors ses « Alternative facts » syntagme forgé par Kellianne Conway. On est dans la désinformation au carré et cela met bien en évidence la complexité du sujet.

contrefacteurs grâce au traçage des transactions financières : « *Follow the money* ». De même pour la propriété intellectuelle, en remettant en question la qualification d'auteur (exemple d'une IA à l'origine de « *The next Rembrandt* »). Face à la rigidité du droit, il semble nécessaire de recourir à de nouveaux modes de réglementation plus incitatifs et plus souples (cf. opposition classique entre la « *Hard law* » et la « *Soft law* »).

Au regard de ces évolutions, on peut constater que les risques concernent aussi bien les grandes que les petites entreprises, et sont universels. En revanche, les enjeux propres aux TPE/PME sont plus critiques du fait de leur surface financière réduite, du manque de compétence locale, de leur moindre résilience liée à la continuité d'activité, du risque de volatilité des clients.

Le « monde cyber » est l'univers des professionnels de ce secteur d'activité. Nouveau paradigme, il se caractérise par un envahissement du monde réel par le cyber, que ce soit volontaire ou pas. Cette omniprésence entraîne une série de failles sécuritaires. Elle pose une série de problèmes en termes de confidentialité et d'intégrité de nos données, et nécessite toute une série de changements dans nos modes de fonctionnement, quelle que soit l'activité exercée.

Mise en œuvre : la cyber-attitude

Au-delà des solutions techniques qui sont à construire et mettre en œuvre par les spécialistes du domaine, il est impératif de revoir l'organisation de l'entreprise. De plus, les composants « numériques » pouvant être aussi bien personnels que professionnels, de même que leur usage et leur cadre d'utilisation, ils présentent le risque de ne plus être protégés par les équipements techniques mis en œuvre dans le seul environnement professionnel. Il faut donc revoir leurs règles d'usage, et il devient nécessaire de sensibiliser chacun des collaborateurs pour développer au sein de l'entreprise une *conscience collective*.

Des outils de prévention existent à disposition des TPE et PME. L'ANSSI a ainsi identifié douze règles essentielles pour la sécurité des systèmes d'information des petites et moyennes entreprises[23]. Elle a également publié un guide sur les bonnes pratiques à l'usage des professionnels en déplacement[24] ainsi qu'un guide pour la protection du potentiel scientifique de la Nation[25]. Malheureusement, aussi pertinents que soient ces documents, l'expérience montre que la probabilité pour que leur cible première (salariés des TPE et PME) en prenne connaissance et s'en inspire est plutôt faible. En général, les directeurs de systèmes d'information en feront une copie disponible sur l'intranet de l'entreprise. Et à partir de là, à chaque salarié de la consulter. Que faire dès lors ? Il faudra agir sur plusieurs volets : la formation, la sensibilisation et le droit.

Trop souvent, les questions de sécurité cyber sont considérées comme relevant de la compétence exclusive des informaticiens. Or, le développement d'une hygiène en la matière est l'affaire de chacun. Il ne s'agit plus, ici, de sécurité informatique. La démarche de cyber-sécurité va bien au-delà et s'inscrit dans une échelle de temps long. L'expérience a montré que la sensibilisation

23 ANSSI, CPME, Guide des bonnes pratiques de l'informatique, 12 règles essentielles pour sécuriser vos équipements numériques, 2017.

24 ANSSI, Sécurité numérique bonnes pratiques à l'usage des professionnels en déplacement, 2019.

25 ANSSI, Protection du potentiel scientifique et technique de la Nation - Guide méthodologique, 2018.

des acteurs économiques et leur mobilisation ne se déclenchent que grâce à certains relais qui ne sont ni les acteurs institutionnels (13 Régions, 96 départements et collectivités de métropole, les 5 territoires ultra-marins et l'ANSSI) ni les professionnels (MEDEF, la CPME et l'U2P malgré leur 77, 250 et 120 fédérations métiers), mais plutôt des relais financiers comme les assureurs et les experts-comptables qui jouent un rôle critique et majeur : les enjeux d'une cyber-attaque sont multiples, mais ceux de nature financière sont sans conteste un facteur déterminant dans la prise de conscience au sein de toute entreprise.

En tant que prescripteurs, les assureurs sont en première ligne afin de sensibiliser les TPE et PME et les inciter à former leurs équipes. La difficulté actuelle est l'absence à ce jour d'une politique enfin claire des assureurs quant à leur offre : quelles conséquences aura pour un assuré le non-respect des règles élémentaires de cyber-sécurité ? Y aura-t-il augmentation de la prime ? Cela entraînera-t-il une déchéance de l'indemnisation ? Il serait probablement utile d'analyser comment les assureurs ont élaboré leurs polices environnement il y a plusieurs années afin de s'en inspirer. De même, leurs questionnaires de « compliance cyber » pourraient être des guides utiles aux TPE/PME.

Les experts-comptables aussi ont un rôle de prescripteur à jouer en mettant en avant les impacts financiers d'une cyber-attaque. Quelles seraient les conséquences sur le compte d'exploitation ? celles d'une condamnation pour divulgation de données à caractère personnel suite à un piratage ? Voilà des éléments qui sont pris en compte par les acteurs bancaires quand il s'agit d'emprunts, de renégociation de crédits…

Le dernier aspect, enfin, sur lequel il est possible d'agir est le volet juridique. Les questions liées à la formation et aux guides d'utilisation des systèmes d'information relèvent de la *« Soft law »*. Cependant, ce type de droit ne suffit pas à lui seul car il présente des difficultés de mise en œuvre et de mesure des effets. Il sera donc nécessaire de compléter les dispositifs par des mesures contraignantes. Par exemple, les compagnies d'assurance devraient formaliser leur politique en matière de couverture des risques cyber en détaillant comme condition préalable les mesures de prévention et de formation à mettre en œuvre, et en précisant aussi les critères de déchéance d'indemnisation, de hausse des primes, etc.

En outre, de même qu'il est pratiqué en matière de protection de l'environnement (ISO 26000), le législateur pourrait imposer aux entreprises d'une certaine taille de rendre compte (reporting) avec un déclaratif cyber comme cela se fait déjà en matière de RSE[26], dont on a simplifié et assoupli les modalités avec le décret de 2017[27] : une déclaration de performances extra financières (DPEF) incorporée dans le rapport annuel en constitue désormais la principale obligation.

26 Article L225-102-1 C. com.

27 Décret n° 2017-1265 du 9 août 2017 pris pour l'application de l'ordonnance n° 2017-1180 du 19 juillet 2017 relative à la publication d'informations non financières par certaines grandes entreprises et certains groupes d'entreprises, JORF du 11 août 2017.

Ces recommandations sont devenues indispensables au regard des enjeux de pillage économique et d'espionnage industriel, ainsi que des problèmes soulevés par l'extra-territorialité du droit des États-Unis qui ont entraîné la planète dans une ère de protectionnisme judiciaire. Alors que la règle de droit a, de tout temps, servi d'instrument de régulation, elle est devenue aujourd'hui une arme dans la guerre de suprématie économique que mènent les États-Unis contre le reste du monde, y compris leurs alliés traditionnels en Europe. Depuis la fin des années 90, on assiste à une prolifération de lois à portée extraterritoriale, essentiellement d'origine américaine, permettant aux autorités de la première puissance mondiale d'enquêter, de poursuivre et de condamner dans le monde entier sur des fondements divers, les pratiques commerciales d'entreprises ou d'individus qui leur déplaisent.

Force est de constater, comme l'a fort justement fait remarquer le député Raphaël GAUVAIN. dans son rapport[28], que « ces procédures informelles conclues par des accords touchent d'abord et avant tout des entreprises non américaines : le tableau montre qu'en matière de lutte contre la corruption d'agents publics étrangers, les autorités américaines utilisent leurs pouvoirs pour viser en priorité des entreprises non américaines et assez souvent européennes. » Ces lois se sont ajoutées à des procédures civiles et pénales très intrusives ou exerçant une forte pression sur les personnes mises en cause, et qui permettaient déjà d'obtenir hors de tout mécanisme d'entraide, et donc hors de tout contrôle des autorités françaises, une quantité importante de données relatives à nos entreprises.

La création du Parquet national financier en 2014, la loi Sapin 2 en 2016 puis la circulaire sur les procédures miroir en 2017 ont permis quelques avancées, encore insuffisantes, pour rétablir notre souveraineté judiciaire. Ces dispositifs s'avèrent aujourd'hui trop datés et encore insuffisants pour contraindre les autorités étrangères à respecter les traités d'entraide et les accords de coopération internationale, lorsqu'elles décident d'obtenir des documents ou des informations sur nos propres entreprises. Comme le souligne le rapport parlementaire de 2019 *« Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale »*[29], il faut rester lucide et ne pas faire preuve de naïveté car la situation actuelle empêche de facto nos entreprises de commercer librement.

Jusqu'ici, l'impact des sanctions économiques américaines est resté limité compte tenu des cibles visées, relativement marginales dans l'économie mondiale, mais le comportement actuel de la présidence américaine nous amène très logiquement à devoir nous interroger. Le risque cyber apparaît en effet ici dans un contexte inattendu, qui n'est ni celui de la dégradation des systèmes d'information des entreprises ni celui d'une intrusion malicieuse dans ces systèmes,

28 https://www.dalloz-actualite.fr/flash/rapport-gauvain-sur-protection-des-entreprises-contre-sanctions-americaines#.XmC_P6hKjic

29 https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000532.pdf

mais celui d'une récupération abusive des données stockées en France par des personnes défendant des intérêts étrangers. Selon le rapport parlementaire, *« Tout écart entre sanctions américaines et sanctions européennes crée ainsi pour les entreprises européennes un risque juridique majeur »,* et il recommande donc :

- de protéger la confidentialité des avis juridiques en entreprise par la création d'un statut d'avocat en entreprise, relevant de la déontologie de l'avocat ;
- de moderniser la loi de blocage datant de 1968 ;
- d'adopter une extension du RGPD aux personnes morales afin de protéger les entreprises françaises contre la transmission de leurs données par leurs hébergeurs à des autorités étrangères.

Toutes ces remarques et préconisations illustrent bien les problèmes que rencontrent plus que d'autres nos TPE et PME : tournées vers une productivité indispensable à leur survie, elles n'ont d'autre choix que le recours à une technologie qui a évolué sur les axes divergents décrits plus haut. Ce grand écart leur impose une réflexion qui relève non seulement d'un aspect technologique mais aussi et au moins autant d'un aspect sociétal.

Principales entreprises condamnées au titre du FCPA* entre 2008 et 2018

	Entreprise	Pays	Année	Amende(M$)
1	Siemens	Allemagne	2008	800
2	Alstom	France	2014	772
3	Telia	Suède	2017	691,6
4	KBR/Halliburton	États-Unis	2009	579
5 T	eva Pharmaceutical	Israël	2016	519
6	OCH-ZIFF CXapital Mngt	États-Unis	2016	412
7	BAE	Royaume-Uni	2010	400
8	Total	France	2013	398,2
9	Vimpelcom	Pays-Bas	2016	397,5
10	Alcoa	États-Unis	2014	384
11	ENI/SNAMPROGETTI	Italie	2010	365
12	Technip	France	2010	338
13	Société Générale	France	2018	293
14	Panasonic	Japon	2018	280
15	JP Morgan Chase	États-Unis	2016	264
16	Odebrecht/Braskem	Brésil	2017	260
17	SBM Offshore	Pays-Bas	2017	238
18	JGC Corporation	Japon	2011	218,8
19	Embraer	Brésil	2016	205,5
20	Daimler	Allemagne	2010	185
21	Petrobras	Brésil	2018	170,6
22	Rolls-Royce	Royaume-Uni	2017	170
23	Weatherford	Suisse	2013	152,6
24	Alcatel	France	2010	138

* FCPA : https://fr.wikipedia.org/wiki/Foreign_Corrupt_Practices_Act

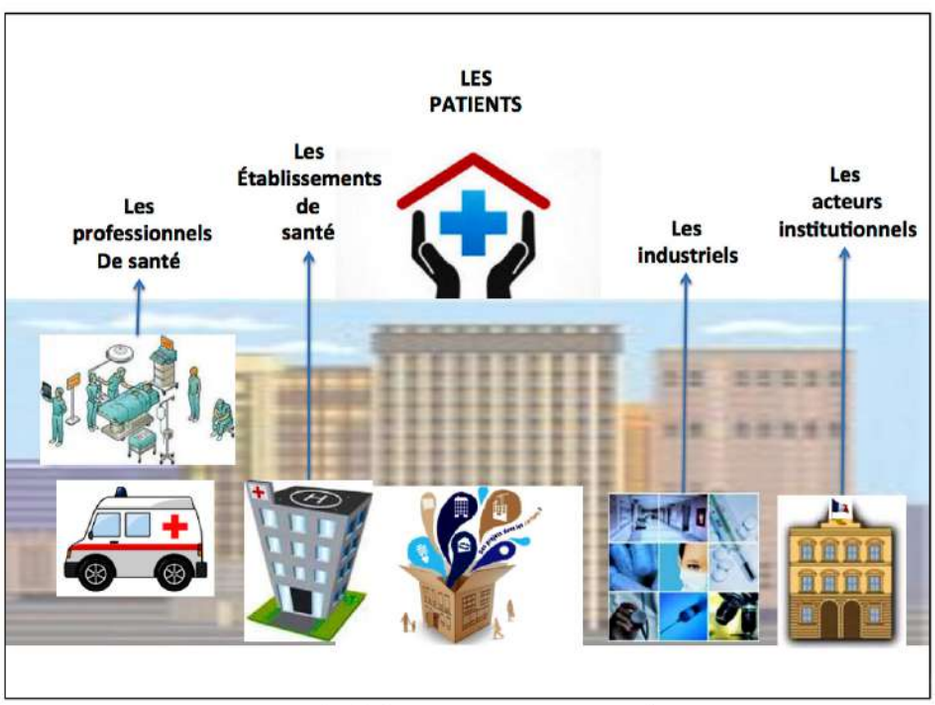
Source : Cabinet Ikarian 2018

Chapitre V

Le cyber en santé, un exemple de progrès

En septembre 2001 avait lieu l'opération Lindbergh, première intervention de télé-chirurgie réalisée avec succès par une équipe chirurgicale située à New York sur une patiente se trouvant dans un service des hôpitaux universitaires de Strasbourg. Sans univers cyber pas de télémédecine. Au-delà de l'exploit médical, la prouesse technologique a démontré une maturité technologique qui a permis de développer d'autres formes de télémédecine. Depuis la personne âgée en Ehpad consultant un spécialiste en cardiologie avec le flux de son ECG (électrocardiogramme) transmis en temps réel, jusqu'au pompier en intervention utilisant des lunettes connectées permettant au médecin régulateur du SAMU de le guider dans ses gestes, les exemples de services à forte valeur ajoutée sont légion.

En santé, le partage d'information est essentiel à la bonne prise en charge des patients, mais il n'est possible que si la confiance existe, le patient se trouvant au centre d'un écosystème :



Source : Ministères et Agences gouvernementales

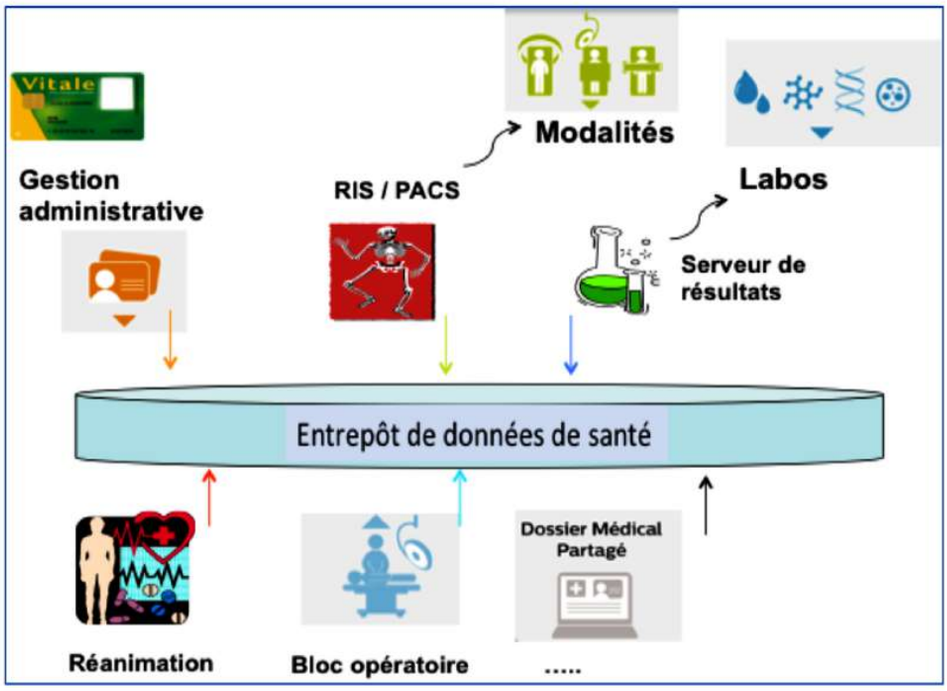
Si, pour simplifier l'analyse, nous nous focalisons sur le milieu hospitalier, nous voyons que l'établissement de santé producteur de soins est dépendant des directives des institutions régaliennes et des industriels fournisseurs de solutions applicatives, pour répondre aux besoins de délivrance de soins dans le système d'information hospitalier (SIH), l'essence même d'un système d'information de santé (SIS) étant de mettre à disposition l'information clinique où et quand on en a besoin. Or la « data » est aujourd'hui ce qu'était le pétrole hier, et la donnée personnelle de santé, est l'une des informations les plus convoitées de nos jours. Outre le fait qu'il représente un réel marché pour les acteurs directs et indirects, l'écosystème hospitalier est donc source de convoitise.

La cyber-sécurité à l'échelle des établissements producteurs de soins est devenue une priorité nationale. 700 incidents ont été signalés sur deux ans, menace soulignée en son temps par la ministre Agnès Buzyn. Dans le projet de loi de santé présenté en conseil des ministres, le plan *« Ma santé 2022 »* propose une transformation structurelle et organisationnelle dont l'un des chantiers — la territorialisation du système de soins — met les centres hospitaliers au sommet d'une approche pyramidale.

À ce jour, nous sommes dans la phase finale de mise en place des groupements hospitaliers de territoire (GHT), dispositif introduit par la loi de santé de 2016 qui prévoyait une coopération entre les établissements de santé autour d'un projet médical pour rendre plus efficient le processus de soins.

Nous sommes à l'aube d'une transition numérique qui inclut la télémédecine, les applications mobiles médicales ainsi que les objets connectés biomédicaux. Il faudra mettre à disposition l'information clinique où et quand le besoin se fait sentir, en fonction des mouvements du patient entre les différents établissements de santé du territoire français. Tout l'enjeu est là, avec des niveaux de sécurité qui s'imposent pour les « data », les données de santé à caractère personnel, qui devront circuler sur la toile.

Une première étape est le recueil de ces données autour d'un dossier patient informatisé :

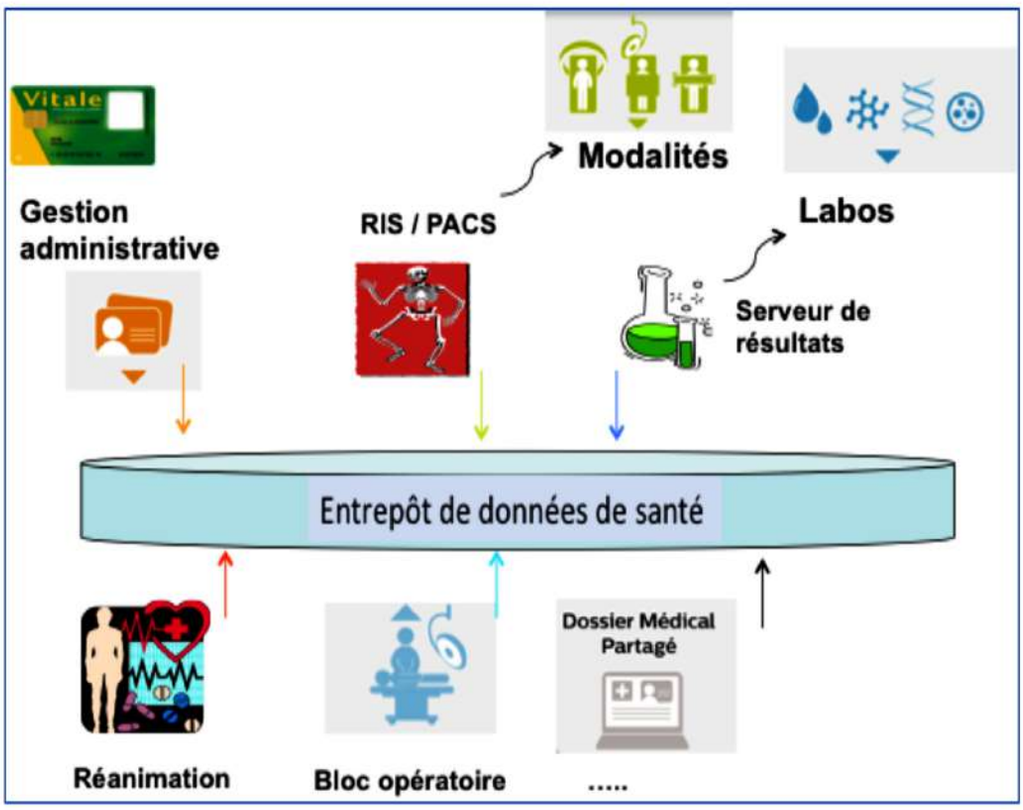


Source : PCI-RPH SAS

Le deuxième niveau, bien compris par les GHT, est de créer un entrepôt de données de santé commun : il devra être accessible au travers d'un système d'information qui en permette l'échange et le partage en toute sécurité. Ces données de santé sont en effet à caractère personnel et, donc, sensibles, leur accès étant encadré par la loi pour protéger les droits des personnes. Elles doivent être stockées dans un *Data center* agréé, un *hébergeur de données de santé* (HDS) (L.1111-8 du code de la santé publique, modifié par la loi n° 2016-41 du 26 janvier 2016). La clé consiste donc à pouvoir accéder aisément aux données du patient présentent sur le réseau tout en assurant strictement leur confidentialité, leur intégrité et leur sécurité.

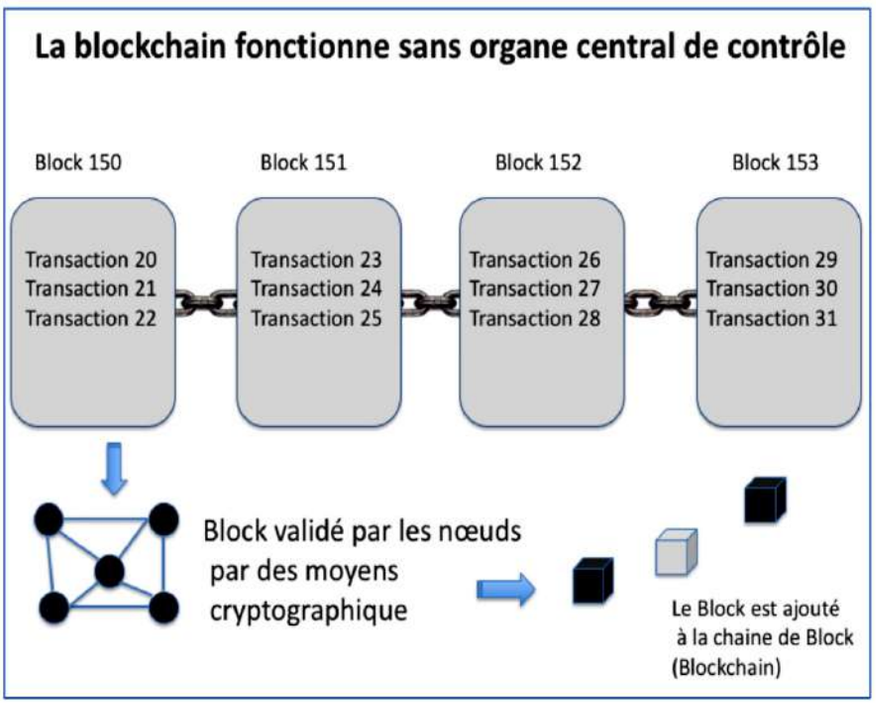
La clé de voûte du système d'échange et partage est l'identifiant patient, pour lequel l'utilisation de l'identifiant national de santé (INS) est un critère de la bonne qualité. Chaque établissement utilise quant à lui un numéro de sécurité sociale, le numéro d'inscription au répertoire (NIR).

Le regroupement des données dans un entrepôt commun nécessite la mise en place d'un identifiant de territoire basé sur l'INS pour servir de clé de référence : cet entrepôt de données devra être interopérable dans sa région sanitaire et à terme permettre une consolidation nationale des données. Des mesures de sécurité, et tout particulièrement la traçabilité des accès, devront être prises pour éviter que l'INS ne soit diffusé plus que nécessaire, risque majeur bien identifié par la CNIL.



Source : PCI-RPH SAS

Outre la mise en place d'un processus d'identification forte, d'hébergeurs agréés HDS et du RGPD, nous manquons encore d'un « tiers de confiance » qui puisse améliorer la sécurité. En effet, les systèmes d'information de santé (SIS) ne sont pas architecturés à ce jour de manière à pouvoir interagir les uns avec les autres, les registres de données étant plus ou moins propriétaires. Faute de truver un oiseau rare, la *blockchain* pourrait jouer ce rôle . Elle répondrait au besoin d'un tiers de confiance neutre (resterait à gérer le droit à l'oubli pour un patient) et d'une réduction des coûts, en sécurisant les transferts de données entre les institutions de santé : l'ensemble des acteurs du système de santé : hôpitaux, recherche, laboratoires d'analyses médicales, pharmacies et centres d'imagerie pourraient stocker et partager les données de santé, les problèmes d'interopérabilité étant résolus par un processus sécurisé.



Source : Blockchain France

La blockchain garantit l'anonymat des patients grâce à son système de clés publiques et de clés privées, l'identifiant unique du patient étant seul visible. Grâce à sa transparence et son inaltérabilité, la blockchain serait un excellent outil pour garantir la traçabilité des accès aux données médicales.

Cette approche technologique peut être enrichie par l'apport de l'intelligence artificielle (IA), ce qui serait possible dans ce système avec la mise en place d'algorithmes de *machine learning* qui travailleraient plus vite que l'humain sur des volumes de données incommensurables. Bien que le médecin garde le dernier mot et sa suprématie dans le raisonnement, nous ne pouvons pas ignorer l'avantage d'un docteur « augmenté » : *Docteur + IA*.

Le courriel, outil de notre quotidien, sera traité dans un espace de confiance, MSSanté, au sein duquel les professionnels habilités à échanger des données de santé, en ville comme à l'hôpital, pourront le faire de manière dématérialisée en toute sécurité. MSSanté facilitera les échanges interprofessionnels et accélèrera l'usage du numérique en santé. Quid, alors, des échanges vers d'autres acteurs légitimes comme les avocats, dans le cadre de dossiers d'indemnisation par exemple, vers la justice… tout en maintenant l'imperméabilité vis-à-vis d'acteurs non autorisés ? Là aussi, la blockchain pourrait être un élément de réponse, au-delà du cadre réglementaire et organisationnel indispensable.

SANTÉ, CYBER ET DROIT

L'Internet des objets, *Internet of Things* (IoT), est devenu aujourd'hui « l'Internet of everything » disait la ministre Florence Parly en conférence plénière du FIC 2018. Si les propos peuvent

paraître anodins, ils signifient en réalité que, de nos jours, les objets connectés sont partout. Cela se vérifie dans l'étude de l'institut Gartner qui prévoit environ 20 milliards d'objets connectés dans le monde en 2020, ce qui correspond à presque trois objets connectés par personne vivant sur notre planète.

Cette estimation du nombre d'objets connectés se traduit également dans le domaine de la santé. En effet, la majorité des pacemakers qui sont posés sur les personnes souffrant de difficultés cardiaques sont désormais reliés à Internet pour permettre au médecin de faire un suivi en temps réel. Malgré cet aspect bénéfique, cela présente aussi certains dangers, car les pacemakers étant reliés à Internet sont, de ce fait, attaquables par des personnes animées de mauvaises intentions. Le danger se précise si l'on se réfère à une étude américaine de 2012 signalant des failles de sécurité sur les pacemakers les plus posés aux États-Unis, et montrant la possibilité pour un individu de pirater des pacemakers et commettre ainsi un homicide en déréglant leur fonctionnement normal.

La question qui se pose alors est : quelles vont être les réactions des différentes administrations face à un homicide commis par Internet ? Si, pour l'Europe, la question a pu être traitée par le RGPD qui impose des principes de sécurité par défaut, elle ne sera pas pleinement résolue au niveau national, en particulier français : en effet, même si les forces de l'ordre bénéficient d'un grand nombre d'unités spécialisées, capables d'enquêter sur des infractions commises via Internet, une question reste en suspens : sur quel motif va-t-on pouvoir poursuivre l'auteur du délit ? Celui-ci a commis deux infractions qui, sur le papier, ne semblent avoir aucun lien, mais qui vont ici de pair : entrave au bon fonctionnement d'un système de traitement automatisé de données (pacemaker) — article 323-2 du Code pénal — et homicide volontaire — article 221-1 du Code pénal. S'agissant des règles de conflits de norme et des sanctions encourues, il semble évident de sanctionner l'individu pour homicide volontaire. Mais la peine encourue pour ce délit pénal pourra-t-elle être modifiée en raison du recours à Internet ?

La circonstance aggravante est ici évidente : homicide volontaire avec usage d'une arme. Cependant, eu égard à la nature des infractions, Internet ne peut guère être une arme au sens traditionnel : « *Tout objet utilisé pour tuer ou blesser* » — article 132-75 du Code pénal. Or en droit pénal à ce jour, un *objet* ne peut être que *matériel* ce qui n'est pas le cas d'Internet. Nous serions ainsi dans une situation où l'auteur d'un *cyber-homicide* ne pourrait être poursuivi que pour un homicide simple sans aggravation, sauf à considérer que c'est l'objet piraté qui a servi d'arme. L'autre difficulté, c'est qu'ici le meurtrier ne manipule pas directement l'arme qui a servi à tuer. Un nouveau concept pourrait alors apparaître par action du législateur, en créant une nouvelle catégorie, « l'arme numérique », pour mieux prendre en compte le cyber si celui-ci est utilisé pour commettre infractions ou délits. Pour la Justice, considérer désormais Internet comme une arme numérique permettrait ainsi de favoriser la prise en compte des évolutions technologiques dans la commission d'infractions, sans qu'il

soit nécessaire de lancer une réforme chaque fois qu'un nouveau *modus operandi* apparaîtrait chez les cyber-délinquants[30].

Le cyber, catalyseur du changement en santé

Il y a seulement deux ou trois générations, le secteur de la santé en France était relativement simple. On pouvait le résumer avec, d'une part la médecine de ville, principalement autour des médecins de famille et, d'autre part, les structures hospitalières réunissant les spécialistes et les plateaux techniques. La santé se caractérisait par une dimension exclusivement médicale. Les données de santé des patients étaient à la main exclusive de leurs propriétaires médecins, une patientèle enrichie de ses dossiers médicaux participant à la valorisation des cabinets lors des reventes.

L'arrivée d'Internet, concomitante ou moteur des changements de mentalité des individus, a toutefois catalysé cette transformation : qui n'a pas consulté un site de vulgarisation médicale pour disposer d'une information sur un symptôme, avoir un avis sur un médicament ou un traitement, ou encore s'informer sur les risques de consulter tel ou tel praticien ou service d'un établissement, à la veille d'une consultation ou d'une intervention médicale ? La santé est devenue un domaine dans lequel chacun est devenu acteur, avec un regard critique sur les avis rendus par les professionnels médecins dont la parole faisait autrefois autorité, et consommateur d'un « produit médecine » sur lequel, pour des besoins de mise en concurrence, chacun est redevenu propriétaire de ses données médicales afin de les mettre à sa guise à disposition de ses fournisseurs de santé.

Cette première transformation a imposé aux pouvoirs publics de changer leurs dispositions sur la protection de ce type de données. Deux options émergent alors dans le mode cyber :

- ***l'initiative privée :*** soit à titre individuel je stocke mes données médicales dans un Cloud que je partage avec ceux que je souhaite ; soit industrielle comme par exemple Google qui voit tout l'intérêt économique potentiel à concentrer de grosses bases de connaissances de santé ;
- ***l'initiative publique :*** le dossier médical partagé (DMP) dont il est intéressant de souligner qu'il s'appelait au départ dossier médical personnel ; ou encore les réseaux de spécialité comme la cancérologie ou reliant les établissements de santé d'un même territoire.

30 Article *Le Monde* sur les vulnérabilités des pacemakers :
https://www.lemonde.fr/pixels/article/2017/09/01/des-porteurs-de-pacemakers-piratables-incites-a-effectuer-une- mise-a-jour-logicielle_5179848_4408996.html
Dans la même idée sur une voiture : Article du Journal *Le Monde* en date du 22 juillet 2015 intitulé « Deux chercheurs parviennent à pirater une voiture à distance » version du 11 novembre 2017 :
Http://www.lemonde.fr/pixels/article/2015/07/22/deux- chercheurs-parviennent-a-pirater-une-voiture-a-distance_4694137_4408996.html
Article du journal *Le Parisien* en date du 10 novembre 2015 : « Plus de 20 milliards d'objets connectés à l'horizon 2020 » :
http://www.leparisien.fr/high-tech/plus-de-20-milliards-d-objets- connectes-a-l-horizon-2020-10-11-2015-5266535.php (version du 28 novembre 2017).
Une étude Gartner de 2017 montre qu'il y en a actuellement 8 milliards :
https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

Cette capacité d'appropriation de la médecine par le grand public a coïncidé en France avec une approche personnelle, non exclusivement médicale, de la santé. Elle reflète la définition santé par l'OMS comme un *« état de complet bien-être physique, mental et social »* qui ne consiste pas seulement en une absence de maladie ou d'infirmité : « je ne souhaite plus seulement guérir d'une maladie, mais je veux rester en bonne santé ». Cette nouvelle définition de la santé interfère avec celle, purement médicale, de notre politique publique nationale.

L'écosystème cyber agit alors comme catalyseur en introduisant des usages qui favorisent des mécanismes de *Soft law* par la forte valeur ajoutée qu'ils proposent. « Le code est la loi » : cette maxime formulée par Lawrence Lessig face au déploiement des systèmes de gestion de droits numériques prend ici tout son sens : autour des dispositifs médicaux utilisés dans un contexte médical professionnel, apparaît toute une gamme de dispositifs grand public, depuis les balances connectées pour suivre notre poids, mais aussi une multitude d'autres paramètres comme l'indice de masse corporel, jusqu'aux smartphones, permettant de quantifier et qualifier notre activité physique, et aux montres qui nous donnent aujourd'hui de l'électrocardiographie, ces dernières étant toutefois — attention ! — des « dispositifs médicaux ».

Le cyber soulève souvent la question de souveraineté, et le secteur de la santé n'y échappe pas. L'exemple du DMP traduit la volonté institutionnelle de concilier réalité opérationnelle et cadre réglementaire : en tant que propriétaire de votre DMP vous pourrez y déverser les documents que vous jugez utiles, et définir qui peut avoir accès à telle ou telle information. Mais, par sa dimension même d'outil public à votre service, le DMP embarquera des mécanismes de « bris de glace en cas de danger » permettant à des personnels médicaux, comme par exemple des urgentistes, d'accéder aux informations lorsque votre survie est en jeu. Exemple également intéressant par les perspectives qu'il offre d'un décloisonnement entre les établissements de santé « officiels » et les autres acteurs d'une prise en charge de la personne, tels que les premiers secours, les associations agrées de sécurité civile ou le service départemental d'incendie et de secours.

Si le cyber est « catalyseur », il est également le support qui pourra permettre de structurer et, surtout, de rebattre les cartes pour les nouveaux usages des données dites de santé, tout en résolvant l'incontournable schizophrénie entre respect de la vie privée et libéralisation des usages.

Chapitre VI

Stratégie de souveraineté cyber de la France

La ***Stratégie nationale pour la sécurité du numérique,*** i.e. la réponse collective pour un numérique de confiance, a été engagée par la France à partir de 2015[31]. Dès 2008 néanmoins, le Livre blanc sur la défense et la sécurité nationale mettait en exergue le risque d'une attaque informatique potentiellement néfaste à la survie de la nation, et invitait l'État à se doter d'une capacité de prévention et de réaction.

C'est en février 2011 que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) rend publique la stratégie de la France en lui fixant quatre objectifs :

- être une puissance mondiale de cyber-défense et appartenir au premier cercle des nations majeures dans ce domaine tout en conservant son autonomie ;
- garantir la liberté de décision de la France par la protection de l'information de souveraineté ;
- renforcer la cyber-sécurité des infrastructures vitales nationales ;
- assurer la sécurité dans le cyber-espace.

Revue en 2015, cette stratégie inclut désormais la nécessité d'informer le grand public, car plus que jamais le citoyen est le principal instrument de la stratégie de sécurité nationale et donc de lutte contre « l'arme de destruction massive des États » dans le domaine de la cyber-sécurité. L'environnement géostratégique exige, en effet, que chaque citoyen devienne un *acteur* œuvrant à la sécurité nationale : c'est plus que jamais son affaire car, en tant que cible, il est au cœur des menaces de nature cybernétique, et sa vulnérabilité devient par conséquent celle de l'État lui-même. De ce fait, l'autoprotection du citoyen devient partie intégrante de la stratégie de sécurité et de souveraineté nationale, dont il constitue le maillon le plus faible. Cet objectif stratégique constitue le socle *de la souveraineté numérique de l'État* érigé en seule entité légitime à *légiférer, contrôler et sanctionner* tous les acteurs publics ou privés. Le pendant de ce processus de monopolisation de la souveraineté numérique par l'État, est la pleine et entière *responsabilité de l'État dans le domaine de la cyber-sécurité.*

Pour ce faire, les pouvoirs publics ont dû élaborer toute une législation propre à réglementer les systèmes d'information, qu'il s'agisse de ceux de l'Administration ou de ses propres citoyens. Démarche de souveraineté qui a été déterminante pour légiférer d'abord et avant tout sur les

31 16 octobre 2015 par le Premier ministre Manuel Valls

infrastructures vitales nationales de l'État lui-même. Cet impératif a ensuite présidé dès 2013 à une extension de la stratégie nationale, afin de normer les opérateurs vitaux (OIV) dépassant ainsi le cadre limité des infrastructures propres à l'État. Enfin, sous l'effet de la législation européenne, ont été inclus dans ce socle indispensable à la préservation de la souveraineté étatique, les opérateurs de service essentiels (OSE), incontournables pour le fonctionnement de l'économie et de la société, ainsi que les fournisseurs de service numérique (FSN).

Ainsi, en l'espèce d'une décennie, l'État aura réussi à constituer la seule entité détenant le monopole de la souveraineté numérique, en déployant sa fonction exécutive, législative (capacité édictale ou normative) et judiciaire (droit pénal). La production de normes dans le domaine de la cyber-sécurité est devenue la seule prérogative de L'État, celui-ci ayant réussi à capter toute une sphère d'activités et de standards autour de la sécurité des SI au détriment des entités privées, et obtenu son indépendance vis-à-vis de celles-ci dans l'offre de sécurité afin de préserver ses propres systèmes d'information stratégiques ainsi que ceux de ses citoyens dans :

- le fonctionnement des moyens de communication des plus hautes autorités de l'État, des ministères et de ses organisations. L'ANSSI a développé une large gamme de systèmes interministériels sécurisés d'information et de communication : l'intranet sécurisé interministériel pour la synergie gouvernementale (ISIS), le réseau interministériel de téléphonie fixe RIMBAUD, le système d'exploitation multiniveaux dénommé CLIP OS avec un haut niveau de résistance aux codes malveillants, les certifications émises par IGC/A (pour authentifier officiellement les autorités de certification des administrations de l'État français), la cryptophonie nouvelle génération TEOREM et le système de vidéoconférence sécurisé au niveau Confidentiel Défense HORUS ;
- la cyber-sécurité des opérateurs d'importance vitale (OIV) publics et privés (plus de 200 dont la liste est confidentielle) qui exploitent ou utilisent des installations jugées indispensables pour la survie de la Nation[32] (activités difficilement substituables ou remplaçables) et qui s'intègrent dans un dispositif interministériel de douze secteurs d'activités d'importance vitale (SAIV)[33] rattachés depuis 2006 à un ministre coordonnateur[34] ;
- à partir de 2013 la législation (LPM) impose à ce dispositif OIV complété par celui des SAIV le renforcement de la sécurité de leurs systèmes d'information d'importance vitale (SIIV), avec un certain nombre de règles indispensables à la protection des infrastructures jugées critiques[35] ;
- en complément de ce dispositif national, la réglementation européenne à laquelle la France a œuvré [*Directive Network Information System Security (NIS) 27 février 2018 - décret*

32 L'article R. 1332-1 du CODEF définit un opérateur d'importance vitale comme gérant ou utilisant *« Un ou des ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population »*.

33 Définis dans un arrêté du 2 juin 2006 (JORF n°129 du 4 juin 2006 page 8502 texte n° 1) et modifié par celui du 3 juillet 2008 (JORF n°0156 du 5 juillet 2008 page 10823 texte n° 6). Les SAIV sont définis à l'article R. 1332-2 du CODEF

34 http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf

35 La sécurisation des systèmes d'information d'importance vitale a été mise en œuvre par deux décrets du 27 mars 2015 : n° 2015-351 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et le décret n° 2015-350 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale.

d'application 25 mai 2018] assure la protection de nouveaux acteurs comme les opérateurs de services essentiels (OSE) pour le fonctionnement de l'économie et de la société des pays européens. Leur prestation étant tributaire d'autres systèmes d'information, ils devront garantir un socle minimal de cyber-sécurité dans des domaines précis[36] pour se prémunir contre une attaque[37]. En cas de non-respect de la réglementation en vigueur par ces OSE, des sanctions pécuniaires sont prévues ;

— la législation européenne fixe également le cadre général des fournisseurs de service numérique (FSN) qui devront analyser les risques courus par leurs systèmes d'information et prendre des mesures techniques et organisationnelles dans les domaines suivants : sécurité des systèmes et installations ; gestion des incidents ; gestion de la continuité des activités ; suivi, audit et contrôle ; respect des normes internationales. Il leur reviendra également le soin de déclarer à l'ANSSI tout incident de sécurité pouvant impacter la *continuité* du service dont ils ont la charge. Ils seront enfin directement soumis à des contrôles de sécurité effectués par l'ANSSI ou par des prestataires de service qualifiés à la demande du Premier ministre ;

— en matière de cryptographie enfin, une réglementation nationale spécifique couvre la commercialisation de produits intégrant des fonctions ou moyens de cryptage, ainsi que les démarches à accomplir pour vendre, importer ou exporter ce type de produits.

Les grands plans

1967 : Plan Calcul

Plan gouvernemental lancé en 1966 sous la présidence du général de Gaulle. Pour développer une capacité d'innovation technologique française et européenne en matière de gros ordinateurs et de réseaux numériques.

1985 : Plan informatique pour tous

Pour initier les élèves du pays à l'outil informatique et soutenir l'industrie nationale des micro-ordinateurs.

1998 : Plan d'action gouvernemental pour la société de l'information

Pour repenser l'apport des technologies à l'ensemble des ministères de concert. Il ne s'agit

36 Ces domaines sont les suivants :

le domaine de la gouvernance de la sécurité des réseaux et systèmes d'information concernant l'élaboration et la mise en œuvre d'une politique de sécurité des réseaux et systèmes d'information ainsi que l'homologation de sécurité des réseaux et systèmes d'information

le domaine de la protection des réseaux et systèmes d'information, sur la sécurité de l'architecture et de l'administration des réseaux et systèmes d'information et le contrôle des accès à ces réseaux et systèmes

le domaine de la défense des réseaux et systèmes d'information, sur la détection et le traitement des incidents de sécurité affectant les réseaux et systèmes d'information

le domaine de la résilience des activités, sur la gestion de crises en cas d'incidents de sécurité ayant un impact majeur sur des services essentiels.

37 Se reporter à l'annexe du décret qui fixe la liste des services essentiels tels que l'énergie, les transports, logistique, banques, infrastructures de marchés financiers, services financiers, assurance, social, emploi et formation professionnelle, santé, fourniture et distribution d'eau potable, le traitement des eaux non potables, infrastructures numériques, éducation, restauration : 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, JORF n°0118 du 25 mai 2018, texte n° 1. C'est sur la base de cette liste que le Premier ministre désigne les opérateurs de services essentiels sur recommandation des ministères concernés et de l'ANSSI. Une liste actualisable tous les deux ans.

pas d'intégrer Internet dans un seul secteur ou d'adapter uniquement un corps de métier, mais de fournir un projet global couvrant toute la société. L'enjeu est que la France prenne la mesure des importantes évolutions sociales, politiques, législatives et économiques, qui se jouent, et qu'elle n'aggrave pas son retard dans l'appropriation des TIC.

2004 : Projet ADELE (Administration électronique 2004-2007)

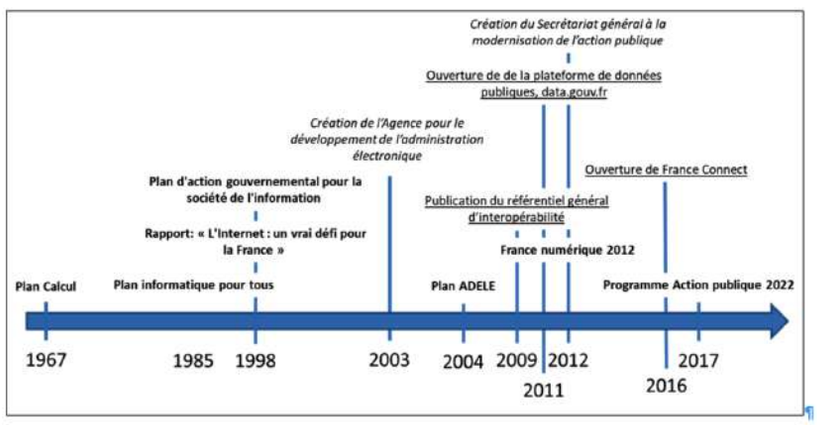
Plan de 140 mesures destinées à rapprocher des services publics leurs usagers en simplifiant les démarches grâce au développement d'une administration électronique qui s'inscrit dans la ligne des projets de réforme de l'État menés par le ministère de la fonction publique. Il permettra aussi de faire exécuter gratuitement par l'usager le travail de saisie qui était effectué jusque-là par des fonctionnaires.

2008 : Plan France numérique 2012

Plan comportant quatre priorités : permettre à tous les Français d'accéder aux réseaux et aux services numériques ; développer la production et l'offre de contenus numériques ; diversifier les usages et les services numériques ; rénover la gouvernance et l'écosystème de l'économie numérique.

2017 : Plan 2022

Plan ayant pour objectif de construire ensemble des parcours d'inclusion numérique adaptés à tous, et de repenser le modèle de l'action publique en interrogeant en profondeur les métiers et les modalités de l'action publique, au regard de la révolution numérique qui redéfinit en permanence les contours de notre société.



Les incidents cyber et leur traitement

Exemple de signalement cyber

Exemple de déclaration d'un incident de sécurité relatif à un produit ou un service qualifié. Ce formulaire sera traité ensuite par le centre opérationnel de la sécurité des systèmes d'information de l'ANSSI.

Informations générales : commune de XXX

Fournisseur de produit : logiciel de gestion de l'état civil et des administrés

Cadre réglementaire de la qualification du fournisseur de produits ou de service : qualification obtenue pour les besoins de sécurité des autorités administratives hors sécurité nationale.

Système d'information affecté : usurpation d'un droit administrateur par un élu, à distance, par un accès VPN dans l'infrastructure. Vol caractérisé de toutes les données des administrés et tentative de dissimulation par effacement des logs applicatifs. Le logiciel de gestion de l'état civil est en lien avec la liste électorale.

Description de l'incident : un suivi des logs des utilisateurs par le responsable informatique a mis en exergue une connexion distante d'un compte d'un agent ayant quitté la collectivité qui n'avait pas été supprimé. Après enquête, nous avons découvert qu'il s'agissait d'une connexion intrusive cyber. L'opérateur Orange a déterminé l'adresse source et nous avons découvert qu'il s'agissait d'une adresse d'un élu de la communauté de commune. N'ayant pas de DPO nous nous sommes appuyés sur les conseils d'Orange et avons imprimés les logs. Le compte incriminé a été inactivé. Le fichier de log a été rétabli.

Qualification de l'incident : incident volontaire et non accidentel, acte de malveillance externe.

Impacts de l'incident : tout le fichier des administrés a été volé portant préjudice à la confidentialité des informations détenues par un organisme public. Le service à la population a été violé dans son intégrité morale et fonctionnelle.

Mesures prises :
- renforcement immédiat des mesures de gestion des comptes, de la gestion des accès aux logiciels, de l'organisation des accès aux serveurs et de la politique générale de sécurité.
- mise en œuvre d'une interdiction d'accès à l'état civil par un accès distant. Fermeture des ports d'accès à la maintenance du système par la mise en œuvre d'une obligation de connexion en présentiel. Rappel des bonnes pratiques à l'ensemble des utilisateurs.

Observations complémentaires. Après investigations globales par un cabinet consultant nous avons constaté :
- des tentatives de dénis de services ;
- des tentatives d'usurpation de droits ;
- une porte dérobée intégrée par un fournisseur, qui à ses dires est juste pour de la souplesse ;
- un rootkit implanté par l'élu pour effacer ses traces.

Nous avons tout catalogué et nous menons des mesures de protection renforcée depuis ce jour. Notre consultant mandate sur ordre de Monsieur le maire un organisme certifié PASSI pour tester toutes les compromissions possibles et mettre en place des améliorations de la gouvernance du SI.

Exemples d'incidents « Crypto locker »

EN EPHAD

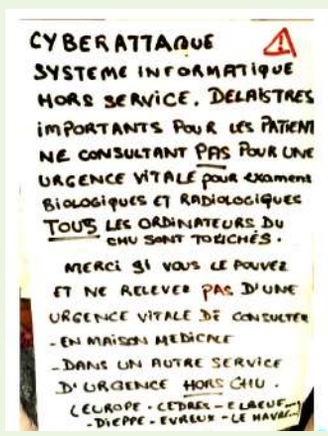
Cet EHPAD, petit établissement d'hébergement de province pour personnes âgées dépendantes, héberge 80 résidents. Pour son système d'information il utilise un serveur virtualisé et un système à double sauvegarde.

Début juillet, les fichiers deviennent progressivement grisés et changent d'extension. En une heure seulement tous les fichiers sont infectés. Ne disposant pas d'équipe en interne, comme la majorité de ce type d'établissement, l'appel est fait au prestataire. La démarche prévue est d'effacer les fichiers et de les remplacer par leur sauvegarde. Mais comme souvent, un malheur n'arrive jamais seul. Plusieurs défauts rendent la manipulation impossible. NAS éteint (sans doute microcoupure due à un essai de groupe électrogène) et sauvegarde sur cassettes défectueuses. Au final entre deux et quatre mois de données ont été perdues pour un coût d'environ 35 000 €.

EN CHU

Début de week-end, les services informatiques sont en effectif minimum ; meilleur moment pour le groupe cyber-criminel TA 505 de lancer une vaste campagne. Il y aura toujours des utilisateurs pour cliquer sur le mauvais lien et installer le logiciel malveillant. Il ne reste plus aux cyber-criminels qu'à activer leur programme. Le soir du 15 novembre c'est fait. Le logiciel malveillant commence à chiffrer les données d'un réseau afin de réclamer une rançon en échange de la clé de déchiffrement.

Pour arrêter la propagation du virus, les systèmes sont arrêtés. Retour au papier et au crayon pour les équipes. Le redémarrage des applications du système d'information va prendre plusieurs jours, perturbant le fonctionnement des services et mobilisant plus de vingt personnes pour permettre de relancer les applications critiques.



Ces exemples ne sont pas isolés. Depuis la mise en place du dispositif de signalement en octobre 2017, l'ASIP Santé a recensé 693 incidents de sécurité déclarés par des structures de santé. La cyber-malveillance représente 43 % des signalements : hameçonnage, rançongiciel, intrusion, etc.

84 % des signalements transmis à l'ASIP Santé proviennent d'établissements de santé, le reste étant principalement émis par des EHPAD, des laboratoires d'analyses médicales ou, encore, des centres de radiothérapie. Sur l'ensemble des incidents déclarés, seuls 13 % ont fait l'objet d'une demande d'accompagnement auprès de la cellule d'accompagnement cyber-sécurité des structures de santé (ACSS) du ministère de la santé[38].

41 % des incidents signalés ont impacté des informations patient à caractère personnel, se caractérisant principalement par l'indisponibilité des données. En outre, pour un incident sur deux, l'établissement a été contraint de passer à un fonctionnement dégradé de son système de prise en charge des patients.

38 https://www.cyberveille-sante.gouv.fr

Chapitre VII

Cyber-stratégie et intelligence artificielle

Le mot stratégie dérive du grec (*stratos* signifiant « armée », et ageîn signifiant « conduire »). Il s'agit bien, face aux cibles et enjeux visés par les cyber-attaques, face aux menaces à venir, de définir des frontières dans le cyber-espace[39] et d'assurer leur inviolabilité. Seule l'intelligence artificielle (IA) possède aujourd'hui la puissance de calcul indispensable pour détecter les infimes anomalies que peut engendrer une attaque « en approche ». Et c'est ce qui va lui permettre de prendre de vitesse les contrevenants.

Source https://www.lebigdata.fr/dossier-big-data-cybersecurite

Task Force IA[40] : défense et dissuasion requises dans le cyber-espace

La France a pris un retard conséquent dans la maîtrise de l'IA. Il convient donc de fédérer, voire, en étant optimiste, de mutualiser les différentes stratégies nationales de défense militaire et civile contre les cyber-attaques. L'objectif est d'identifier grâce à l'IA une attaque, à partir de données brutes ou d'un comportement caractéristique.

En 2018, l'IA avait la capacité d'analyser 93 millions de milliards de données par seconde (contre 90 000 en 1999). En 2020, celle-ci sera d'un milliard de milliards d'opérations par seconde et, en 2045, on prévoit des milliards de milliards de milliards d'opérations par seconde. Plusieurs

39 Le cyber-espace est l'ensemble des ordinateurs connectés dans le monde. Chacun d'entre eux agit comme une tête chercheuse et cible des citoyens qui eux aussi cherchent à atteindre leurs objectifs.

40 *Task force :* Force opérationnelle pour exécuter des missions temporaires de protection et de surveillance. Correspondante en France : Jeanne Heure - jeanne.heure@capgemini.com

vies ne suffiraient pas pour analyser la masse de données brassées par un ordinateur. C'est l'agrégation de ces milliards de calculs qui donne à l'IA sa puissance et sa capacité d'interaction.

L'IA est en pleine expansion et ses principaux objectifs pratiques sont posés : robots autonomes, compréhension et traduction de l'écrit et de la parole, vision artificielle, résolution de problèmes mathématiques, aide à la décision. L'IA est capable de tweeter, de monter 25 000 vidéos par mois (1 minute pour monter une vidéo), de de légender avec un minimum d'erreurs des photos, d'écrire des articles. En 2017 une entreprise américaine a même implanté sur 50 employés une puce sous-cutanée pour l'ouverture des portes, l'identification sur l'ordinateur, la cantine. Un robot humanoïde ERICA, créé par un japonais, présente maintenant le journal télévisé. Google a récemment réalisé une application vocale permettant de prendre des rendez-vous, et l'échange pour les finaliser est bluffant. Microsoft a créé créé une intelligence artificielle capable de lire et comprendre un texte aussi bien qu'un être humain. La prochaine étape sera quand l'IA apprendra à lire à une nouvelle intelligence artificielle qui deviendra elle-même experte dans ce nouveau domaine.

Détection de cyber-attaques : Cas d'utilisation

Une attaque informatique n'est pas nécessairement une action fulgurante, mais plus généralement une opération phasée où peuvent s'écouler de plusieurs semaines à plusieurs mois entre l'intrusion initiale et l'effet final (vol de données, sabotage, etc.). La lutte contre les attaques informatiques repose donc sur une stratégie combinant des architectures robustes aux attaques (ce qui rend les actions de l'attaquant plus complexes, et donc les ralentit), à la capacité à détecter celles qui ont réussi avant que l'effet ne s'en fasse ressentir. Pour cela, les données issues de l'activité des systèmes d'informations sont collectées par de nombreux capteurs disposés sur les réseaux, dans les terminaux et dans les serveurs, que l'activité soit habituelle (connexion d'utilisateurs, transmission de message) ou à risque (détection antivirale, identification de trafic réseau malveillant) .

Applications au domaine de la défense

Le rapport de la Task Force IA met en exergue *« l'impact opérationnel déterminant de l'IA dans la cyber-défense »* :

- analyse de traces dans un réseau à des fins de détection d'intrusion ou d'activité malveillante ;
- anticipation des menaces, en se basant sur les sources d'information disponibles (source ouverte) ;
- mesure du niveau de résistance des systèmes ;
- lutte dans le domaine de l'influence numérique ;
- détection des tentatives de cyber-attaque ;
- analyse des vulnérabilités ;
- analyse et anticipation des menaces ;
- assistance aux opérations cyber défensives et offensives.[41]

41 Rapport Task Force IA page 18 sept 2019.

Dans ce but, la détection et l'anticipation des attaques s'appuient sur la structure Artemis[42] qui permet l'acquisition et le traitement de la donnée par l'IA, qui permet de gagner du temps en s'adaptant aux menaces de demain et en évitant tout décrochage.

Le Comcyber[43] (Commandement de la cyber-défense), placé sous l'autorité du chef d'état-major des armées rassemble depuis le 1er janvier 2017 l'ensemble des forces de cyber-défense des armées françaises sous une même autorité opérationnelle, permanente et interarmées. Il est responsable de la protection des S.I. (systèmes d'information) placés sous la responsabilité du chef d'état-major des armées, de la conduite de la défense des S.I. du ministère (à l'exclusion de ceux de la DGSE et de la DRSD) ainsi que de la conception, de la planification et de la conduite des opérations militaires de cyber-défense. Il est également responsable de la préparation de la politique RH du domaine cyber et s'articule autour de trois organismes :

- le centre d'analyse en lutte informatique défensive (CALID) est un centre opérationnel expert. Il pilote 24 heures sur 24 la détection, le traitement et la réponse aux cyber-attaques. Créé en 2006, il est basé à Paris et à Rennes. Il est devenu un organisme interarmées rattaché au Comcyber depuis janvier 2019.
- Le centre de la réserve et de la préparation opérationnelle de cyber-défense (CRPOC) est chargé du recrutement et de la gestion des réservistes de cyber-défense, de l'entraînement et de la préparation opérationnelle des états-majors, directions et services (EMDS), avec le montage d'exercices nationaux et internationaux de cyber-défense. Créé en 2015, il est localisé en région Bretagne et à Paris.
- Le centre d'audits de la sécurité des systèmes d'information (CASSI) a une mission d'audit qui couvre deux domaines : la sécurité des systèmes d'information (SSI) et les signaux parasites compromettants (SPC). Crée en 2008, il est basé à Maisons-Laffitte, Brest, Orléans et Toulon.

Notons que la France ne fait pas partie des *Five Eyes*, accord de coopération anglo-saxon qui réunit autour de la NSA américaine les services de renseignement électroniques des Britanniques, Canadiens, Australiens et Néo-Zélandais. Bernard Barbier, qui a vécu à la DGSE la militarisation du cyber-espace, serait plutôt favorable à ce que nous soyons le sixième œil, notamment parce qu'il y a un *« no spy agreement »* entre ses signataires qui en principe ne s'espionnent pas entre eux. Mais au niveau politique, la France n'accepte pas cet engagement. On est donc le sixième œil sans l'être tout à fait, allié assez particulier par rapport aux Américains, les Allemands restant en retrait dans ce domaine. Il va sans dire toutefois qu'une interaction est nécessaire, ainsi qu'une mutualisation entre services dédiés au renseignement, à la surveillance et à la sécurité du cyber-espace. Et la capacité technique de la France reste quand même à ce jour la première de l'Europe continentale pour contrer ces vulnérabilités…

42 Artemis (Architecture de traitement et d'exploitation massive de l'information multi-source). L'objectif au lancement du programme a été annoncé comme étant : *« de fournir dès 2019 un démonstrateur de plate-forme sécurisée et distribuée d'intelligence artificielle pour les besoins spécifiques des armées. »*

43 Habituellement connu sous la graphie COMCYBER, qui est contraire ux règles actuelles d'écriture des sigles et logos : en majuscules ceux qui s'épèlent en minuscules ceux qui se rononcent comme un mot.

Application aux entreprises

« *Face à la multiplication des cyber-menaces, les entreprises se tournent vers des solutions à base d'intelligence artificielle (IA) pour renforcer la protection de leurs actifs numériques.* » (Rapport international du Capgemini Research Institute : Reinventing Cybersecurity with Artificial Intelligence 07/2019 - 850 décideurs informatiques interrogés sur 10 pays : France, Allemagne, Espagne, Italie, Pays-Bas, Suède, Royaume-Uni, Inde, États-Unis, Australie). Près de sept décideurs informatiques sur dix pensent que sans IA leur organisation ne serait pas en mesure de répondre aux cyber-attaques à venir.

Les opérateurs d'une cyber-sécurité dans le privé

Le DSI, directeur des systèmes informatique et/ou d'information (en anglais : CIO) est l'exécutif en charge de la stratégie IT et des systèmes informatiques nécessaires aux objectifs de l'entreprise. Dans les années 80 son rôle était essentiellement technique, mais à mesure que le stockage, la transmission et l'analyse d'informations par électronique gagnaient en importance, le DSI est devenu un contributeur clé dans la formulation des objectifs stratégiques. Dans nombre d'entreprises, il reporte directement au directeur général et il siège souvent au Comité de direction. Il doit sensibiliser les cadres ainsi que tous les autres employés à la valeur de l'information et aux risques que les systèmes informatiques peuvent induire pour l'entreprise.

L'avènement des ordinateurs personnels au sein de l'entreprise au début des années quarre-vingts marque la fin de la concentration des systèmes informatiques dans des services de traitement de données aux mains de spécialistes. Les systèmes deviennent alors distribués à l'échelle de l'entreprise, chaque unité métier commençant à acquérir ses propres systèmes auprès de tout un panel de fournisseurs spécialisés. Les employés quant à eux s'habituent à avoir à portée de main une technologie bureautique puissante. Mais il devient pourtant rapidement évident que ces « poches » informatiques autonomes (*Shadow IT*) sont globalement inefficaces et coûteuses. Beaucoup d'entreprises adoptent alors un modèle mixte fédéré, dans lequel certains systèmes et services informatiques sont sous contrôle centralisé, d'autres restant sous contrôle local, mais avec des normes. Déterminer comment et avec quels fournisseurs acquérir, architecturer et mettre en réseau de bout en bout les solutions constitue dès lors une part importante du rôle du DSI.

C'est l'époque où émergent les suites ERP[44] qui visent à collecter et gérer les données produites aux différents niveaux de l'entreprise. La mise en œuvre de ces systèmes gigantesques et complexes est coûteuse et difficile, elle nécessite en général la refonte complète des processus métier, débouchant parfois sur des échecs spectaculaires. Pour autant 100 % des 1 000 premiers groupes européens utilisent un ERP.

44 Un ERP (Enterprise Resource Planning) ou également appelé PGI (progiciel de gestion Intégré) est un système d'information qui permet de gérer et suivre au quotidien, l'ensemble des informations et des services opérationnels d'une entreprise. Les quatre principaux éditeurs mondiaux d'ERP sont allemand SAP Hana et américains Oracle, Infor, Microsoft Dynamics 365, et Sage (en parts de marché mondial). Les Français résistent très bien sur leurs terres : SAP, Sage, Cegid.(Étude *Ariane Beky, 19 juillet 2019*)

Au début des années 90, l'accès au World Wide Web étend encore le rôle de l'informatique au sein de l'entreprise. Le DSI, principale autorité technologique de l'entreprise, devient une force de proposition et de normalisation. À mesure que les processus métier se numérisent et que les clients génèrent des données numériques, la portée et le portefeuille du DSI évoluent en conséquence. Certaines de ses responsabilités sont transférées à d'autres rôles exécutifs. Parallèlement au directeur technique (CTO) et au responsable de la sécurité des services informatiques (RSSI), on voit poindre tout un panel de nouveaux « managers » comme le responsable des données (CDO ou Chief Data Officer). Leurs compétences incluent la nécessaire maîtrise du Cloud computing, de l'informatique mobile, du Big data et des plates-formes de collaboration.

Dans nombre d'entreprises, le budget informatique accordé au DSI est calculé en pourcentage du chiffre d'affaires. Ce taux varie selon le secteur économique et sa dépendance à la technologie, et oscille entre 1 % (construction, matériaux, ressources naturelles) et 6,7 % (édition de logiciels, services Internet), selon le rapport Gartner *IT Key Metrics Data 2014*. À l'instar du budget informatique, la rémunération d'un DSI varie aussi considérablement. Elle est fonction des années d'expérience, du chiffre d'affaires et de la taille de l'entreprise. En France, elle varie de 70 K€ par an à plus de 150 K€.

IA et cyber-sécurité : une alliance stratégique pour les DSI

Selon le rapport du Capgemini Research Institute déjà cité, sept décideurs informatiques sur dix pensent que, sans IA, leur organisation ne sera pas en mesure de répondre aux cyber-attaques à venir car la surface des attaques s'étend et le volume de données échangées augmente. Les analystes en cyber-sécurité sont submergés par les alertes (56 % des répondants). 42 % font état d'une hausse des attaques ciblant leurs applications sensibles et 43 % observent une accélération de la vitesse d'exécution des attaques cyber. Face à la multiplication de ces cyber-menaces, les entreprises se tournent donc vers les solutions à base d'intelligence artificielle pour renforcer la protection de leurs actifs numériques. Le passage de la preuve de concept à un déploiement à grande échelle n'est pas simple. Mais une organisation sur cinq utilisait déjà l'IA avant 2019 pour renforcer sa cyber-sécurité, et près de deux sur trois prévoient un déploiement d'ampleur en 2020. Pour renforcer la précision de la détection, les organisations prévoient de se doter de systèmes de détection/protection en temps réel dopés à l'apprentissage machine (ML) afin d'endiguer le flot de cyber-menaces et de distinguer les connexions légitimes des tentatives hostiles. 48 % des répondants prévoyaient une augmentation de 29 % en moyenne des budgets consacrés à l'IA cyber-sécurité en 2020.

L'ISACA a été fondée aux États-Unis en 1967 par un groupe d'experts travaillant comme auditeurs sur le contrôle des systèmes informatiques, qui devenait de plus en plus critique pour les opérations de leurs entreprises. Ils avaient reconnu la nécessité d'une source centralisée d'information et d'orientation dans ce domaine. 86 % des membres de l'ISACA ont observé une baisse mondiale du nombre de professionnels de cyber-sécurité disponibles et la pénurie de compétences dans ce secteur est une préoccupation croissante pour les DSI, dont beaucoup

s'inquiètent de leur manque de formation sur les initiatives qu'on s'attend à les voir conduire. Au regard des cyber-menaces, il y a insuffisance des ressources humaines pour analyser et « vectoriser » en temps réel : en 2020 le manque de techniciens informaticiens en France est de 80 000, et on l'estime à 2 millions d'ingénieurs dans le monde. D'où l'intérêt de prioriser l'Intelligence artificielle, incontournable dans l'étude du cyber-espace, mais qui a encore besoin d'être mise sous le projecteur des décideurs stratégiques : *« Celui qui détiendra l'intelligence artificielle sera le leader du monde »* (Vladimir Poutine - septembre 2017).

L'intelligence artificielle en France

L'IA est le maillon faible de la chaîne. Elle est restée un écosystème isolé, ignoré par les pouvoirs publics jusqu'en 2017. Riche de l'excellence de ses chercheurs, de ses jeunes pousses et des ingénieurs français qui ont conduit leur quête avec brio, mais pauvre faute de moyens. Toutefois l'IA équipe déjà de nombreux systèmes. Elle est un levier de puissance, et son appropriation par les décideurs et les utilisateurs est devenue une urgence. Il y a heureusement eu fin 2017 un « *remue-méninges* » autour de l'intelligence artificielle, et il ne s'agit plus de faire prendre conscience de l'enjeu puisque c'est désormais acquis, mais de hisser l'IA au rang de capacité stratégique et de force de dissuasion. (Rapport Villani).

Petit historique national

France IA : Groupe de travail lancé en janvier 2017 avec différents chercheurs et acteurs de l'IA, qui a dévoilé dans son rapport final l'état des recherches en France et ses propositions *« Pour faire de la France un acteur de premier plan en matière d'IA »* : *« La France doit se poser la question de sa souveraineté à l'aune de l'émergence de l'intelligence artificielle »*. Ce rapport contenait une cinquantaine de propositions couvrant le financement de la recherche, la formation pour conserver les talents sur le territoire français et le moyen de faciliter l'interaction entre les laboratoires de recherche et les entreprises du numérique. La France était très en retard *« ne figurant pas dans le top 5 mondial du secteur, dominée par les États-Unis, la Chine, la Russie, Israël, le Canada et le Royaume-Uni »*. Peu avant de quitter ses fonctions de ministre de la défense, Jean-Yves Le Drian faisait de l'IA *« un élément de notre souveraineté nationale »*. La France faisait enfin le pari de l'IA.

Panorama actuel

THALES[45] a inauguré en octobre 2017 à Paris une *Digital Factory*[46] qui doit accueillir 70 personnes et regrouper les experts de l'entreprise sur les quatre technologies stratégiques du groupe : la connectivité, le Big Data, l'intelligence artificielle et la cyber-sécurité.

45 Un géant très diversifié, né en 2000, de la fusion de Thomson CSF et Dassault Electronique,

46 Digital Factory : Dominique CHAPUIS : En investissant 150 millions d'euros sur trois ans…

DASSAULT Systèmes veut devenir « l'Amazon des ingénieurs » et a lancé son programme MMT (Man Machine Teaming) pour développer l'autonomie de la machine et son interaction avec l'homme.[47]

DGA : recherches françaises concernant « la détection de cibles furtives, la reconnaissance d'objets, l'assistance à la décision, l'interface homme-machine adaptative, l'autonomie des robot et l'incontournable cyber-sécurité. »[48]

MONDOBRAIN est une plate-forme d'intelligence augmentée qui propose une « solution d'aide à la décision utilisant l'intelligence artificielle, conçue pour être utilisée par des opérationnels », le but étant, selon le DGA Lab, de « pouvoir les aider à déterminer les variables clés d'un problème ».

SENTIENT Technologies, dont le PDG co-fondateur est le Français Antoine Blondeau, est l'une des entreprises les plus avancées en matière d'intelligence artificielle.

ENSIBS est une école d'ingénieurs dédiée à la cyber-défense : à Vannes, au cœur de cette Bretagne devenue « pôle d'excellence » cyber, elle forme depuis 2013 une petite armée de cyber-défenseurs, avec, comme point d'orgue de la formation, la simulation de cyber-attaques d'une infrastructure vitale.

Livres blancs de l'INRIA qui examinent les grands défis actuels du numérique et présentent les actions menées par des équipes-projet pour résoudre ces défis. Coordonnés par Bertrand Braunschweig avec des contributions de 45 chercheurs de l'Inria et de ses partenaires.

École normale supérieure : Le nouveau parcours intelligence artificielle (IA) est proposé depuis septembre 2019 aux normaliens ayant suivi une formation pré-master en mathématiques ou en informatique et désireux de devenir des experts-concepteurs.

Google a choisi Paris pour son deuxième centre européen d'IA : *« Nos équipes travailleront sur des usages à venir, pour explorer à quoi ressembleront demain les utilisations de l'IA »* indique Sébastien Missoffe, directeur général de Google France qui mise sur l'IA. La France est l'un des pays qui dispose du plus gros écosystème de recherche en « intelligence artificielle », selon Olivier Bousquet, chercheur français en intelligence artificielle chez Google et chargé de mettre en place cette initiative. *« Nous voulons attirer les talents de l'étranger pour qu'ils viennent à Paris et s'insèrent dans le système académique »*. Google a aussi annoncé le lancement d'une initiative dédiée à la formation au numérique en France. Quatre espaces physiques seront ouverts, dont le premier à Rennes.

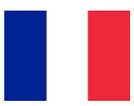
47 Lancement du projet mars 2018

48 Communication de la DGA : « La direction générale de l'armement se penche sur l'intelligence artificielle » par Laurent LAGNEAU · 1er décembre 2017

VAD BeMSP, spécialisé dans les solutions à destination des MSP (*Managed Service Providers* : sociétés de services informatiques gérant à distance les systèmes informatiques de ses clients, de manière proactive et sous un modèle forfaitaire) annonce un contrat de distribution avec l'éditeur américain de solutions de protection contre le *dark web,* ID Agent. Son outil de surveillance du dark web repère et analyse les données utilisateurs compromises (notamment leurs identifiants et mots de passe) et permet aux MSP de proposer des services de remédiation aux entreprises concernées. Outre cette plate-forme de protection, ID Agent propose une solution de renseignements sur les menaces et une formation à la sécurité.

Chapitre VIII

Où en est la France dans le monde



Les enjeux cyber de la France

Le véritable enjeu pour la France est de faire de la cyber-sécurité un sujet politique avec comme objectif la définition et la mise en œuvre d'une véritable stratégie globale cyber. Celle-ci aura pour vocation de donner une vision, d'établir un plan d'action et un pilotage transverse unifié *politique-défense-entreprise*, l'objectif ultime étant de redevenir à court terme une cyber-puissance de rang international.

La France dispose d'un énorme potentiel de compétences, mais qui avancent pour le moment en ordre dispersé. Une forte coordination public-privé, la structuration des entreprises et des talents présents sur le territoire afin de faire émerger quelques champions locaux, sont les facteurs clés de succès.

Il faut donc en finir avec une gouvernance cyber uniquement technique ou militaire pour aller vers une réelle approche réunissant classe politique et monde des entreprises sphère où se trouvent les opportunités cyber et où en sont supportés les coûts. Or à ce jour et pour l'instant, les entreprises françaises subissent plus qu'elles ne profitent de ce nouveau facteur de compétitivité mondiale qu'est la cyber-sécurité.

Le nombre d'attaques informatiques a nettement augmenté au cours des dernières années. On en recense annuellement plus de deux millions au plan mondial. Leur fréquence et leur intensité soulèvent des interrogations, tout comme les moyens utilisés de plus en plus complexes, combinant l'ingénierie sociale, les programmes malveillants et les techniques d'intrusion sur les systèmes d'information pour polluer des logiciels en utilisant leurs failles de sécurité.

Les conséquences de ce type de risque sont catastrophiques : perte d'affaires, atteinte à la réputation, perte de confiance. La perte de données sensibles prend la première place au niveau mondial des inquiétudes potentielles. Le virus *WannaCry* a paralysé plus de 300 000 ordinateurs de sociétés multinationales et de services publics dans 150 pays. La cyber-sécurité

est donc devenue un élément stratégique à prendre en compte dans le management des organisations.

Les DSI[49] relèvent comme mode d'attaque le plus fréquent le *phishing*, le *Shadow IT* étant le cyber-risque le plus répandu. En tête des enjeux, le recours massif au *Cloud* pose des problèmes de perte de maîtrise imputables à l'accès aux données, à la chaîne de sous-traitance, à l'utilisation d'outils spécifiques en plus de ceux proposés par le prestataire, à la non restitution des données, et à la localisation des données

Au plan technique, face à la menace, une panoplie de solutions existent**.** Celles-ci semblent en phase avec les attentes des entreprises, mais restent sous-utilisées en raison de la transformation numérique rapide des organisations impliquant en permanence une revue des exigences et des mesures.

Les acteurs de l'écosystème cyber sont nombreux et couvrent tous les domaines: *Infrastructure security, Endpoint security, Application security, Messaging security, Web security, IOTsecurity, Security Operations & Incident Response, Threat intelligence, Mobile security, Data security, Transaction security, Risk & Compliance, Specialized threat Analysis & protection, Identity & Access management, Cloud security*[50]. Bien qu'aux yeux des DSI l'intervention humaine reste nécessaire, 56 % d'entre eux ont mis en place des solutions fondées sur l'IA pour contrer les attaques ou envisagent de le faire. Au plan ressources, la pénurie de profils est constatée par 91 % des RSSI, alors que seulement 50 % des répondants prévoient d'augmenter leurs effectifs. Seuls 44 % des informaticiens considèrent avoir des compétences de base en cyber, et une entreprise française sur deux estime ne pas disposer de RH sécurité suffisantes, un million de postes étant encore vacants. La cyber-sécurité continue donc d'être une filière en plein essor :

- 18 métiers dont : RSSI, administrateur sécurité, développeur sécurité, chef de projet cyber-sécurité, consultant/auditeur sécurité technique, consultant/auditeur sécurité organisationnelle, correspondant sécurité, DPO, cryptologue, analyste SOC, expert juridique cyber-sécurité, chargé de réponse aux incidents ;
- 19 compétences techniques et fonctionnelles : sécurisation des applications, gestion des accès et des identités, audit de sécurité, protection de l'information, gestion de continuité d'activité, supervision cyber-sécurité, adaptabilité et flexibilité, respect des règles de confidentialité, curiosité intellectuelle…
- plus de 500 formations initiales et continues, dont 150 dispensées par des établissements d'enseignement supérieur et lus de 400 modules de formation courte dispensée par les organismes de formation continue.

Mais bien que la France soit plutôt bien dotée pour cette filière dynamique et en croissance

49 Directeurs des systèmes d'information.

50 Le lecteur nous pardonnera ces termes, l'anglais étant la langue véhiculaire, pour ne pas dire maternelle, du cyber.

avec des entreprises qui recrutent, on note toujours un réel problème d'attractivité. Des axes de travail ont été avancés pour y remédier :

- accroître l'attractivité et la lisibilité :
  - structurer la filière cyber-sécurité,
  - faire connaître la filière et ses acteurs à un public plus large,
  - valoriser les métiers de la cyber-sécurité auprès des lycéens et des étudiants ;
- faciliter l'orientation des lycéens et des étudiants :
  - orienter les bons profils vers la formation initiale,
  - développer des lieux d'échange pour faciliter l'accès à la filière,
  - valoriser les initiatives vertueuses et les bonnes pratiques ;
- accompagner la mobilité professionnelle et la montée en compétences :
  - actualiser les compétences des salariés en cyber-sécurité par la formation continue,
  - renforcer les passerelles IT-cyber-sécurité pour les salariés,
  - sensibiliser les DRH aux métiers de la cyber-sécurité pour orienter les salariés vers des formations qualifiantes et certifiantes ;
- renforcer la sensibilisation des dirigeants d'entreprises sur la cyber-sécurité.

Pour les RSSI[51], le facteur humain reste pour l'avenir l'enjeu principal de la cyber-sécurité. Il impose la formation des utilisateurs**,** qui restent encore peu impliqués et ne suivent guère les recommandations :

- manque de vigilance face aux tentatives d'ingénierie sociale (hameçonnage par exemple) ;
- lacunes dans la sécurisation des systèmes liés à l'Internet, souvent à cause d'une sous-estimation des capacités des attaquants ;
- absence de revue régulière des accès depuis Internet à des comptes privilégiés.

80 % des attaques cyber, qu'il s'agisse de vols, de destruction de données ou de fraudes, sont liées à des comportements à risque des collaborateurs. 41 % des Français utilisent un équipement personnel pour traiter des données professionnelles (étude CLUSIF[52]). Il est donc primordial que chaque salarié soit sensibilisé aux risques informatiques et à leurs enjeux économiques et financiers. Si les mesures d'hygiène et sécurité de l'ANSSI ou *a minima* la charte informatique de l'entreprise étaient respectées, ces chiffres baisseraient rapidement. Le RGPD impose d'ailleurs également que les salariés soient sensibilisés. Idéalement, il serait souhaitable que chaque salarié ait pu suivre un MOOC de l'ANSSI, et soit sanctionné en cas de non-respect des règles de sécurité établies.

Les éditeurs et fournisseurs d'accès ont intégré des fonctionnalités répondants à sept critères : protection contre le cyber-harcèlement, contrôle de l'accès aux contenus pour adultes, contrôle du transfert de données privées, contrôle du temps d'utilisation des appareils, protection contre les pièges à argent en ligne, protection contre le pédo-piégeage *(grooming)*, sécurisation de la sphère privée.

51 Responsable de la sécurité des systèmes d'information.

52 www.clusif.fr

Si l'on en croit des études internationales, dans les pays industrialisés, environ 25 % des enfants ont leur propre smartphone dès six ans. Jusqu'à douze ans, ce taux augmente jusqu'à plus de 90 %. C'est donc une population particulièrement vulnérable qu'il faut protéger, non seulement des contenus inappropriés, mais aussi de l'addiction aux écrans et de l'installation d'applications tierces, les enfants pouvant sans le savoir installer un *malware*. En règle générale, il n'existe pas de fonction particulière pour une menace spécifique. Les fonctions de contrôle parental d'une application doivent plutôt interagir pour éliminer le danger.

L'association *e-enfance* reconnue d'utilité publique, membre du dispositif cybermalveillance.gouv.fr, a pour objectif de protéger les mineurs sur Internet. Son rôle est de sensibiliser les jeunes aux bonnes pratiques du numérique et de conseiller parents et professionnels de l'éducation. Les contenus sont adaptés à la cible, 7-12 ans, 13 ans et plus. En 2017, l'association a rencontré 89 000 jeunes partout en France. Ses journées d'information sont animées par des intervenants professionnels et des volontaires du service civique formés par e-enfance. Dans le cadre de ces activités, les *Trinômes académiques*[53] auraient légitimité à soutenir les actions de *e-enfance,* en alimentant l'association à la fois en ressources pour intervenir auprès des jeunes et en contenus ou en conférences, et en incitant les enseignants à communiquer sur l'existence de ces dispositifs au cas où les jeunes ne les connaîtraient pas.

L'action de sensibilisation permanente pourrait se poursuivre lors du SNU (service national universel), susceptible aussi d'aider à détecter des talents potentiels que l'on pourrait diriger vers une formation initiale en cyber-sécurité. Par ailleurs, la gendarmerie nationale a créé une version « spécial PJGN[54] » de *Time's up*, jeu apprécié des enfants, adapté spécialement à la thématique cyber-sécurité et qui pourrait être utilisé par des intervenants anciens auditeurs IHEDN. Notons aussi une autre initiative intéressante, l'excellent cahier de vacances « les as du Web » de l'INC.

Alors qu'aucun secteur n'est à l'abri et que le cyber-espace permet des attaques massives et ciblées, le RGPD, qui est intrinsèquement lié à la cyber-sécurité, apporte des réponses, notamment en matière d'innovation : sécurité, responsabilité des sous-traitants en leur imposant des obligations, connaissance de l'ensemble de ses traitements et adoption de mesures appropriées, selon le niveau de criticité et d'impact sur les personnes concernées. Il est toutefois rarement perçu comme tel, mais plutôt comme une contrainte administrative et un centre de coût, son adoption effective restant encore très largement insuffisante.

Il était donc intéressant d'examiner en détail la stratégie des principaux acteurs cyber dans le monde, et de comparer l'avancement respectif des États en la matière avec une esquisse de baromètre cyber (page suivante).

53 Organisation décentralisée au niveau des académies, placée sous la tutelle du recteur, de l'autorité militaire territoriale et du président de l'association régionale des auditeurs de l'IHEDN.

54 Pôle Judiciaire de la gendarmerie nationale.

Maturité cyber comparée des pays	IGNORANT 0	NEOPHYTE 1	DEBUTANT 2	CONFIRME 3	EXPERT 4
Niveau de dépendance de la société aux outils numériques et informatiques	Le problème n'est pas compris	Le problème est identifié, les mesures simples sont prises	Le problème est compris, les mesures essentielles sont prises	Les mesures permettent de repousser toutes les attaques connues	Les mesures permettent de détecter et comprendre les attaques à venir et de repousser plus de 80% des attaques inédites
Stratégies publiques de protection et réaction		Inde			États-Unis / Chine / Israël / UK / Estonie / Russie / Luxembourg / France / Japon
Stratégies privées de protection et réaction	Inde			France / Japon / Luxembourg	Chine / Estonie / Israël / UK / États-Unis
Connaissance des menaces actuelles et futures			Inde		États-Unis / Chine / Israël / UK / Estonie / Russie / Luxembourg / France / Japon
Niveau de compétence des spécialistes			Inde	Japon / Luxembourg / Estonie	États-Unis / Israël / UK / Russie / Chine / France
Niveau de compétence des utilisateurs			États-Unis / France / Japon / Chine / UK / Luxembourg	Israël / Estonie	
Audit des vulnérabilités (organismes auditeurs, fréquence des audits et auto-audits)			Inde	France / Russie / Japon / Luxembourg	Chine / États-Unis / UK / Israël / Estonie
Performance de la sauvegarde des données			Inde	Russie / Japon / Luxembourg	Chine / États-Unis / Israël / France / Estonie
Performance de la protection des données			Inde	Russie	Chine / États-Unis / Israël / France / Estonie / Japon / Luxembourg
Garantie de l'intégrité des données				Russie	Chine / États-Unis / Israël / France / Estonie / Japon / Luxembourg
Détection des attaques et pannes			Inde		États-Unis / Chine / Israël / UK / Estonie / Russie / Luxembourg / France / Japon
Réaction technique aux attaques et pannes			Inde	Japon	États-Unis / Chine / Israël / UK / Estonie / Russie / Luxembourg / France
Réaction juridique aux attaques et pannes			Russie / Inde		États-Unis / Chine / Israël / UK / Estonie / Russie / Luxembourg / France / Japon
Capacité de poursuite des activités			Inde	États-Unis / Chine / Israël / UK / Estonie / Russie / Luxembourg / France	
Coopération public / privé		Inde		France / Japon / Russie / Luxembourg / Japon	États-Unis / UK / Israël / Estonie
Coopération internationale	Chine			Israël / Japon	États-Unis / UK / France / Estonie / Luxembourg

États-Unis : le leader en cyber-stratégie

La spécificité de la stratégie cyber des États-Unis vient de leurs deux points de fixation : la Chine et la Russie. Elle doit de plus tenir compte de contraintes de transparence et de respect des lois qui n'existent pas chez leurs deux challengers. Les stratégies classiques de dissuasion par menace de ripostes ne sont pas concevables en cyber, où l'identification de l'origine de la menace n'est pas possible faute de preuves, si ce n'est en se basant sur des menaces révélées passées donc obsolètes, et dont l'auteur n'est pas identifié avec certitude. La persistance de l'engagement à un niveau inférieur à la notion de conflit caractérise donc l'environnement cyber. Il s'en dégage une notion de défense d'anticipation, à l'extérieur des frontières.

Les quatre points saillants de la *National Cyber Security Strategy* (qui date de 2018) sont :
- la supervision des systèmes et des fournisseurs du gouvernement ;
- le développement des compétences en cyber-sécurité ;
- la sécurisation de la chaîne d'approvisionnement fédérale ;
- l'actualisation des statuts juridiques et de la législation des cyber-crimes.

Le cyber-espace a été défini comme domaine stratégique et a donc donné lieu à la création d'une autorité militaire spécifique (USCYBERCOM). L'élévation de l'US Cyber Command au niveau de l'équivalent de nos trois armées fait qu'il développe une doctrine cyber qui lui est propre. Les missions du DoD *(Department of Defense)* en cyber sont :
- défendre ses propres réseaux, systèmes et données ;
- défendre les intérêts nationaux américains contre des attaques cyber d'importance : pertes de vies humaines, atteintes signifiantes aux biens, conséquences sérieuses sur la diplomatie américaine, impact économique important ;
- sur requête du Président ou du secrétaire d'État, fournir un soutien cyber aux opérations et aux plans d'urgence militaires, et à la destruction des réseaux militaires ennemis.

L'arsenal cyber du gouvernement américain comprend également la NSA, dont les activités cyber ont commencé dès les années 50 avec la cryptologie. Elle est plus particulièrement chargée des aspects COMINT, SIGINT, ELINT, protection et soutien des opérations cyber. Sa coopération avec les entreprises privées américaines a permis un efficace espionnage industriel de concurrents des intérêts économiques américains par l'intermédiaire du département américain du commerce. Les activités HUMINT et opérations restent du domaine de la CIA. Les États-Unis collaborent dans le domaine du renseignement avec quatre pays anglo-saxons : le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande *(Five eyes)*. Les activités correspondantes sont confidentielles, mais des indiscrétions montrent clairement qu'elles incluent la cyber.

Le directeur du renseignement national coordonne les activités de dix-sept agences travaillant sur la même thématique du renseignement (sauf la CIA), avec un budget estimé à plus de 80 milliards US$, dont les ⅔ sont des achats à des entreprises privées, lui donnant ainsi un pouvoir d'influence sur le secteur privé en tant qu'acheteur public. C'est par un système basé

sur les commandes des administrations que la stratégie provoque sa propre mise en œuvre. Ainsi, Internet est né d'une commande de la DARPA qui voulait une connexion directe entre les instances du département de la défense US, les chercheurs des universités américaines (Stanford, Berkeley, CalTech, MIT, Harvard), les laboratoires de recherche de l'industrie d'armement américaine (Lockheed, Martin Marietta, etc.), et les entreprises cyber (IBM, Data General, HP,etc.). Ce qui est vrai pour les achats l'est aussi pour le financement des projets de recherche.

L'existence de groupes américains privés spécialisés dans la cyber (les GAFAMI) de taille mondiale permet en outre au gouvernement de contrôler leurs activités dans le monde (extraterritorialité de la loi américaine), comme on a pu le voir avec l'exemple récent de Huawei. Cette utilisation de la position dominante se retrouve dans le domaine de l'audit, où le marché mondial est sous le contrôle des grands cabinets américains, qui ont accès aux informations stratégiques de leurs clients et peuvent se trouver sollicités par les agences américaines dans le cadre du *Patriot Act*. Les grandes compagnies américaines ont une position ambivalente dans cette situation, se présentant comme bons citoyens dans les pays où elles opèrent, mais profitant de cette imbrication entre intérêts privés et intérêt supérieur de l'État américain.

Les États-Unis ont une culture du secret qui leur permet de s'affranchir des règles courantes dans le but de servir les intérêts américains, économiques ou autres. Réciproquement, les agences fédérales sont susceptibles d'intervenir au profit de groupes privés américains dans le cadre de grands contrats (exemple Airbus). Le fait de faire collaborer les agences fédérales et le secteur privé, de construire des relations solides avec les pays alliés et les organismes internationaux, de s'appuyer sur des personnels compétents et sur la capacité nationale d'innovation en matière de cyber, a permis aux États-Unis de se positionner en leader du domaine cyber et d'adopter une posture offensive envers tout ennemi potentiel cyber.

La stratégie nationale cyber des États-Unis indique en quatrième priorité : « *Expand American influence abroad* ». Mais leur ambition se heurte à celles d'autres nations ayant les moyens de leur politique : la Chine, par la taille de son marché et de ses champions (BATX + Huawei), la Russie, qui fait usage du cyber offensif en s'appuyant sur des hackers spécifiquement missionnés, et bientôt l'Inde, partenaire clé dans le domaine des logiciels, et par là-même en position de force en cas d'affrontement. Dans ce contexte, l'Europe et *a fortiori* la France sont inexistantes, bien qu'elles aient des moyens comparables pour leur politique.

Bonnes pratiques à retenir[55]

- un complexe à la fois militaire et économique, public et privé, sociétal et scientifique, en particulier en matière de recherche et d'équipements ;
- maîtrise des éléments clés sur lesquels s'appuient les autres nations pour leurs activités cyber ;

55 International Institute for Strategic Studies / RAND Corporation / Defence Technical Information Center / IEEE / The White House

— commandes de l'administration non focalisées sur le mieux disant, mais sur une stratégie cyber globale.

Royaume-Uni : le pragmatisme anglo-saxon en toute chose

Selon le classement 2018 du GCI (Global Cyber Security Index) le Royaume Uni est le pays leader devant les États-Unis et la France. Il est donc tout à fait intéressant d'identifier les éléments de son leadership qui semble tenir en un seul mot : *mindset.*

Au Royaume-Uni, quatre organes principaux sont en charge des aspects cyber-sécurité et cyber-défense.

— **NCSC (National Cyber Security Center) : «** *Helping to make the UK the safest place to live and work online* **»**. Il a pour mission de protéger et éduquer face aux menaces cyber le secteur privé, le secteur public et les particuliers. Sa doctrine est le Cyber Security Sharing qui met en commun les informations de plusieurs milliers d'entreprises du royaume ;
— **GCHQ (Government Communications Headquarters) : «** *World-leading intelligence, cyber and security agency with a mission to keep the UK safe* **»**. Fondé pendant la seconde guerre mondiale, il a pour mission de lutter contre le terrorisme et l'espionnage industriel, développer l'intelligence économique, lutter contre le crime organisé et apporter un soutien aux « services » et à la cyber-sécurité. Il est en prise directe avec le *Prime Minister Office* comme en France l'ANSSI et L'IHEDN ;
— **SIS (Secret Intelligence Service) MI6 :** Ce service se concentre sur les aspects de cyber-intelligence au sens des menaces extérieures ;
— **SS (Security Service) MI5** : Organise son soutien via le *Centre for the Protection of National Infrastructure* (CPNI) qui produit les recommandations destinées à protéger les services essentiels du pays face aux menaces contre la sécurité nationale.

Bonnes pratiques :

— la NCSC est orientée solutions et particuliers alors que l'ANSSI semble se concentrer davantage sur des publications, textes, etc. Le NCSC a ne approche de fond très pragmatique qui s'adresse dans un langage intelligible aux particuliers autant qu'aux entreprises de toutes tailles ;
— l'objectif de ces services est non seulement la défense mais aussi de faire du Royaume Uni une superpuissance cyber.

Conclusion

Faire en France du cyber un sujet de politique nationale, traité comme majeur, obligeant à la coopération de tous les services nationaux et en collaboration avec L'ENISA afin d'assurer notre indépendance et notre rayonnement sur le sujet. Au moment où le Royaume-Uni quitte l'EU, ce serait une opportunité pour la France de prendre le leadership cyber européen.

Luxembourg : un pays attractif pour les industries du numérique

L'approche luxembourgeoise est très volontariste et vise à motiver l'ensemble des acteurs publics et privés grâce à une organisation lisible, connue et facile d'accès. Il s'agit de garantir la mise en œuvre d'un niveau de protection adapté pour chaque acteur, de conserver en permanence une attitude dynamique, de rester capable de diffuser très vite l'information au sein de la communauté SSI du pays qui partage son savoir relatif aux menaces et aux parades.

Le Grand-Duché de Luxembourg favorise activement l'installation sur son territoire d'acteurs du numérique tels que les distributeurs de contenu numérique, les gestionnaires de données numériques, les vendeurs en ligne, les *cloud services* et les opérateurs de paiement électronique. Depuis 2014, cet effort est coordonné dans le cadre de l'initiative *Digital Lëtzebuerg*. De bonnes infrastructures informatiques et une offre de cyber-sécurité très mature (SMILE, LuxTrust, C3, CIRCL, CASES) facilitent la réussite de cette stratégie avec deux constantes : une très étroite coopération public-privé et une approche pragmatique, résolument orientée vers le meilleur équilibre résultats/ressources.

Bonnes pratiques à retenir

- La recherche d'un double continuum privé/public et professionnel/personnel est un levier de réduction et de traitement des cyber-menaces.
- Savoirs partagés et règles de bon comportement suivies en toutes circonstances.

Estonie : elle a tout des grands

Ayant revu complètement ses priorités depuis la cyber-attaque massive dont elle a fait l'objet en mai 2007, l'Estonie a structuré et solidement articulé sa défense cyber. Dans l'organisation de l'État, on remarque le rôle du ministère de l'économie et des communications, la clarté des responsabilités de chaque organisme, la mise en avant de la police et des douanes, l'imbrication du public et du privé, voire des ONG, l'implication des universités, l'accent mis sur les exercices annuels, les actions vers les utilisateurs finaux, la coopération et la présence internationale, l'élan que donne l'Estonie dans les développements de solutions.

L'Estonie maintient un document officiel sur sa stratégie en matière de cyber-sécurité et le révise tous les quatre ans. Ce document aborde trois domaines : les développements récents, les menaces sur la cyber-sécurité de l'Estonie, les mesures à prendre. Le gouvernement estonien a un Comité de la sécurité auquel a été rattaché un conseil de la cyber-sécurité, dont la mission est de faciliter la coopération interministérielle, et superviser la mise en œuvre des objectifs stratégiques de cyber-sécurité.

L'autorité estonienne des systèmes d'information a la responsabilité de la protection des infrastructures, des technologies de l'information et de la communication de l'État. Elle a un

département de protection des infrastructures et des informations critiques, qui fait une cartographie des interdépendances des services vitaux sur les systèmes d'information, et identifie les besoins pour le fonctionnement des systèmes d'information vitaux de l'État (à comparer à notre ANSSI). Une commission travaille sur la coopération public-privé.

Les attributions de la police et des gardes aux frontières ont été renforcées en matière de cyber-crime, et ont été consolidées en matière de preuve avec les préfectures. La fonction de policier cyber a été créée avec des attributions de sensibilisation, de prévention et d'investigation.

La création de l'unité cyber de la Ligue de défense de l'Estonie permet de développer les collaborations public-privé, et ses volontaires contribuent par leur expertise à l'amélioration de la sécurité des systèmes d'information des administrations et des entreprises par des exercices coordonnés, des tests de solution et de la formation. En situation de crise ils peuvent être engagés pour protéger les infrastructures critiques et venir en soutien des institutions civiles. La participation à des exercices domestiques et internationaux joue un rôle important dans le développement et l'évaluation des capacités. Un partenariat public-privé permet de faire croître la perception et les compétences des utilisateurs de smartphones ou tablettes.

Un champ d'exercice cyber a été mis en place et à la disposition des formations des universités. La Fondation pour l'éducation sur les technologies de l'information est le premier fournisseur en sensibilisation et formation, pour les jeunes et les adolescents. Un Master en cyber-sécurité a été ouvert avec deux universités.

L'Estonie a un e-Centre d'excellence en cyber-crime faisant partie du réseau de l'Union européenne. Elle contribue à l'Otan et à l'UE dans la définition des politiques correspondantes, et coopère avec de nombreux pays. Elle participe au groupe des experts des Nations unies, et à l'OSCE.

La dépendance croissante au cyber de l'État, des entreprises et de la population, détermine les trois points clés de la stratégie cyber de l'Estonie :
- garantir les services vitaux ;
- mieux combattre le cyber-crime ;
- faire évoluer les capacités de défense nationales.

Les domaines connexes sont :
- formaliser le cadre juridique ;
- promouvoir la coopération internationale ;
- accroître la prise de conscience ;
- former les spécialistes et développer les solutions techniques.

Les interdépendances dues aux traitements transfrontières nécessitent des solutions alternatives, l'échange d'informations et l'interopérabilité avec les partenaires internationaux. L'Estonie

a fait le choix stratégique d'expatrier ses centres de données dans des e-ambassades dans des pays de confiance (*Data Embassy* au Luxembourg). La stratégie cyber est confiée au ministère de l'économie et des communications qui dirige et coordonne sa mise en œuvre ; sont impliqués tous les ministères et secrétariats, en particulier la défense, l'autorité des systèmes d'information, la Justice, la police et les douanes, les affaires étrangères, l'Intérieur, l'éducation et la recherche. Les ONG, la société civile, le monde de l'éducation sont appelés à coopérer. L'Estonie a un ambassadeur itinérant sur les questions cyber (Ambassador at large for cyberdiplomacy).

Bonnes pratiques à retenir

- Le secteur privé est partie prenante :
  - considéré comme élément vital du pays,
  - susceptible de développer des solutions,
  - contribue à l'élaboration et au suivi de la stratégie cyber du pays.
- La détermination de l'État est lisible dans son organisation.

JAPON : ACCENT SUR LES CHAÎNES D'APPROVISIONNEMENT

Bien que très sensibilisé à la cyber-sécurité à cause des JO initialement prévus en 2020, mais reportés d'un an, le Japon est en retard par rapport à des nations comparables, isolé, entre autres, par sa barrière linguistique. Par le passé, le Japon a été infecté par *Wanacry* transmis par des compagnies étrangères, partenaires de la chaîne d'approvisionnement.

Il manque au Japon 200 000 informaticiens, malgré une industrie informatique ancienne et développée.

Le patronat local (la *Japan Business Federation* = Keidanren) a rédigé en 2017 un « *Call for Reinforcement of Cybersecurity To Realize Society 5.0* ».

Le NISC, *National center of Incident readiness and Strategy for Cyersecurity*, y joue le rôle de l'ANSSI.

Parmi les besoins, il faut moderniser l'arsenal juridique en matière cyber, revoir l'aspect fiscal pour stimuler l'accélération du passage vers *Society 5.0*, et traiter les risques d'approvisionnement. La « *Japan's cybersecurity policy for supply-chain incuding IoT* », publiée par le ministère de l'économie, du commerce et de l'industrie, inclut une approche en t'rois couches :

- connexion entre les organisations et le milieu physique ;
- connexion entre le physique et le cyber (fonction de transcription : IoT systems) ;
- connexion avec le cyber-espace (fiabilité des données).

Noter que la 5G est vue comme un ordinateur, pas comme un réseau.

Israël : la plus petite des grandes puissances cyber

Des statistiques impressionnantes :

- 109 publications scientifiques/10 000 habitants (1er rang mondial) ;
- 1er rang nombre de brevets/habitant ;
- 4,7 % du PIB consacré à la R&D (1er rang) ;
- 4 prix Nobel ;
- niveau d'éducation : 2e rang mondial ;
- plus grand nombre de start-ups au monde ;
- 20% des investissements privés mondiaux en cyber-sécurité (1/3 en intelligence artificielle) ;
- 750 entreprises de cyber-sécurité : 10 % du business cyber-sécurité mondial.

Le contexte défense : Israël a subi depuis sa création en 1948 plusieurs guerres avec ses voisins arabes. Il est encore en butte à des menaces régionales (Iran, Turquie, Arabie saoudite, Syrie…) et à des attaques constantes, en mode classique (milices chiites) ou cyber (hacking, virus). De ce fait, le pays consacre 5 % de son budget annuel à la défense. Au cours de leur service militaire obligatoire, nombre de jeunes intègrent des unités de R&D ou de cyber comme la fameuse « 8200 ». Certains créent après l'armée leur start-up cyber-sécurité, la plus célèbre étant *Checkpoint*.

Le contexte sécurité nationale : Les cyber-attaques massives permanentes que subit Israël visent ses infrastructures d'importance vitale (télécommunications, centrales électriques ou nucléaires, réseaux de transport, traitement de l'eau), ses sites industriels, ses hôpitaux, ses systèmes bancaires, Internet et les applications associées : mail, media et, surtout, objets connectés. Criminel ou étatique, on est passé du « simple » espionnage au déclenchement de dommages de toutes sortes et à des tentatives d'influence (*fake news*, sondages, cours de bourse). Affronter jour après jour ces agressions explique sans doute la résilience acquise par Israël et son excellence dans le domaine cyber.

INCD (Israël National Cyber Directorate) : Agence civile relevant directement du Premier ministre avec pour mission de traiter tous les aspects de la défense cyber dans le domaine civil, depuis la définition d'une politique et l'élaboration d'une capacité technologique jusqu'à la défense opérationnelle de l'espace cyber civil. En dépend IL-CERT *(Israël Computer Emergency Response Team),* centre de commandement civil qui opère 365 jours par an en 24x24, avec pour vocation de traiter les incidents de sécurité numérique, d'en évaluer l'impact et d'en tirer des recommandations au public qu'il a aussi mission de sensibiliser à ce type de risques.

Contexte système éducatif : accès à l'enseignement supérieur via des tests psychométriques qui conditionnent l'orientation de chaque étudiant en fonction de son profil : tout le monde n'a pas accès à tout. Ces tests permettent de détecter les talents, en particulier en cyber — domaine pour lequel un dépistage est opéré dès le lycée, les meilleurs éléments se voyant proposer un cursus complémentaire.

Israël Innovation Authority : bras armé du gouvernement pour développer la R&D scientifique et technologique dans l'industrie, encourager l'innovation et l'entrepreneuriat, stimuler la croissance économique. Elle gère des partenariats avec l'UE, les États-Unis et autres pays, encourage la coopération entre universités et industrie sur les biotechs, les nanotechs, le cyber et l'équipement médical. Finance 24 incubateurs sur des projets de deux ans (10 % dans le domaine de la cyber-sécurité). Injecte chaque année plus de 500 millions de US$ dans les start-ups.

Jeu global : Le marché intérieur du pays étant beaucoup trop limité, l'entrepreneur israélien raisonne global dès le départ et noue des partenariats à l'international. trente groupes mondiaux dont PayPal, EMC, RSA, VMWare, Deutsche Telekom, Lockheed Martin, CA Technologies et McAfee ont établi des centres de R&D en Israël, et des acteurs majeurs comme IBM, Cisco et GE y ont même installé certains de leurs mégacentres cyber. Israël est partenaire cyber de plus de 80 pays, des plus grands aux plus petits (Singapour).

Cause nationale : Dans ce contexte de tension sécuritaire permanente, la cyber-sécurité est une priorité gouvernementale dans la durée, à la fois instrument de dissuasion, facteur de puissance et vitrine du pays. Mais c'est surtout une cause nationale qui répond au sentiment d'urgence partagé par une population enthousiaste pour les avancées scientifiques et techniques. L'écosystème *Silicon Wadi* réunit des acteurs aussi divers que l'armée, l'enseignement supérieur (Technion, Université de Tel-Aviv, Université Ben-Gourion), des agences gouvernementales, l'industrie, des start-ups, des compagnies à maturité, des incubateurs, des *clusters* comme le Cyber Park de Beer-Shev'a, bouillon de culture cyber-sécurité. Noter le programme gouvernemental Yozma (initiative) d'encouragement à la mise de fonds privés (source : Keyrus).

Bonnes pratiques à retenir

Proximité entre les entreprises, la défense et les centres de compétences, à la hauteur des pays les plus avancés en matière de cyber-sécurité. Organisation basée sur le service militaire et la réserve, permettant de passer facilement du monde de la défense au monde des affaires. Pays attractif pour les grands noms du cyber.

Chine : déjà un leader en cyber et en cyber-sécurité

Très peu d'éléments filtrent sur le fonctionnement cyber derrière la muraille de Chine. Mais une chose est certaine, les lois y sont appliquées strictement et la compliance est une vertu nécessaire. La doctrine cyber-sécuritaire s'articule autour d'une loi fondamentale appelée : la *Chinese Security Law* (CSL). Les exigences de sécurité de la CSL s'organisent autour de la *Multi Level Protection Scheme* (MLPS) qui définit les cinq niveaux de sécurité des entités et leurs obligations.

La Chinese Security Law

Entrée en vigueur le 1er juin 2017 dans le but de renforcer et de sophistiquer l'arsenal législatif chinois depuis l'accession au pouvoir du Président Xi Jinping, cette loi est corollaire à la création

de la *Cyberspace Administration of China* (CAC) en 2012. Ses objectifs affichés sont d'accroître les pouvoirs de surveillance et d'assurer un contrôle total sur le cyber-espace de l'État chinois par la sanction de tout écart, aux fins d'éradication de toute non-conformité à la loi. C'est une loi de type « poupée russe » qui, par une imbrication de lois, définit un cadre général qui met en œuvre la stratégie nationale de cyber-sécurité de la Chine de 2016 spécifiant qu'« il n'y a pas de sécurité nationale sans cyber-sécurité ».

Qui est impacté par la *Chinese Security Law* ? La CSL définit son champ d'application à deux typologies de cibles, décrites ci-après.

NO : Network Operators (opérateurs de réseau),

Ils sont définis comme :
- les entités ou personnes possédant ou gérant un réseau informatique en Chine, et les prestataires de services réseau ;
- les entités ayant soit un site Internet, soit cinq ou plus ordinateurs connectés, soit une adresse IP fixe. Ainsi, même un particulier connecté peut tomber dans ce champ d'application ;

CIIO : Critical Information Infrastructure Operators (opérateurs d'infrastructure d'information essentielle),

Ils sont définis comme sous-ensemble des Network Operators, i.e entités exploitant et/ou gérant des installations réseau et systèmes d'information.

L'idée est de les protéger contre des dommages, destruction, perte de fonction, fuites ou perte de données, ce qui pourrait entraîner une grave menace pour la sécurité nationale, l'économie nationale, les moyens de subsistance des personnes ou l'intérêt public (à rapprocher de nos OIV : Opérateurs d'importance vitale). Ils comprennent :
- les agences et entités gouvernementales dans les secteurs de l'énergie, des finances, des transports, de la conservation de l'eau, de la santé et de l'hygiène, de l'éducation, de l'assurance sociale, de la protection de l'environnement et des services publics ;
- les réseaux d'information, Internet, les services cloud, big data, et autres services de réseau d'information à grande échelle à destination du public ;
- les entités de recherche et de fabrication dans les secteurs comme la science et la technologie pour la défense nationale, les grands équipementiers, les industries chimique, alimentaire et pharmaceutique, la production industrielle ;
- les organes de presse.

Les *Guidelines for Cybersecurity Examination* (juin 2016) élargissent le champ d'application des CIIO's à d'autres structures répondant aux conditions suivantes :
- Pour les sites internet :

- plus d'un million d 'utilisateurs en trafic quotidien moyen,
- risque de violation des données personnelles de plus d'un million de personnes par un incident de cyber-sécurité ;

— Pour les plates-formes :
- plus de dix millions d'utilisateurs enregistrés, ou plus d'un million d'utilisateurs actifs par jour,
- montant moyen des commandes ou du CA quotidien > à 10 millions de RMB (1 Renminbi = 0,13€),
- les *Data Centers* avec plus de 1500 racks standard,
- risque d'incident de cyber-sécurité pouvant :
  - affecter l'approvisionnement en eau, électricité, gaz, pétrole et chauffage, ou le transport de 100.000 personnes,
  - causer la mort de plus de 5 personnes ou des dommages corporels graves à plus de 50 personnes,
  - causer une perte économique directe de plus de 50 millions de RMB,
  - entraîner la violation des données personnelles de plus d'un million de personnes.

En clair, personne ni aucune structure n'échappe à la loi.

Le *Multi Level Protection Scheme* / le MLPS détaille les directives d'organisation sécuritaire des CIIOS.

— Niveau 1: dommages causés au système d'information (ou au réseau *général*) portant atteinte aux droits des citoyens ou des personnes morales, mais ne portant pas atteinte à la sécurité nationale, à l'ordre social ou à l'intérêt public.
— Niveau 2: dommages causés au système d'information (ou au réseau *général*) portant gravement atteinte aux droits des citoyens ou des personnes morales, ainsi qu'à l'ordre social ou à l'intérêt public, mais pas à la sécurité nationale.
— Niveau 3: dommages causés au système d'information (ou à un réseau *important*) nuisant gravement à l'ordre social et à l'intérêt public, et nuisant à la sécurité nationale.
— Niveau 4: dommages causés au système d'information (ou à un réseau *très important*) nuisant gravement à l'ordre social et aux intérêts publics, et à la sécurité nationale.
— Niveau 5: dommages causés au système d'information (ou à un réseau *extrêmement important*) nuisant très gravement à la sécurité nationale.

Ces obligations contraignent les entités à mettre en place de nombreux outils et systèmes de contrôle, afin de réaliser leurs propres audits de conformité et de pouvoir en faire état à la demande des autorités :

— système et règles internes de gestion de la sécurité des SI et réseaux ;
— localisation en Chine des infrastructures ;
— localisation en Chine de la maintenance ;
— localisation en Chine des data personnelles et importantes (dont la définition est assez floue) ;

- personnel dédié à la cyber-sécurité ;
- mesures techniques contre les virus informatiques, les attaques, intrusions, etc.
- conservation des logs pendant au moins six mois ;
- classification des données ;
- back-up et cryptage des données personnelles et importantes ;
- plans d'intervention d'urgence ;
- Monitoring de la sécurité et audits et évaluations des risques
- coopération avec les autorités ;
- notification des incidents aux autorités dans les 24 h ;
- identité réelle des utilisateurs clients ;
- contrôle du contenu ;
- test et auto-évaluation des processus en place ;
- sanctions pénales : jusqu'à 1 million RMB pour les entités en contravention, emprisonnement et jusqu'à 100 000 RMB pour le personnel directement concerné.

Bonnes pratiques à retenir

- La doctrine chinoise en matière de cyber-sécurité est claire : c'est une priorité politique absolue depuis 2012 à laquelle toute entité doit se soumettre sous peine de sanctions lourdes et systématiques.
- Le respect de ces lois est contrôlé par les forces de police, ce qui met sous pression toute entité nationale ou extra-nationale sur le territoire chinois.
- L'ensemble des processus doivent être localisés sur le territoire national, tout étant fait pour une imperméabilité maximale intra-muros.
- La CSL s'étoffe chaque année depuis 2012 dans une imbrication de lois de plus en plus inclusives et précises.

Avec la directive NIS[56], l'Europe accélère, mais reste encore loin derrière la Chine en termes de cyber-sécurité, car elle ne se focalise que sur les OSE[57] et les FSN[58].

Russie : une des grandes cyber-puissances

L'information comme arme de guerre : la Russie a été marquée par le conflit en Tchétchénie. Le pays a des capacités très sophistiquées et a intégré les cyber-outils dans sa politique étrangère et de sécurité beaucoup plus que les autres acteurs internationaux. La cyber-sécurité doit être envisagée sous deux angles : partenariats dans la lutte contre la cyber-criminalité dont le pays et ses acteurs peuvent être victimes ; cyber-renseignement aux fins d'espionnages à l'extérieur et à l'intérieur du pays.

56 Network and Information System Security (juillet 2016).
57 Opérateur de services essentiels.
58 Fournisseur de services numériques.

Il convient de souligner l'extrême opacité qui entoure la Russie sur sa stratégie cyber et les mesures mises en place, et la disparité entre les annonces publiques et la réalité. La Russie a développé un arsenal cyber-offensif de longue date, et sa présence dans le monde cyber est marquée par certains des plus importants intervenants mondiaux : antivirus Kaspersky et réseau social VKontakte (25e site le plus visité au monde), par exemple. Elle est l'auteur (présumé) de cyber-intrusions et d'opérations orchestrées à l'encontre de pays, d'organismes internationaux et d'entreprises. Les premières cyber-attaques connues lancées par Moscou contre l'armée américaine datent de 1986 au moins.

Nombre de pays se sont retrouvés victimes des cyber-attaques russes, destinées à saboter leurs infrastructures physiques (Géorgie, Estonie, Ukraine, Monténégro), ou à alimenter des campagnes de désinformation pendant des périodes électorales ou de tensions diplomatiques accrues (États-Unis, France, Royaume-Uni). Des organisations Internationales comme l'Agence mondiale antidopage (AMA) et l'Organisation pour l'interdiction des armes chimiques (OIAC) ont aussi été ciblées. À l'origine de ces cyber-attaques, deux équipes de piratage les plus compétentes de Russie : APT28 et APT29.

En 2017, les menaces persistantes avancées (*Advanced Persistent Threats* = APT) d'origine russe ont reçu une attention considérable en Europe. Le gouvernement allemand aurait subi une cyber-attaque à grande échelle, lorsque le groupe de piratage russe APT28 a placé des logiciels malveillants dans le réseau gouvernemental et a infiltré à la fois le ministère des affaires étrangères et celui de la défense. Elles ont été mises au jour grâce à de minutieuses enquêtes criminelles cyber reposant sur les indices suivants :

- une sophistication contraire à la recherche mercantile rapide (postulat de soutien logistique d'un État) ;
- des morceaux de code réutilisés dans diverses attaques, signature permettant de suivre les groupes de piratage et d'établir plus précisément le cercle des auteurs ;
- un stratagème pour attirer les attaquants dans des « pots de miel » ou des « balises » (systèmes et informations délibérément implantés afin de les surveiller et de les suivre ou même pirater en retour) ;
- la langue, la géolocalisation, les détails relatifs aux moments réels où les pirates étaient actifs en ligne.

Dès le début des années 2000, la Russie a investi dans des cyber-capacités pour lutter contre les campagnes d'information en ligne tchétchènes, ainsi que pour surveiller, perturber ou réprimer l'activisme en ligne de divers groupes d'opposition russes et de médias indépendants. Elle a investi indirectement dans Facebook et Twitter, adoptant ainsi une approche complémentaire de présence dans la suprématie cyber.

Avec le temps, le besoin d'un minimum de réglementation globale s'est fait sentir. D'où avec les États-Unis (depuis 2013), des règles internationales appelées CBM ou *« Confidence-Building Measures »*, dont la Russie a approuvé en juin 2013 un accord bilatéral dans le domaine cyber.

Une ligne directe a également été établie entre les instances cyber des États-Unis et celles de la Russie, qui est très active dans les instances internationales (UN GGE on ICT, UN OEWG GIP) et recherche les accords bi- ou multi latéraux.

Précédemment connu sous le nom de direction de la sécurité informatique et de l'information (UKIB), l'I*nformation Security Centre* (ISC) du *Federal Security Service* (FSB), est depuis 2002 la principale branche cyber du service de sécurité russe. Responsable au départ de la protection des réseaux informatiques et de la recherche des pirates, il dispose aujourd'hui de cyber-outils développés pour répondre aux menaces à la sécurité nationale et pour museler l'opposition. Au-delà de la simple protection des réseaux informatiques du gouvernement, ses activités englobent désormais également la surveillance étroite d'Internet et des médias, ainsi que des opérations à l'étranger. On a vu en 2013 la création de cyber-troupes, basées sur des hackers patriotes.

Vladimir Poutine a signé en 2000 la doctrine de sécurité de l'information *(Russia´s National Security Strategy 2020)* : la confrontation dans l'arène mondiale de l'information s'intensifie, et la supériorité de l'information dans le cyber-espace est l'objectif essentiel de la Russie. Car les frontières géopolitiques peuvent y être facilement et rapidement franchies, alors qu'il existe encore des obstacles de souveraineté quand il s'agit de systèmes de câbles physiques.

Bonnes pratiques à retenir

- Poursuivre la stratégie défensive de l'UE, faire monter en puissance une approche européenne de la cyber-sécurité,
- Faire émerger des groupes européens de taille mondiale en cyber et cyber-sécurité.
- À partir des compétences existantes, faire de la France une cyber-puissance équipée d'outils de pilotage cyber :
  - traduire la volonté politique par la création d'un grand ministère cyber-industrie et économie (cf. poste de Thierry Breton au niveau de l'UE) ;
  - nommer un coordinateur de politique étrangère et économique cyber avec les experts et institutions déjà existantes ;
  - décliner concrètement le cyber- pour les petites entreprises (PME / TPE / professionnels indépendants / libéraux) ;
  - veiller à la protection de l'infrastructure physique (câbles sous-marins).

Inde : sous-traitant du monde en software

Troisième pays du monde en nombre d'internautes après les États-Unis et la Chine, c'est l'un des premiers émetteurs de spams dans le monde, mais aussi une des cinq nations les plus exposées au cyber-crime (Symantec). L'Inde possède le plus grand centre de développement logiciel au monde à Bangalore, ce qui expose tout pays y faisant appel à une dépendance forte, similaire à celle envers la Chine pour l'industrie numérique.

Parmi les points à noter :

- le *Ministry of Communications and Information Technology* en charge des questions cyber ;
- *National Cyber Coordination Centre* avec des attributions de surveillance ;
- faible niveau de sécurité, exposition aux menaces ; pas d'organisme d'État équivalent à l'ANSSI ;
- *National Cyber Security Policy* datant de 2013. L'Inde a le projet de s'inspirer du GCHQ britannique ; un MOU (*Memorandum of Understanding*) a même été signé entre les agences de cyber-sécurité indiennes et UK,
- projet de recrutement d'experts cyber et de partenariats avec les grands de la cyber-sécurité internationale ;
- NKN (réseau entre les universités indiennes) ;
- *Digital India* (initiative gouvernementale d'accès aux services administratifs) ;
- partenariat national avec Google : Digital Unlocked (le CEO de Google est indien) pour promouvoir le cyber.

En conclusion que retenir ?

L'étude des pays considérés fait ressortir un élément commun saillant : tous les pays étudiés ont pour objectif de faire du cyber un levier de rayonnement et de puissance intérieure comme extérieure :

- les États-Unis en ont fait une arme économique et d'influence en dominant l'offre technologique et de services via leurs géants industriels ;
- la Chine en a fait un outil de contrôle intérieur puissant sur ses concitoyens, ses entreprises et une arme de contrôle des intérêts étrangers présents sur son territoire ;
- la Russie en a fait une arme économique et politique par l'habileté de ses pirates, créant de ce fait un outil de dissuasion extérieure ;
- le Royaume-Uni a clairement exprimé son intention de devenir une cyber-puissance en coordonnant parfaitement l'action de ses Services et en organisant de façon efficace l'éducation de ses entreprises et concitoyens ;
- Israël, à l'instar des États-Unis, atteint une position technologique dominante grâce à ses partenariats et à une armée en mode start-up ;
- l'Estonie, consciente de ses vulnérabilités passées, en a fait une priorité nationale traduite dans une organisation claire et une véritable volonté politique ;
- la Corée du Nord en fait une arme de dissuasion militaire et économique.

La France doit absolument faire du cyber un *sujet politique prioritaire* afin d'élaborer un plan d'action qui lui permette de devenir à court terme une cyber-puissance dans plusieurs domaines à définir, comme la cyber-sécurité. Elle dispose d'un vivier d'experts, certes leaders dans leur domaine, mais disséminés (notamment dans des PME ou à l'étranger, comme aux États-Unis et en Grande-Bretagne), et qui ne sont pas intégrés dans une stratégie nationale globale qui reste encore largement à définir. La politique cyber doit se décliner en une *cyber-économie* et une *cyber-industrie*, où la détermination de la France pourra se révéler au travers d'un écosystème performant, de ses investissements et de sa capacité d'impulsion européenne.

Chapitre IX

Et demain ? Une prospective cyber

L'objectif recherché est de réaliser une étude prospective afin de déterminer ce que pourrait être le cyber-espace[59] dans quinze ans et ses implications pour la France. Il s'agit d'en envisager les types d'acteurs, les grandes logiques, les enjeux et les problématiques qui risquent de se poser à différentes échelles géographiques : nationale, européenne, internationale. Le groupe de travail était constitué d'anciens auditeurs de l'IHEDN, d'étudiants de l'ILERI[60] et de membres de l'association Cyb-RI[61]. Il était intéressant d'impliquer dans cette réflexion les jeunes, acteurs actifs de l'environnement cyber dans quinze ans, leur point de vue sur l'avenir étant une des clés de cette analyse prospective.

Méthodologie

Faire une projection dans le futur à quinze ans dans le domaine des technologies de l'information est un pari audacieux et risqué, compte tenu de leur vitesse d'évolution et de la difficulté à anticiper les phénomènes de rupture. Ce choix de quinze ans a le mérite d'être suffisamment proche pour ne pas risquer d'écrire une nouvelle d'anticipation farfelue, mais suffisamment lointain pour dépasser le *business model* des entreprises et les projets politiques du moment. Il dispose de l'horizon de temps nécessaire pour porter une réflexion ambitieuse pour l'avenir, tout en s'affranchissant autant que possible de spéculations purement technologiques que nous souhaitons dépasser.

Un des risques de l'exercice est de considérer le futur comme un continuum linéaire du présent: *« La plus étrange prédiction à ne pas s'être réalisée dans le domaine des transports, bien que dans des circonstances éminemment excusables, date des années 1890. On prévoyait à l'époque que les rues de New York seraient recouvertes de cinquante centimètres de crottin de cheval dans un délai de trente ans en raison de l'accroissement de la circulation »* (Jean Gimpel - *La fin de l'avenir : la technologie et le déclin de l'Occident)* . Une prédiction qui n'avait évidemment pas prévu l'apparition de l'automobile…

59 Nous utiliserons dans ce document la définition du cyber-espace issue du glossaire de l'ANSSI (https://www.ssi.gouv.fr/entreprise/glossaire/c/, consulté le 1er janvier 2020). Le cyber-espace est un espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

60 ILERI : Institut libre d'étude des relations internationales.

61 Cyb-RI : travaille sur les interactions entre les aspects cyber et les relations internationales.

Dans un premier temps, conscients qu'une des difficultés de la projection est la quasi impossibilité d'anticiper les prochaines ruptures technologiques, nous avons posé comme postulat que ce ne sont pas elles qui façonnent la société, mais que c'est la société qui suscite l'émergence de ces ruptures. À titre d'exemple, l'iPhone, rupture technologique majeure apparue en 2007, avait un prédécesseur, le Newton MessagePad d'Apple, sorti 14 ans plus tôt sans réel succès. Une technologie nouvelle n'entre dans la société que si le contexte le permet. Nous avons donc choisi d'étudier ce que pourraient être les contextes possibles dans 15 ans en nous appuyant sur une classique analyse PESTEL[62]. L'approche retenue est donc multidimensionnelle et prend en compte des considérations politiques, géopolitiques, socio-économiques, juridiques, technologiques et éthiques. Elle permet de prendre du recul sur l'évolution des technologies que nous connaissons aujourd'hui et qui laisseront la place à d'autres qui répondront mieux aux problématiques futures.

Dans un second temps, nous avons décidé de créer une « machine à remonter le temps ». Afin d'imaginer ce que sera le cyber-espace dans 15 ans pourquoi ne pas revenir 15 ans en arrière et étudier ce qui, au début des années 2000, nous aurait permis d'anticiper le cyber d'aujourd'hui ? Cette approche a permis d'identifier, sélectionner et pondérer les facteurs multidimensionnels, qualitatifs et quantitatifs à transposer dans le futur. Les éléments de ce modèle composé pourront être discutés et ajustés, un peu comme les modèles météorologiques qui mûrissent au fil des années pour devenir de plus en plus fiables.

Le troisième temps a consisté en une confrontation avec des experts que, sans prétention de détenir une vérité, ce travail donne l'occasion de solliciter et de mobiliser dans différents domaines. L'avantage d'un modèle multidimensionnel multi-facteurs est que chaque indicateur peut être projeté individuellement dans le futur avec l'aide des spécialistes de ces phénomènes et de leur évolution. D'où une première série d'entretiens auprès de personnalités appartenant à différents secteurs : public ou privé, recherche ou entreprise, corps d'État, ingénieurs, etc…

Scénarios

À l'issue de ces trois phases, et en particulier de la phase d'entretiens, il est apparu indispensable de scinder l'étude en deux scénarios possibles : l'un optimiste ou « souhaitable », vers lequel il s'agirait de tendre, l'autre pessimiste ou « non-souhaitable » qu'il s'agirait d'éviter, chacun de ces scénarios devant être suffisamment extrême pour que la réalité se situe entre les deux. Les indicateurs proposés pour évaluer une politique rationnelle d'évolution et mesurer ses effets, devraient permettre de définir le stade auquel se situe la France entre ces deux scénarios extrêmes.

62 L'analyse PESTEL est un modèle permettant d'identifier l'influence que peuvent exercer les facteurs macro-environnementaux politique, économique, sociologique, technologique, environnemental et légal.

Le cyber il y a quinze ans

Les origines

Même si le cyber-espace ne se limite pas à la seule technologie internet, celle-ci en est quand même une partie importante et son histoire perpétue l'importance stratégique des technologies de l'information et de la communication.

La guerre franco-prussienne de 1870 a montré à quel point les télécommunications, en l'occurrence le télégraphe, étaient un facteur important de la tactique, de la logistique et, donc, de la progression militaire dans le cadre de conflits armés[63]. La Seconde Guerre mondiale a démontré le rôle des calculateurs dans la cryptographie et la cryptoanalyse[64]. À la sortie du conflit mondial, ces deux technologies restaient intéressantes militairement dans un contexte de guerre froide, mais elles permettaient aussi de répondre à des besoins de la société civile. Le téléphone se développait de son côté, commençant à supplanter le télégraphe, mais toujours sur un modèle de transmission de messages.

En 1961, Leonard Kleinrock du MIT imagine pour la première fois une transmission d'informations « par paquets », les messages étant fractionnés et transmis indépendamment dans le réseau, pour être réassemblés à la fin. Ce système offre l'avantage de ne devoir retransmettre en cas d'erreur que les paquets manquants, ce qui augmente la performance globale de la transmission, chaque paquet étant capable d'emprunter un chemin alternatif en cas de panne, ainsi que la fiabilité et la résilience[65] du réseau.

Les États-Unis d'Amérique sont alors très intéressés par ces capacités qui devraient permettre, dans un contexte de guerre froide et de menace nucléaire, de limiter les possibilités de sabotage sur les transmissions, tout en préservant une capacité de riposte maximale grâce à la résilience du réseau. L'ARPA[66] se voit ainsi confier la réalisation d'Arpanet, réseau de communication fondé sur les théories de Kleinrock, et impliquant académiques et industriels.

En France, un réseau, baptisé projet Cyclades et piloté par Louis Pouzin[67], est aussi mis au point expérimentalement. Il donne naissance au concept de télématique qui, grâce au Minitel, facile d'usage et accessible gratuitement à tous, offrira aux citoyens français les tout premiers services en ligne : services bancaires, annuaire en ligne, messagerie électronique, vente à distance, accès aux services administratifs, etc.

63 Aymeric Bonnemaison et Stéphane Dossé, *Attention: cyber ! : Vers le combat cyberélectronique,* Economica, 2014.

64 Dermot Turing, *Enigma: Ou comment les Alliés ont réussi à casser le code nazi,* Nouveau monde * ministère des armérs, 2019.

65 Résilience : capacité d'un système ou d'une architecture réseau à continuer de fonctionner en cas de panne.

66 *Advanced Research Projects Agency* : agence du DoD (Département de la défense des États-Unis) chargé de la recherche et du développement des nouvelles technologies à usage militaire, ancêtre de la DARPA.

67 Louis POUZIN : https://fr.wikipedia.org/wiki/Louis_Pouzin.

Vers la fin des années 70 existent de nombreux autres réseaux issus de recherches universitaires ou industrielles, et les ingénieurs commencent à prôner leur interconnexion. Ce concept d'*inter-networking*, passerelle entre les réseaux ou réseau de réseaux, se raccourcira finalement en « Internet ».

Internet

Il y a quinze ans Internet émergeait de la « bulle Internet », période effervescente durant laquelle de nombreuses organisations ont sauté le pas d'une présence web via le réseau Internet. Une nouvelle économie pleine de promesses voyait le jour, eldorado pour les uns, spéculation pour les autres, mais au final faisant connaître ce nouvel outil au grand public au travers de publicités et de produits dérivés « point.com ». La conception même de sites Internet est facilitée par de nouvelles technologies qui permettent de répondre à la demande croissante de la société. De nouveaux outils apparaissent comme des sites clé en main personnalisables, offrant à des novices en informatique la possibilité de créer leurs propres sites web, blogs, forums ou boutiques en ligne, sans devoir passer par un « professionnel ».

Cette volonté du grand public de s'affranchir d'experts pour partager des idées et des contenus est un premier indicateur et une des clés de compréhension du monde cyber aujourd'hui.

Les télécommunications

La croissance de la demande en accès internet a poussé les acteurs des télécom à investir dans de nouvelles technologies. Du seul appui sur la téléphonie via l'utilisation de modems, le réseau a petit à petit migré vers le « tout IP ». L'émergence de l'ADSL, de la 2G et de la 3G a permis l'augmentation des performances, la diminution des coûts et une omniprésence des moyens d'accès. Là encore, les besoins de la société ont transformé les modèles classiques de télécom et expliquent la présence 15 ans après de moyens capables de faire transiter sur Internet, voix, télévision, vidéo à la demande, etc.

Les terminaux

Cette évolution des télécom, et le volume gigantesque d'équipements utilisés par cette industrie, ont facilité les investissements dans la micro-électronique et dans la miniaturisation des composants. De nouveaux types d'écrans de haute résolution et intégrant le tactile ont vu le jour et ont remis au goût du jour des technologies comme celle du vieux Newton MessagePad d'Apple, réincarné en iPhone et iPad. De nouveaux systèmes d'exploitation ont été développés spécifiquement pour exploiter ces « smartphones » devenus des micro-ordinateurs bien plus que des téléphones. Les ordinateurs eux-mêmes ont accéléré leur évolution, devenant de plus en plus souvent des terminaux permettant l'accès « en ligne » à des ressources (stockage par exemple) et des services (SAAS[68]).

68 Le logiciel en tant que service, ou Software as a Service (SaaS), est un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur. (wikipedia)

Le cyber dans quinze ans : scénario optimiste/souhaitable

Il s'agit d'encourager le processus de pacification, de régulation et de démocratisation du cyberespace

Les États

Au cœur de la réflexion stratégique française, le cyber-espace doit être appréhendé comme un élément de souveraineté et un espace géopolitique, tant du fait de ses réalités matérielles que du fait des conséquences économiques, diplomatiques, politiques et géographiques concrètes, des actions menées dans la sphère cybernétique. Considérant que le cyber-espace apparaît comme un nouveau théâtre de compétition, voire d'affrontements entre États, ce sont ces derniers qui auront en priorité la charge d'assurer son caractère pacifique et sa démocratisation par des processus de négociation opérables à plusieurs échelons.

À l'échelon international

Dans une perspective idéale, le cyber-espace a vocation à être régulé par le concert des nations sur une base volontariste et universelle. C'est un objet central des relations entre États, dans un monde globalisé faisant des nouvelles technologies de l'information et de la communication un enjeu affectant l'ensemble des nations sans distinction. Il est donc à la fois logique et légitime d'instaurer des mécanismes internationaux de régulation adaptés à l'ampleur du phénomène, impliquant tous les membres de l'ONU à travers son Assemblée générale, organe privilégié pour encadrer les applications cyber sur une base égalitaire et universelle. Cette AG de l'ONU semble être l'organe le plus susceptible de mener un débat constructif, doté de la plus forte légitimité, pour démarrer des concertations et des projets de coopération, chaque État bénéficiant d'une voix égale[69], pour ne pas marginaliser les États qui n'ont pas moyen de faire entendre leur voix autrement que dans ce cadre institutionnel, ni renforcer les inégalités existant entre pays membres de l'OCDE et pays en développement.

L'ajout aux six commissions existantes de l'ONU d'une septième commission « cyber », compétente sur des questions techniques, mais aussi juridiques, économiques et sécuritaires serait le signal d'une réelle prise en considération des défis cyber-cruciaux qui se présenteront dans les années à venir. Cette commission spécialisée permettrait d'alléger l'agenda et la programmation de la première commission, dont la part de travaux sur le cyber-espace s'intensifie depuis 2017[70].

Il devrait revenir au Conseil de sécurité de l'ONU de prendre en charge la question de la paix et de la sécurité dans le cyber-espace, tant dans sa dimension physique (protection des câbles de

69 Fonctionnement de l'Assemblée générale, Organisation des Nations unies, https://www.un.org/fr/ga/about/background.shtml.

70 Entretien avec Chelsey Slack (Deputy Head of the Cyber Defence Section), le 13.11.19

fibre optique, des infrastructures, des serveurs) que dans sa dimension immatérielle (protection des réseaux, des flux de communication, des systèmes d'exploitation, des applications voire des données elles-mêmes). À cet effet, la France doit promouvoir l'intégration de la question cyber dans les prérogatives du Conseil de sécurité, au titre de sa mission de maintien de la paix et de la sécurité internationales[71].

INDICATEURS QUANTITATIFS	INDICATEURS QUALITATIFS
- Nombre de résolutions de l'Assemblée générale de l'ONU sur les problématiques cyber - Degré de consensus ayant permis l'adoption des résolutions (votes pour, contre, abstentions) - Caractère contraignant ou déclaratif des résolutions adoptées	- Contenu des résolutions de l'AG de l'ONU
-Durée des débats au sein de l'AG concernant les problématiques cyber	- Existence ou non d'organes chargés de surveiller l'application des engagements des États
- Nombre de résolutions adoptées par le Conseil de sécurité concernant les questions cyber	- Utilisation des chapitre VI ou VII de la Charte ONU pour des opérations de maintien de la paix et de la sécurité internationale dans le cyber-espace

À l'échelon de l'Europe

Dans le contexte d'une France européenne et européiste, il faut promouvoir dans les années à venir l'intégration comme voie privilégiée pour aborder la régulation du cyber-espace afin, notamment, de faire apparaître l'Union européenne comme un contrepoids crédible face aux États-Unis, à la Russie et à la Chine.

L'UE a pratiquement perdu la bataille du *hardware* et du *software*, mais elle a encore un rôle à jouer dans la bataille des normes en tant que premier marché au monde. Et dans la mesure où avec le Brexit elle n'a plus désormais de membre partie se des *Five Eyes*[72], elle est face au le défi de devenir une troisième voie à part entière face aux puissances concurrentes[73]. Il faudrait donc veiller à :

- créer les conditions fiscales, juridiques et technologiques favorables à l'émergence de géants du numérique européens, avec un capital réparti entre les différents États et groupes privés existant à l'échelle de l'UE ;
- soutenir le développement des acteurs du numérique français (à l'instar de Qwant, OVH) et européens existants, afin qu'ils deviennent véritablement concurrentiels face aux GAFAM et aux BATX ;

71 Chelsey Slack, op.cit.

72 *Five Eyes* : Alliance des services de renseignement de l'Australie, du Canada, de la Nouvelle-Zélande, des États-Unis et du Royaume-Uni

73 Entretien avec Stéphane Bortzmeyer (ingénieur R&D à l'Afnic et auteur de *Cyberstructure : Internet, un espace politique, C&F éditions, 2018*), le 15.12.19

- œuvrer au développement d'un cadre légal national et européen favorisant l'émergence de solutions et d'entreprises avec pour objectif de devenir les prochains leaders mondiaux de cette technologie blockchain qui révolutionnera nos sociétés comme l'a fait Internet ;
- faire du couple franco-allemand le moteur d'une Europe du numérique, qui pourrait prendre pour modèle les programmes d'intégration existant déjà au niveau régional pour les industries de défense ;
- intégrer les moyens de lutte contre le cyber-terrorisme et les cyber-attaques en coordonnant les efforts et les ressources des 27, et en s'appuyant sur des technologies de partage d'informations sécurisée ;
- renforcer l'ENISA[74] (budgets, ressources humaines, visibilité) ;
- définir une politique cyber commune, qui pourrait devenir à terme une compétence supranationale et totalement intégrée, suivant par exemple le modèle actuel de compétence de l'UE en matière monétaire.

Faire de l'UE un acteur crédible du cyber-espace suppose une forte volonté politique. Il faudrait qu'un certain nombre de critères de convergence à la fois économiques, juridiques et politiques soient remplis et que les processus d'intégration obtiennent l'aval de l'ensemble des pays membres[75], chacun devant faire preuve d'une réelle volonté de progresser vers un traitement commun et renforcé des affaires cyber. À défaut de voir l'UE des 27 réussir cette convergence, il ne faudrait pas hésiter à créer de toutes pièces une Communauté européenne du numérique avec ceux des États membres qui auraient une vision et une volonté communes. Elle serait le pilier d'une nouvelle coopération régionale dans ce secteur stratégique, avec possibilité d'un éventuel futur élargissement.

Indicateurs à prendre en compte

QUANTITATIFS	- production juridique du Parlement européen sur le cyber - production juridique de la Commission européenne sur le cyber déclarations et résolutions émanant du Conseil de l'UE sur le degré d'intégration cyber souhaité par les États
QUALITATIFS	- prérogatives de l'ENISA et moyens alloués - évolution de la jurisprudence européenne cyber et impact sur les juridictions nationales

À l'échelon bilatéral

La capacité de la France à répondre avec réactivité et célérité aux défis posés par le cyber est cruciale. Afin de pallier les éventuelles difficultés en matière de développement de la coopération

74 ENISA : *European Networks and Information Security Agency :* Agence européenne chargée de la sécurité.

75 La prise de décision dans l'Union européenne, *Commission européenne*, https://ec.europa.eu/info/strategy/decision-making-process_fr

multilatérale et/ou régionale, la mise en place de partenariats stratégiques bilatéraux pourrait constituer une première étape à privilégier, dès lors que les conditions de coopération à plus de deux États ne sont pas réunies. Il s'agira alors d'établir une liste de critères hiérarchisés pour identifier les états partenaires les plus susceptibles de favoriser les intérêts français dans le cadre d'accords cyber bilatéraux.

À l'échelon national

La France s'est engagée dans l'élaboration d'un *New Deal* afin de devenir une grande puissance numérique, sur la base de trois concepts clés que sont le volontarisme, la résilience et l'innovation. Ce *New Deal* doit permettre de mettre en place un minimum d'éducation cyber à tous les stades de la scolarité (épreuve au brevet des collèges, cours en seconde, épreuve au niveau baccalauréat, cours en licence, cours/épreuves en Master), afin qu'aucun élève ou étudiant n'échappe aux bases minimales nécessaires à la future vie du citoyen connecté.

En quinze ans, toute une génération aura été formée et initiée aux enjeux sécuritaires du numérique et sera en mesure de déployer ses compétences à travers tous les pans de la société, en participant activement à la transition numérique et en développant des solutions uniques au niveau international. Une mise à niveau régulière aura été effectuée à l'échelle nationale sur la base des MOOC de l'ANSSI appuyés par des campagnes de promotion.

Les acteurs non étatiques

Le développement des NTIC et la généralisation des enjeux cyber, phénomène transnational par excellence, dans les domaines diplomatique, militaire, économique et scientifique, conduisent à ne pas réduire celui-ci à un seul « problème » d'État à État, qui aurait le droit international comme seul cadre normatif de réglementation. Des acteurs non-étatiques doivent aussi être pris en compte : les géants du numériques (et leurs sous-traitants) ainsi que leurs lobbies, les cabinets de conseil et d'audit, les hackers dans leur diversité, les professionnels (experts techniques, juristes, avocats…), les groupes terroristes, et bien sûr les citoyens.

Multiplication des codes de conduite sur le cyber et développement de la « Soft Law »

Les « codes de conduite » sont un ensemble conventionnel de pratiques et d'attentes considérés comme liant tous les membres d'un groupe particulier. Selon la théorie juridique classique, ils sont définis comme du « droit mou » (*soft law*) car ils n'ont pas de caractère contraignant et ne reposent que sur l'engagement volontaire d'acteurs variés qui acceptent de s'imposer mutuellement des normes les astreignant à un certain comportement[76].

76 RICHARD J., CYTERMANN L., Conseil d'État, *« Le droit souple : quelle efficacité, quelle légitimité, quelle normativité ? »*, https://www.dalloz-actualite.fr/interview/droit-souple-quelle-efficacite-quelle-legitimite-quelle-normativite#.XiTK4chKg2w

Ces acteurs à la base de l'émergence de nouveaux codes de conduite sont extrêmement divers : organisations internationales (ONU, OCDE), États à titre individuel, acteurs privés (entreprises, ONG, associations, clusters, organismes de labels et de certification) ou encore groupes mixtes[77]. Cette dernière catégorie est d'ailleurs susceptible d'obtenir le plus large consensus, le plus grand développement et la plus forte légitimité, dans la mesure où elle implique le nombre le plus important d'acteurs et la plus grande diversité[78].

Exemples de codes de conduite pouvant servir de modèle : Droit international humanitaire et des conflits armés

ONG « Appel de Genève (2000) »[1] :

Acte d'engagement portant sur l'interdiction des mines anti-personnelles, la protection des enfants et l'interdiction des violences de genre dans les conflits armés. Quand des acteurs armés adhèrent à l'un de ces engagements, ils s'engagent à respecter ce code de conduite, qui est en réalité une reprise de normes conventionnelles existantes. Cela permet à des acteurs dont le statut ne permet pas d'adhérer aux conventions internationales, de respecter certains engagements (dans le but d'acquérir une plus large légitimité ou visibilité). C'est aussi un moyen de contourner les États (notamment ceux réticents à s'engager dans les processus multilatéraux, refusant de participer aux protocoles de coopération, et enclins à poser un veto systématique au Conseil de Sécurité). L'ONG prévoit un protocole de surveillance et de sanctions opéré par des experts de l'Appel de Genève : dans l'hypothèse d'un non-respect par l'acteur.

1 Site officiel de l'Appel de Genève, https://www.genevacall.org/how-we-work/

Document de Montreux (2011)[1]

Code de conduite élaboré à l'initiative de la Suisse et du CICR (Comité international de la Croix-Rouge) auquel 53 États ont adhéré à ce jour. Il réglemente les actions des entreprises militaires et de sécurité privée. Les entreprises qui y adhèrent s'obligent à respecter les standards du droit international humanitaire et des conflits armés, ainsi que le droit international des droits de l'Homme, nonobstant la législation des États sur le territoire duquel elles opèrent.

1 Intégralité du document de Montreux disponible sur https://www.eda.admin.ch/dam/mission-otan-brussels/fr/documents/Montreux-Dokument_fr.pdf

Technologies innovantes et enjeux éthiques

L'espace urbain du futur : Les *Smart Cities* (villes intelligentes) connaissent une croissance importante à l'échelle globale et occupent un champ de plus en plus présent dans les politiques publiques françaises à l'échelle nationale et locale. L'optimisation de l'espace urbain touche à quatre domaines principaux : l'énergie, le management des ressources naturelles et des services publics, la mobilité et les relations sociales[79].

77 FRYDMAN B., *Petit manuel pratique de droit global*, Académie royale de Belgique, 2014

78 GESLIN A., *Introduction au droit global*, IEP d'Aix-en-Provence, 2018

79 OURAL A., Rapport au ministère de l'Europe et des affaires étrangères, http://www.smartcitymag.fr/src/ressources/00/00/00/61/vers_un_modele_francais_de_villes_in_522516_a.

Énergie

Dans le contexte global d'urgence climatique, il s'agit pour la France, de comprendre son environnement pour mieux l'appréhender et de mettre en place des projets d'adaptation efficaces dans l'espace et dans le temps. Voyons les possibles scénarios quant à l'utilisation future du cyber et son impact sur l'environnement.

La *Smart City* doit être durable, et tendre vers un objectif de décarbonation de l'énergie. Étant le secteur le plus énergivore *devant le transport*, le secteur énergétique doit opérer une transition vers les énergies renouvelables tout en optimisant la production, le transport et la consommation de l'énergie. De multiples communautés énergétiques[80] locales émergent, portant sur de nouvelles méthodes de gestion de l'énergie et de diversification de la production (solaire, éolienne, biomasse), de même que de nouveaux usages liés à l'habitat et la mobilité. Dans ce contexte, associer les enjeux de transition énergétique aux possibilités des technologies numériques, doit devenir pour la France l'axe de développement majeur, celui qui la fera entrer dans le club des pays les plus innovants.

Parmi les plates-formes de sciences participatives dans le domaine énergétique en France citons COMEPOS et ENERGIHAB. L'initiative COMEPOS[81] se base sur l'étude, la conception technologique, la simulation et le monitoring de 25 bâtiments à énergie positive répartis sur le territoire français. Depuis 2013 des citoyens (constructeurs, résidents) sont impliqués dans le suivi et le retour d'expérience sur l'efficacité du projet. La plate-forme ENERGIHAB[82] permet quant à elle de suivre et d'améliorer la performance thermique des bâtiments. Il s'agit de combiner des approches socio-économique et technique afin de mieux comprendre le comportement des habitants et d'en tenir compte dans les plans d'urbanisation, en créant des indicateurs fiables qui permettront d'élaborer un observatoire de la consommation énergétique des ménages, associant pratiques spatiales et performances techniques des bâtiments.

Au niveau de l'industrie, l'utilisation de s*martgrids* (réseaux électriques intelligents) dans les écoparcs industriels est un bon moyen d'optimisation, en utilisant les rejets énergétiques pour créer de l'électricité et réduire ainsi le gaspillage. À l'échelle individuelle, une utilisation plus responsable des énergies, notamment avec la domotique dans le cadre de l'habitat, devrait permettre de coordonner l'effort environnemental de la ville avec celui de l'industrie. La mise en place d'installations photovoltaïques et éoliennes sur des maisons individuelles pourrait également réduire l'empreinte carbone de la ville, tout en réduisant la part du budget des ménages réservée à la facture énergétique. Chaque ville ayant ses spécificités et capacités propres, il va de soi que chaque ville élaborera sa propre évaluation de ses besoins et des solutions énergétiques les plus susceptibles d'y répondre.

80 Planete energies, « *Nouvelle gestion des « communautés énergétiques »,* 5 mars 2018. https://www.planete-energies.com/fr/medias/decryptages/nouvelle-gestion-des-communautes-energetiques

81 Concept de maison individuelle à énergie positiveitive tous usages http://www.comepos.fr/

82 Jean-Pierre Lévy de l'Agence nationale de la recherche (ANR), 'La consommation énergétique : de la résidence à la ville. Aspects sociaux, techniques et économiques – ENERGIHAB', *Villes Durables*. https://anr.fr/Projet-ANR-08-VILL-0006

Gestion des ressources naturelles et services publics

Dans le contexte de modification et de perturbation climatiques déjà évoqué, l'utilisation des ressources naturelles devrait être conforme au principe de soutenabilité (*sustainability*). La collaboration entre les différents acteurs de la ville devrait permettre un meilleur pilotage des services publics, une réduction de l'empreinte écologique et une économie d'énergie massive. Parmi les dispositifs fondés sur l'IoT (Internet des objets) qui peuvent aider les pouvoirs publics à optimiser la consommation de ressources naturelles, citons:

Gestion de l'eau	arroseurs connectés pour la gestion des systèmes hydrauliques des espaces verts, dotés de détection des fuites et d'analyse de la consommation. (exemple de Montpellier*) contrôle en temps réel de la qualité de l'eau, permettant de réduire les dépôts sauvages. (exemple d'Angers**)
Gestions des déchets	bennes à ordures connectées, alertant les services techniques lorsqu'elles sont pleines. (exemple de Cannes***). réseaux pneumatiques souterrains (exemple du quartier Clichy-Batignolles à Paris****)
Éclairage	généralisation du 'smart lighting'*****, dispositif permettant de s'alimenter à l'énergie solaire, de servir de relais pour les réseaux mobiles et le WiFi, et d'accueillir des capteurs environnementaux (exemple de Toulouse[6]).

* UCOPIA, 'Smart Cities : les nouvelles technologies au service de l'espace urbain'. https://ucopia.com/actualites/nouvelles-technologies-espace-urbain/

** Bastien L, 'Angers investit 178 millions € pour devenir la première smart city française', 26 novembre 2019. https://www.objetconnecte.com/angers-smart-city/

*** Romain Sost, 'Des poubelles connectées, qui alertent quand elles sont pleines, installées à Cannes', France Bleu Azur, 8 février 2018. https://www.francebleu.fr/infos/insolite/poubelles-connectees-la-ville-de-cannes-en-ajoute-10-1518083766

**** Fanny Le Jeune, 'Smart city : vers quelle gestion intelligente des déchets ?', 16 mai 2018. https://les-smartgrids.fr/smart-city-gestion-intelligente-dechets/

***** Bastien L, 'Smart cities : le marché des lampadaires connectés va croître de 30% par an', 7 octobre 2019. https://www.objetconnecte.com/smart-cities-lampadaires-connectes/

****** UCOPIA, op.cit.

Mobilité

L'optimisation de la mobilité des citoyens en ville est un enjeu majeur des années à venir, au croisement des préoccupations sociale, environnementale, politique et technique. Avec le développement des télécom et de l'IoT, les exemples de solutions technologiques permettant une meilleure mobilité se sont multipliés dans les dix dernières années : *gestion en temps réel des transports en commun, de la circulation, du stationnement, du parc automobile et des bornes de recharge, stations de vélos partagées, trottinettes électriques, navettes autonomes, métros ou tramways automatisés…* Ces initiatives proposent une mobilité moins polluante tout en invitant les citoyens à porter un autre regard sur le partage par rapport à l'attachement traditionnel à la propriété privée.

Réduisant les émissions de CO_2 ainsi que la part du budget des ménages consacrée à l'énergie, ces dispositifs deviennent des solutions que s'approprient progressivement les citoyens, et qui deviendront d'ici 2035 la voie privilégiée de mobilité en centre urbain. À deux conditions toutefois : sensibiliser le plus grand nombre au partage de l'espace urbain, à la sécurité routière, à la sécurisation du réseau des objets connectés et, surtout, équiper les villes en infrastructures adaptées.

Relations sociales et personnelles

Les relations sociales, qu'elles se déroulent dans la sphère professionnelle, publique ou privée, sont de plus en plus dématérialisées : *accroissement de l'utilisation de visioconférences, du télétravail, du travail collaboratif et du recrutement digital par exemple*. Le gain de productivité offert par ces technologies peut avoir pour contrecoup la dégradation du lien social existant entre les gens. Une implication croissante des citoyens est donc nécessaire dans le fonctionnement de ce nouveau type d'environnement. Elle doit découler d'une réflexion socio-économique et éthique menée en amont du déploiement de ces dispositifs, avec des études d'impact menées par des cabinets d'experts à la demande des collectivités territoriales, en n'oubliant pas que seule une démarche politique associant le plus grand nombre, permettra de faire émerger le sentiment d'appartenance indispensable pour garantir l'investissement de chacun dans la future *smart city*.

Recherche environnementale : « IT for Green »

Ingénieurs et scientifiques coopèrent en vue d'améliorer la protection de l'environnement au moyen de la géo-ingénierie. Les deux techniques au cœur des programmes de recherche actuels sont le retrait du carbone de l'atmosphère, et la réflexion des radiations solaires vers l'espace.

Ce travail sur l'environnement reste au stade embryonnaire et encore théorique, et soulève des problématiques d'ordre social, politique, moral et légal. La technique de décarbonation, par exemple, peut revêtir plusieurs formes : l'afforestation et la reforestation, la fertilisation de l'océan (ajouter des nutriments pour augmenter la production de phytoplanctons), ou enfin le retrait puis la séquestration du CO_2 de l'atmosphère dans des roches océaniques ou dans des cuves artificielles. Malgré les avantages que laissent entrevoir ces techniques de CCS — *Carbon Capture & Storage* —, certaines expérimentations laissent penser qu'elles pourraient représenter un risque environnemental plutôt qu'une solution, point abordé plus bas.

Parmi les outils numériques les plus importants dans la compréhension et la prévision climatiques on trouve les modèles mathématiques, nécessaires pour discerner la part due à la variabilité climatique de celle à attribuer à l'activité de l'homme. Mieux comprendre les cycles climatiques passés, permet une meilleure compréhension du climat présent et de meilleures prévisions sur le climat futur, et partant la possibilité d'organiser une meilleure adaptation au

changement climatique. Le dévoilement par le CEA en 2019[83] du super-calculateur Joliot-Curie, entièrement destiné à la recherche et destiné à être utilisé dans les domaines climatique, astrophysique, géophysique et biologique, est un indicateur qui permet de déceler les orientations prises et les efforts fournis par les centres de recherche en matière environnementale. Basé sur l'exploitation de big data provenant de bases de données climatiques, ce supercalculateur permettra très probablement d'améliorer la résolution et la finesse des prévisions.

« Citizen Science »

Au-delà de la recherche institutionnalisée émergent des initiatives de science participative *(citizen science)* associant des citoyens à la recherche, principalement biologique et écosystémique. L'objectif de cette approche, dont le développement est facilité par les NTIC et les plates-formes participatives, est d'associer davantage le citoyen à la production des savoirs, permettant ainsi d'accroître les découvertes, leur impact et leur diffusion, et d'encourager chacun à se sentir concerné : Une population plus informée et plus sensibilisée sera plus apte à répondre à un enjeu aussi complexe que le changement climatique. Parmi les bonnes pratiques à promouvoir, notons celle de la skipper Alexia Barrier (Route du Rhum 2018) : elle a équipé son bateau *4myplanet*[84] de sondes permettant de réaliser différents types de mesures (*température, salinité de l'eau)*, mises ensuite à la disposition des centres de collecte et de traitement de ce type de données[22].

Muki Haklay, professeur de '*Geographic Information Science'* au University College de Londres propose quatre niveaux de participation dans les sciences citoyennes :

Niveau de participation	Terme associé	Rôle des citoyens
Niveau 1	*Crowdsourcing*	Les citoyens contribuent comme capteurs de données (*sensors*).
Niveau 2	Intelligence distribuée	Les citoyens contribuent à l'interprétation de données.
Niveau 3	Science participative	Les citoyens contribuent à la définition du problème et à la collecte de données.
Niveau 4	Collaboration complète	La recherche est collaborative dans les différentes phases (définition des problèmes, collecte de données, analyse).

Source : Pr Muki Haklay -University College, London

Un rapport de 2016[85] sur les sciences participatives en France propose quant à lui de distinguer trois grandes classes de dispositifs : les sciences citoyennes, la Community-based research, et les sciences participatives.

83 Commissariat à l'énergie atomique et aux énergies alternatives (CEA), 'Inauguration du supercalculateur français, dédié à la recherche française et européenne, Joliot-Curie', 3 juin 2019. http://www.cea.fr/presse/Pages/actualites-communiques/ntic/inauguration-supercalculateur-Joliot-Curie.aspx

84 4myplanet, Les missions scientifiques, 21 mai 2019. https://4myplanet.org/2019/05/21/sciences-collecte-de-donnees-scientifiques-a-bord-du-monocoque-4myplanet/

85 Mission conduite à la demande du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche & du secrétariat d'état à l'enseignement supérieur et à la recherche, *'Les Sciences participatives en France : État des lieux, bonnes pratiques & recommandations'*, Février 2016

	Les sciences citoyennes	La *community based research*	Les recherches participatives
Objet	Contribution des **citoyens-amateurs à la collecte et à l'analyse** de données (scientifiques, amateurs)	Collaboration entre chercheurs et **groupes concernés** pour diagnostiquer et résoudre des problèmes qui les affectent (communautés, minorités, familles, chercheurs)	Collaboration entre chercheurs et **groupes de citoyens ou de professionnels** pour résoudre des problèmes (professionnels, utilisateurs, associations, coopératives, chercheurs, médiateurs)
Histoire	Très longue tradition de la participation des amateurs à la production des sciences naturalistes et aujourd'hui développement d'une forme de « curiosité équipée »	Tradition longue aux États-Unis, en santé publique, au Canada, en relation avec les communautés indigènes	Tradition longue dans le domaine de la recherche pour le développement. Différentes approches influencées par des traditions intellectuelles différentes (Kurt Lewin, Paolo Freire, Chambers, etc.)
Moteur	**Curiosité et volonté d'impact** aujourd'hui amplifiées par les TIC et le *crowdsourcing*	**Amélioration des conditions d'existence** ou d'exercice particulières de la communauté	**Contribution à relever des défis sociaux ou scientifiques,** soutenus parfois par de grandes organisations internationales (ex. Banque Mondiale)
Objectifs	Produire des **connaissances et indicateurs**, éduquer les citoyens aux méthodes scientifiques	Produire des **connaissances actionnables**, favoriser l'***empowerment*** (capacitation)	Produire des connaissances actionnables dans une perspective d'**innovation et de transformation sociale**
Domaines principaux	Environnement, astrophysique, biodiversité	Santé publique, éducation, travail social	Agriculture, gestion des ressources naturelles, questions urbaines
Exemples français	Vigie Nature (biodiversité)[18] L'observatoire des saisons[19] (environnement) Observations solaires[20] (astronomie)	Le Groupe de réflexion avec les Associations de malades de l'Inserm - GRAM[21] Les projets de l'ANRS en collaboration avec les associations de patients (santé)	Sélection participative[22] (agriculture) COMEPOS[23] (énergie)

Source : Ministère de l'éducation nationale, de l'Enseignement supérieur et de la Recherche

L'objectif de ces interactions entre scientifiques et citoyens est de permettre à n'importe quel individu ou communauté d'utiliser des outils scientifiques pour collecter, analyser, interpréter et utiliser les informations disponibles dans leur environnement. Ces collaborations sont des situations « gagnant-gagnant » qu'il s'agira de promouvoir dans les années à venir. La France est aujourd'hui classée 3e pays européen (derrière le Royaume-Uni et les Pays-Bas) en matière de publications scientifiques en sciences participatives. Celles-ci sont principalement issues de dispositifs liés aux domaines agricole et écologique (25 %), environnemental (17 %), des sciences sociales (11 %) et biologique (9 %).

Il est clair qu'un accent doit être mis dans les Quinze ans à venir sur l'utilisation d'outils numériques (applications, forums, plates-formes de discussions) pour améliorer cette mise en relation des différents acteurs participant ou souhaitant participer à des projets de recherche et à la diffusion au niveau géographique ou politique des données collectées.

Protection animale

Les NTIC facilitent la prise en compte par les citoyens, les professionnels et les ONG, des risques pesant sur la condition animale et des moyens d'organiser leur protection. Si ces technologies ne sont pas nouvelles, certaines émanant du domaine de la biotique sont en cours de

développement, et soulèvent des enjeux à la fois économiques et éthiques. C'est, par exemple, le cas des puces sous-cutanées de radio-identification (RFID) posées sur certains animaux de compagnie. À l'avenir, la RFID a vocation à être utilisée sur l'ensemble des animaux et à voir ses fonctionnalités multipliées. Celle de l'entreprise *Vethica*[86] contient par exemple le numéro d'identification, les coordonnées et les données médicales, ainsi que la géolocalisation des animaux, les données étant cryptées et accessibles que par le seul vétérinaire. Des travaux de recherche portent actuellement sur des puces qui seraient susceptible de relever l'état de santé complet d'un animal en temps réel, puis de reporter les informations sur une application de smartphone. Alors que les puces RFID sont aujourd'hui en vente libre sur des sites de commerce en ligne comme Amazon, une réflexion éthique et juridique s'imposeaux pouvoirs publics et les instituts de recherche, en amont du développement des fonctionnalités de ces puces. À défaut de celle-ci, une utilisation potentiellement anarchique de ces technologies par des individus, voire par des professionnels de l'élevage ou de l'agro-alimentaire, pourrait amener à une totale négation de droit à la condition animale et à une utilisation abusive de ses capacités biologiques. Sans même parler du risque d'un glissement de ces pratiques à l'être humain…

Le cyber dans quinze ans : scénario pessimiste/non souhaitable

Risques émanant d'un développement anarchique des technologies

Énergie

Dans un processus de transition énergétique, il est primordial d'identifier et d'adapter les énergies renouvelables aux spécificités du territoire où elles ont vocation à être implantées. Cette transition repose sur des études menées au préalable au cas par cas dans chacune des régions concernées. Opérer une transition sans examen préalable de la dépendance météorologique de la zone et du niveau de la demande, est une lourde erreur qui pourrait conduire à l'inefficacité des politiques menées, à un rejet par la population, ainsi qu'à une utilisation erratique du budget alloué.

À l'échelle individuelle, la gestion de l'énergie au sein du foyer (notamment avec les dispositifs de domotique) ne s'avère être une solution efficace que lorsqu'elle est encadrée et sécurisée. Le développement harmonieux de l'IoT doit en effet être considéré comme un enjeu primordial de cyber-sécurité à l'échelle de la totalité du territoire, dans la mesure où elle constitue une capacité d'irruption au sein des foyers et des services publics. Les pouvoirs publics ont ainsi le devoir d'encourager la mise en place, en parallèle du développement des technologies domestiques de gestion des flux énergétiques, des campagnes de sensibilisation et des sessions de formation de tous les consommateurs au regard des cyber-attaques potentielles qui prendraient pour cible les objets connectés de plus en plus présents dans nos foyers.

86 http://www.vethica.com/

Mobilité

Les risques principaux émanant d'un développement anarchique des nouvelles technologies de mobilité sont d'ordre à la fois socio-économique et sécuritaire. Une mobilité plus « propre » et optimisée implique des coûts plus élevés pour les consommateurs jusqu'à ce que l'installation de son infrastructure soit rentabilisée. La question de l'accès au transport public se pose alors, elle doit faire l'objet d'une prise en compte politique et juridique en amont des décisions de développement de transformation. Il s'agit non seulement de garantir une égalité d'accès aux nouvelles technologies de mobilité, mais aussi de s'assurer de la prise en compte du coût d'opportunité et des risques d'éviction qui pourraient résulter d'un développement non contrôlé de ces solutions. Sans un encadrement au départ du prix de transports publics « propres », les utilisateurs risquent de retourner vers des solutions individuelles de transport et favoriser des modes de mobilité à empreinte carbone plus importante, mais susceptibles de préserver leur pouvoir d'achat, venant ainsi annuler l'effet recherché d'une transition de la mobilité écologique.

L'autre enjeu soulevé par un développement non encadré des technologies de mobilité réside dans le partage de l'espace urbain et dans la sécurité des utilisateurs. L'exemple actuel des trottinettes électriques est significatif : leur déploiement s'est fait en amont de leur prise en charge par le droit et les politiques urbaines, provoquant une réelle anarchie sur les trottoirs, et occasionnant litiges, accidents et malaises politiques. À l'heure où les études prospectives (*américaines notamment, telles que celles de Gartner*) indiquent que dix ans à peine nous séparent de l'émergence et de la diffusion généralisée de technologies comme les voitures autonomes, la définition d'un encadrement politique et juridique préalablement à leur usage doit devenir une priorité absolue des pouvoirs publics.

Liberté, anonymat, vie privée

La préservation de l'anonymat dans l'espace public est aujourd'hui une question cruciale. Elle apparaît comme un enjeu à la fois éthique et sécuritaire et elle doit faire l'objet d'une réflexion globale des pouvoirs publics au niveau national (législation, validation constitutionnelle) et local. À l'ère du RGPD et d'un encadrement renforcé de la récolte, de la diffusion et de l'utilisation des données personnelles, certains dispositifs intelligents mis en place au cœur des villes peuvent voir leur légalité contestée. Des villes de plus en plus surveillées, quadrillées, qui suivraient le modèle de science-fiction de *Minority Repor*t ou, encore, l'exemple bien réel des métropoles chinoises, constituent des modèles aisément contestables. Elles pourraient alimenter un débat croissant sur le niveau juste et raisonnable de liberté à sacrifier afin de garantir une meilleure sécurité et une optimisation de l'espace public. Le concept même de *smart city* suppose le déploiement d'outils permettant de recueillir des données de terrain, mais également des données personnelles. La première question à prendre en compte est donc de savoir quel acteur de confiance, *privé ou public, national ou local*, sera chargé de

cette récolte et du stockage des données. Le second enjeu réside dans la sécurisation de ces données et leur utilisation. Sans directive claire donnée par le Conseil constitutionnel ou par un organisme national *ad hoc*, l'utilisation des données personnelles dans le cadre de la ville intelligente pourrait amener à différentes dérives : surveillance abusive des citoyens, ségrégation, délation, revente de données personnelles à des fins commerciales, spéculation immobilière, voire exposition accrue à des menaces sécuritaires personnelles ou professionnelles dans le cas où les données seraient interceptées[87].

Environnement

L'utilisation d'outils numériques dans le cadre de l'*IT for Green* ne saurait être bénéfique si l'on ne prend pas en considération les dérives potentielles liées au phénomène de pollution numérique, qui peut revêtir deux formes distinctes : la pollution liée à la production et au recyclage des composants physiques des outils numériques, et celle due à l'utilisation de ces derniers. Les matériaux utilisés pour la production des composants électroniques qui constituent le cœur des technologies numériques que nous utilisons (smartphones, ordinateurs, puces électroniques), sont pour l'essentiel des « terres rares » extraites de mines à ciel ouvert, principalement en Chine et en République démocratique du Congo. Les conséquences environnementales (appauvrissement des sols, transports, rejets toxiques) et humanitaires de l'exploitation de ces ressources telle qu'elle est faite aujourd'hui, sont insoutenables à longue échéance.

Sans la mise en place et l'application d'une réglementation internationale efficace conditionnant l'extraction et le commerce de ces ressources, doublée d'une exigence de traçabilité forte, nos modes de consommation actuels des technologies numériques se traduiront par une multiplication des crimes contre l'environnement et contre l'humanité, ce que soulignent déjà certaines ONG comme Amnesty International ou Oxfam.

Au-delà de la prise en charge politique et juridique de ce problème, des technologies alternatives et une industrie du recyclage pourraient constituer de réelles solutions. À titre d'exemple, mentionnons dans le domaine des smartphones :

- l'**initiative Phonebloks**[88], créée par Dave Hakkens aux Pays-Bas : c'est un concept de smartphone modulaire, avec comme objectif la réduction des déchets électroniques ;
- le concept d'**Urban Mining**, développé par l'ONG Green Urban mining, qui rachète aux consommateurs et ONG du monde entier des appareils électroniques usagés pour les reconditionner et les revendre[89];

87 « La cybersécurité : une priorité pour les collectivités territoriales », *Cybersécurité et Politiques publiques,* 1er trimestre 2019, https://cybercercle.com/wp-content/uploads/2019/02/cs2p_n2_1T2019_collectivites_bdef.pdf

88 Liens vers le site officiel de l'entreprise : https://phonebloks.com.

89 Fondée en 2010 par Juan Carlos Villatoro, Green Urban Mining est une entreprise basée en Floride spécialiste du recyclage des appareils électroniques, dans une approche durable. Plus de détails sur : http://www.urmining.com/about-us/our-story/

— l'**initiative FairPhone**[90] de fabricants néerlandais, qui cherchent à intégrer des critères et exigences équitables au processus de production des téléphones, en collaboration avec des ONG et des acteurs de la grande distribution.

Autre aspect majeur de la pollution numérique, le stockage gigantesque des données dans les *data centers* et la consommation d'énergie qui en résulte, supposent une réelle réflexion des pouvoirs publics ainsi qu'une profonde sensibilisation des entreprises et des citoyens. Des gestes simples, mais répétés de manière systématique et généralisée comme le nettoyage systématique par chacun de ses boites mails, spams et newletters (CleanFox ; Newmanity) devraient permettre de réduire de manière significative la pollution numérique liée au stockage des données.

Dans le domaine de la géoingénierie, la permanence d'incertitudes fortes liées à l'imprévisibilité des conditions climatiques, ainsi que les questions de gouvernance ou de juste échelle d'implémentation, empêchent un développement optimal des capacités offertes par ces technologies au sein des instituts de recherche. En outre, une promotion de la géoingénierie qui serait présentée comme la science permettant de dépolluer l'atmosphère par le retrait des particules de CO_2 (au lieu de viser une mitigation globale) et l'ignorance actuelle des implications d'une telle démarche, pourrait bien conduire à une réelle déresponsabilisation des pollueurs.

Enfin, la mise en place de tous ces processus sans implication suffisante des populations, aggravée par un cloisonnement entre les nations, risquerait d'entraîner un rejet de la part des citoyens et consommateurs, incapables de mesurer l'impact de solutions technologiques qui ne seraient pas appliquées à l'échelle mondiale.

Recherche scientifique et technique

Les différentes personnalités du monde de la recherche interrogées dans le cadre de l'étude ont fait état des difficultés croissantes pour accéder à l'utilisation à des fins scientifiques d'outils à forte composante numérique comme les satellites d'observation, les modèles climatiques, les sondes hydriques, etc. Cela vient notamment du coût extrêmement élevé de l'accès à ces technologies, qui supposent des moyens financiers propres très importants, et soulignent le besoin d'une augmentation constante des subventions d'État allouées au monde de la recherche.

Dans le contexte actuel d'incertitude climatique, ne baser des décisions politiques ou une gouvernance de la transition écologique que sur des modèles et des modes de calcul fondés

90 Voir notamment : « Fairphone 2 : le retour du smartphone équitable », par Romain Thuret, sur lesnumériques.com, 16.06.15 ; « Taking Back Phones for a Circular Economy: E-waste in Ghana », sur le blog de Fairphone, de Bibi Bleekemolen, le 21.11.13 ; et « Tech5: Fairphone named Europe's fastest-growing startup of 2015 » de Jelle van Wijhe, publié sur le site de The Next Web, le 29.04.14.

sur les seuls B*ig data*, constituerait un risque majeur auquel sont confrontés les scientifiques aujourd'hui, la variabilité des données de masse pouvant fausser mesures et prévisions. Ces obstacles techniques se combinent en outre à une volonté politique bien trop faible de la communauté internationale, qui laisse les représentants des pays les plus pollueurs, et bien souvent les plus puissants, refuser de s'engager dans de tels protocoles d'intérêt global (accords de Paris, COP22, etc.).

Du protectionnisme numérique à la brutalisation du cyber-espace

Au niveau mondial, l'attention devra se fixer en priorité sur :

- les menaces cyber pesant sur les États et les OIV[91], FSE et OSN :
  - menaces étatiques (à portée économique, politique, géostratégique),
  - menaces terroristes (à portée politique, symbolique, idéologique),
  - menaces économiques (espionnage, sabotage, intelligence économique, crime organisé) ;
- les menaces cyber pesant sur le monde de l'entreprise ;
- les menaces cyber pesant sur les citoyens et les ménages ;
- les ingérences extérieures dans le processus démocratique et les risques de surveillance ;
- les conflits dans le cyber (aux différentes couches, de la couche physique à la couche applicative) ;
- le blocage des instances de régulation internationales ;
- les tentatives de repli et d'isolationnisme numérique, à l'encontre de l'idéal originel de « village global ».

Les risques à envisager plus spécifiquement du côté de l'Union européenne sont :

- l'exposition accrue de certains États (d'Europe de l'est notamment) à des attaques cyber ;
- la demande d'un transfert total de la compétence en matière de cyber à la Commission européenne au détriment de la souveraineté des États, qui provoquerait un rejet intense de l'UE ;
- la mise en commun des technologies, qui pourrait conduire à une perte d'avantage stratégique pour les nations les plus avancées ;
- un renforcement des frontières économiques de l'UE, qui risquerait d'accroître les tensions avec les États hors de l'espace régional européen (Russie, Chine, États-Unis) ;
- une harmonisation difficile, voire une concurrence entre l'ENISA et les organes cyber nationaux (ANSSI, CNIL, etc).

91 Thèse de Danilo D'Elia, *La cybersécurité des opérateurs d'importance vitale : analyse géopolitique des enjeux et des rivalités de la coopération public-privé,* Soutenue le 07-12-2017à Paris 8 , dans le cadre de École doctorale Sciences sociales (Saint-Denis, Seine-Saint-Denis), http://www.theses.fr/2017PA080136

Une proposition d'indicateurs de vulnérabilité cyber

INDICATEURS QUANTITATIFS	INDICATEURS QUALITATIFS
- dépenses liées à la défense cyber en France (budget MDA), ou niveau des moyens humains dédiés. - nombre d'entités considérées comme « terroristes » et ayant recours à des outils informatiques pour leur promotion, leurs menaces, ou comme mode d'action. - nombre d'États ayant été la cible d'attaques cyber. - nombre d'États à qui ont été imputées des attaques cyber. - nombre d'appareils connectés susceptibles de devenir des cibles ou des vecteurs d'attaques. - nombres d'OIV. - nombre de vétos déposés au CS de l'ONU sur le cyber.	- degré de numérisation des forces armées françaises (LIO et LID), européenne et internationales. - classification des entités considérées comme terroristes selon leur dangerosité, leur visibilité et leur capacité de recrutement via le cyber-espace. - classification des doctrines de défense des États ou Alliances d'États au regard de la menace cyber : réplique cyber ? conventionnelle ? défense nationale ou collective ? - évolution des mesures de protection auxquelles sont soumis les OIV

Chapitre X

Que faire à court terme ?

Les populations vulnérables

Au même titre que les grandes entreprises et les administrations centrales ou régionales, les ETI, PME/PMI, les collectivités territoriales de petite taille réparties sur tout le territoire ou hors métropole, sont soumises au risque de voir leurs systèmes informatiques détournés, espionnés voire sabotés, même si les modes d'attaque, les sources de menaces et les impacts se déclinent et n'appellent pas les mêmes réponses pour des raisons évidentes de taille, d'organisation et de ressources.

Or si l'impact d'un incident de cyber-sécurité sur l'un de ces acteurs de petite taille peut en général être considéré comme mineur vis-à-vis de l'économie globale, du patrimoine industriel et des services publics vitaux de la nation, le nombre très important de ces petits acteurs, la vulnérabilité de leurs systèmes informatiques et leur faible résilience aux attaques, font qu'aujourd'hui la plus forte probabilité de cyber-attaque vise ce tissu fragmenté et hétérogène, qui représente en fin de compte l'essentiel des parties prenantes du cyber-espace comme du tissu économique et social de la France.

Qu'elles soient intégrées dans des démarches sans contrôle d'intelligence économique extrême, d'espionnage privé ou étatique, d'activité mafieuse, de terrorisme ou de cyber-guerre, les cyber-attaques sont majoritairement automatisées et exploitent les vulnérabilités des systèmes connectés à l'Internet, en dépit de toutes les bonnes pratiques. Dans le cas de PME/PMI (encore plus pour des ETI), si leurs informations, leur capacité financière, ou leur activité industrielle et commerciale peuvent représenter une valeur importante pour leurs concurrents ou pour des organisations criminelles, les attaques peuvent devenir ciblées (sans être forcément sophistiquées) et impacter lourdement ces petits acteurs, au point parfois d'hypothéquer leur survie. Si, depuis les années 1990, des milliers de PME/PMI/ETI n'ont pu résister ou se développer, du fait de leur impréparation à faire face à l'hyper compétitivité globalisée ou à protéger leur information stratégique, le phénomène s'est encore plus accentué avec l'hyperconnexion des systèmes et la montée en puissance de nouvelles sources de menaces, non seulement économiques mais aussi mafieuses, idéologiques et militaires.

Pour ces « nouveaux entrants », les PME/PMI, les collectivités territoriales et les particuliers représentent un objectif global majeur, même si elles ne représentent individuellement qu'un faible intérêt au plan économique. Aujourd'hui les cyber-attaques massives ne ciblent plus ces acteurs pour leurs biens propres, mais pour contrôler l'énorme volume de nœuds internet et d'ordinateurs qu'elles opèrent en toute ignorance d'une prise de contrôle extérieure discrète. Si les attaques virales représentent la partie visible de l'iceberg, la partie cachée est constituée de réseaux d'ordinateurs zombis (botnet) qui fabriquent de l'argent numérique (en « minant du bitcoin »), espionnent ou influencent les pratiques numériques des utilisateurs (spyware, adware, climat social, élections…), relaient massivement des courriels publicitaires ou des logiciels malveillants (spam), déclenchent des attaques massives coordonnées (DDOS) ou encore référencent des milliers de vulnérabilités exploitables et pré-positionnent leurs troupes cyber pour des cyber-attaques ultérieures qui pourraient paralyser les infrastructures vitales de territoires entiers.

Ce constat est familier aux stratèges « cyber » des armées, des mafias, des pirates, des professionnels de la cyber-sécurité. Mais, bien que médiatisé de plus en plus auprès du grand public grâce au cinéma et à la presse spécialisée, il demeure curieusement ignoré de la plupart des centaines de milliers d'entreprises et d'administrations qui ne protègent que rarement, et avec une efficacité toute relative, leurs systèmes et leurs informations — exposant ainsi non seulement leurs ressources propres déjà fragiles, mais aussi et surtout le maillage numérique collectif du territoire national.

Face à ce risque de perte de souveraineté numérique dû au morcellement et au volume de ces acteurs, il est difficile pour les organes centraux publics ou privés, pour les prestataires de service experts, mais en sous-nombre, d'agir efficacement au plus près des territoires, de prendre en compte les spécificités métiers et opérationnelles propres à chaque acteur et de mobiliser à un coût supportable les ressources nécessaires pour faire face à d'aussi gros volumes. *A contrario*, les acteurs de petite taille ne mobiliseront jamais les faibles moyens dont ils disposent pour se conformer à de nouvelles contraintes normatives ou juridiques, ou pour prêter attention à un discours complexe qui ne correspond ni à leur niveau d'expertise ni à leurs préoccupations opérationnelles.

Comment donc répondre au besoin de sensibiliser de manière pertinente, efficace et à coût faible les dirigeants de ces petites organisations afin qu'elles prennent conscience du danger, mobilisent leurs ressources internes et fassent appel à des partenaires sur ce défi supplémentaire de la cyber-sécurité ? Sans une compréhension par chaque acteur des enjeux de son périmètre, sans solutions simples de sécurité, jamais les risques directs (pour ne pas parler des indirects) ne pourront être abordés concrètement au niveau local, bien que devenant de plus en plus critiques au niveau national consolidé.

Déploiement d'un programme de sensibilisation

Les actions de sensibilisation aux risques et à la sécurité numérique doivent donc cibler en priorité les acteurs les plus fragiles de par leur taille, leurs ressources, leur secteur d'activité, leur éloignement des prescripteurs et conseils, privés ou publics. Ces petits acteurs constituent l'essentiel des besoins d'accompagnement, mais sont aujourd'hui difficilement couverts du fait de leur nombre, de leur fractionnement et de l'exigence de pragmatisme dans l'analyse de leur modèle de fonctionnement comme dans les conseils à leur délivrer. Ils concentrent des difficultés que les prescripteurs n'ont en général pas capacité à résoudre, soit parce qu'ils ne sont pas présents dans les territoires, soit parce que leurs relais locaux qui traitent avec ces acteurs ne sont pas assez informés des enjeux stratégiques, du type d'accompagnement souhaitable, ou suffisamment formés aux supports méthodologiques.

Petites entreprises

Dans un premier temps, la cible prioritaire devra donc être constituée des petites entreprises abordées en fonction de leur taille (TPE, PME/PMI, ETI) et de leurs enjeux de sécurité numérique : données métiers ou à caractère personnel, systèmes critiques, objets connectés vulnérables, fonctions métiers impactées par les risques numériques.

- PME dont le cœur d'activité repose sur le traitement des données (dont celles à caractère personnel) ;
- PMI dont la performance dépend de systèmes connectés ou du développement d'objets connectés ;
- entreprises de taille intermédiaire ayant des fonctions (DAF, IT, Juridique…) exposées au risque cyber.

Jeunesse

Les administrations territoriales et les jeunes devraient ensuite être ciblés en profitant des actions récurrentes organisées par les associations régionales IHEDN (formation de conseillers défense, séminaires d'élus, conférences et par les trinômes académiques (auprès des étudiants, enseignants et collégiens, ou dans le cadre du Service national universel).

Territoires

(administrations territoriales et décentralisées, élus, conseillers défense)

La prise de conscience des principales menaces cyber et une initiation aux bonnes pratiques de sécurité constituent les fondamentaux à intégrer. Les organismes de moins de dix personnes (TPE, collectivités) concentrent le management stratégique, opérationnel et technique sur deux

ou trois personnes qui doivent réduire leur exposition aux principaux risques. Ce socle commun doit être complété pour les PME de méthodes et outils leur permettant de protéger leurs données sensibles, leur informatique de gestion (IT), et de répondre aux exigences légales et de leurs clients.

Les PMI qui dépendent aussi de l'informatique pour leurs infrastructures, leurs produits et services connectés (IoT, OT production, logistique, santé…) doivent en assurer l'intégrité et la haute disponibilité, ce qui nécessite des compétences supplémentaires (développement & tests, exploitation, plans de reprise). Les organismes de taille intermédiaire (ETI, collectivités) et au-delà peuvent assigner ces différentes expertises à plusieurs responsables métier et fonctions support, pour aborder la notion de risque et spécialiser les mesures de sécurité (informatique, sûreté, juridique, humaine).

La France des territoires hors Paris, celle des TPE/PME/PMI, celle des petites et moyennes collectivités territoriales, celle des jeunes, toutes ces « France » sont peu ou mal informées des risques croissants et polymorphes de la cyber-sécurité et des impacts de la guerre *de facto* quoique non déclarée dans le cyber-espace, et constituent donc des populations vulnérables. Les 3,1 millions de TPE-PME représentent l'immense majorité des entreprises en France (99,8 %). Elles réalisent 1 300 milliards d'euros de chiffre d'affaires annuel (36 % du total français) et 44 % de la valeur ajoutée du tissu productif français. 360 000 d'entre elles (11,7 % du total) sont des entreprises exportatrices. Elles pèsent au total pour 49 % de l'emploi salarié en France (55 % d'entreprises individuelles inclues)[92].

Or, en France, la seule sensibilisation d'ampleur nationale et territoriale, quoique non contraignante — à l'opposé des chinois —, a été, depuis février 2018, le « *Tour de France de la cyber-sécurité* » organisé par CCI France et le CyberCercle. Afin de pouvoir répondre à toutes ces menaces et contraintes normatives, on pourrait commencer par élaborer un dispositif de sensibilisation de *tous* les territoires et d'un maximum d'écosystèmes, en s'appuyant sur des kits d'introduction à la cyber-sécurité, issus par exemple du dispositif cyber-malveillance[93]. En s'inspirant du succès marqué des *trinômes académiques* et en adéquation avec les nouveaux tryptiques ANSSI-Comcyber-gendarmerie, le dispositif de déploiement national de « sensibilisation à votre cyber-sécurité » pourrait:

- s'appuyer sur les organisations professionnelles françaises et autres dispositifs territoriaux, pour répondre à l'enjeu de sécurité nationale ;
- s'inspirer des « retex[94] » des 700 PME membres du dispositif national cyber-malveillance dans leur croisade de remédiation sur tout le territoire ;
- s'articuler autour d'auditeurs IHEDN référents bénévoles dans le cadre du projet CYBUNIH ;
- réaliser un pilote terrain pendant six mois sur plusieurs territoires.

92 INSEE, Les Entreprises en France 2014 (données 2011), étude Ipsos pour Randstad (données 2016) & Revue de la gendarmerie nationale (Aavril 2019 / N° 264)

93 https://www.cybermalveillance.gouv.fr

94 Retour d'expérience.

Il existe aujourd'hui en France trois types de réseaux professionnels pertinents pour répondre à ces objectifs :

- les réseaux structurés et représentatifs officiels, nationaux ou territoriaux, mobilisables pour leur connaissance du tissu PME/PMI/TPE/indépendants/artisans/commerçants ;
- les ordres professionnels qui véhiculent des données très sensibles pour la collectivité et qui mobilisent d'autant plus facilement et régulièrement leurs troupes que leurs contraintes normatives vont croissant ;
- les grandes entreprises et organisations, privées ou publiques, en soutien logistique et donneurs d'ordres ou référents de leurs écosystèmes.

Parmi eux, plusieurs têtes de réseau sont immédiatement pertinentes pour nos cibles, en sensibilisant ou en formant des formateurs, et peuvent toucher potentiellement un million d'entreprises TPME/PMI que ce soit en présentiel ou en webinar :

- la confédération CPME, ses 13 délégations régionales et 104 départementales regroupent, sensibilisent et forment chaque mois des centaines de TPE / PME / PMI ;
- le syndicat CINOV Numérique et les 15 chambres régionales de la fédération CINOV (cofondatrice de la CPME), qui ont organisé un Tour de France de la Transformation Numérique (20 territoires en 2019, autant sur 2020/2021) ;
- CCI France constitue un maillage de 126 établissements publics nationaux, régionaux et locaux, à travers lesquels elle a déployé un « Tour de France de la cyber-sécurité » au côté du CyberCercle :
- le réseau des Chambres de métiers et de l'artisanat, qui regroupe 93 établissements publics de l'État et constitue un potentiel lourd avec un million de personnes reçues, 225 000 porteurs de projets accueillis et 120 000 stagiaires en formation continue :
  - 1 établissement national : l'Assemblée permanente des chambres de métiers et de l'artisanat (APCMA),
  - 13 établissements d'échelon régional dans l'Hexagone + cinq outre-mer,
  - 74 établissements d'échelon départemental ;
- le Groupement des industries de construction et activités navales (Gican) constitue un excellent pilote proche de nos préoccupations, de même que le GIFAS (Groupement des industries françaises aéronautiques et spatiales) et le GICAT (Groupement des industries françaises de défense et de sécurité terrestres et aéroterrestres), mais leur tissu de PME/PMI reste à consolider ;
- la fédération des centres de gestion agréés (FCGA) réunit une centaine de centres AGA et CGA, en relation de confiance plusieurs fois par an avec plus de 300 000 entreprises, dont 92 % de TPE sur tout le territoire.

Les principaux ordres professionnels (avocats, architectes via leur organisme de formation GEPA), leurs syndicats et organismes de formation attachés, sont également pertinents par les contraintes qu'ils imposent à leur écosystème et, par-delà, à leurs millions de clients, notamment dans le cadre des données qu'ils partagent avec les parties prenantes.

Les réseaux de grandes entreprises pourraient héberger gracieusement certaines séances de sensibilisation, venant en complément des organismes professionnels représentatifs. Cette démarche volontariste de grands groupes serait bénéfique pour leur image auprès de leur écosystème de fournisseurs et de TPME sur leur territoire, et leur permettrait d'assumer leur positionnement de têtes de filière, à l'instar du mode opératoire de Vivatech, le Las Vegas français des grands clients de Publicis. Citons aussi le Cigref, dont les membres forment collectivement un excellent maillage territorial tout à fait pertinent sur le domaine cyber, et qui pourrait rassurer les TPME et autres indépendants de leur écosystème.

Un autre réseau très pertinent car mutualiste (solidarité, confiance), est celui du Crédit Mutuel CIC, quatrième réseau bancaire français, cinquième opérateur de réseau mobile et premier MVNO. Reconnu pour son orientation « gestion de l'information », il est lui-même réseau de PME et de proximité de facto et, donc, très orienté clientèle PME/PMI et commerçants sur tout le territoire.

Dernier moyen incontournable depuis 2017, le dispositif national cyber-malveillance, porté par le Groupement d'Intérêt public ACYMA. Le label ExpertCyber a été lancé en mai 2020 dans l'esprit de celui de l'ANSSI, à destination des TPE/PME/PMI membres de sa plate-forme. Les futurs labellisés seront, de ce fait, bien positionnés aussi pour accompagner un déploiement territorial de sensibilisation.

Identification des compétences cyber

Dans le milieu cyber, contrairement à la plupart des environnements classiques, les compétences ont une date de fraîcheur, une durée de vie limitée qui nécessite une mise à niveau permanente sur les nouvelles technologies de l'information : alors que la durée de vie générale d'une compétence technique est aujourd'hui de cinq ans (contre trente dans les années 1980)[95], elle descend entre douze et dix-huit mois dans l'environnement cyber. Notons d'ailleurs que les technologies utilisées correspondent de plus en plus à des champs transverses comme l'informatique, la théorie de l'ordonnancement, l'intelligence artificielle, etc. Il est donc nécessaire d'avoir une capacité de raisonnement particulièrement flexible, pour pouvoir travailler efficacement dans un environnement cyber qui doit être adapté à la fois aux besoins actuels et aux évolutions futures, sachant, par ailleurs, que le taux de renouvellement de ces technologies et de ces concepts est élevé.

95 https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/human-capital/ca-FR-HC-The-Intelligence-Revolution-FINAL-AODA.pdf – Deloitte - *La révolution de l'intelligence Préparer l'avenir de la main-d'œuvre canadienne*

Source : Cap Gemini – Digital Mastery 2019

Par le biais d'Internet, la technologie des systèmes d'information a permis de voir émerger des professionnels disposant des compétences adéquates et d'un savoir opérationnel pointu, sans qu'ils soient forcément issus des cursus traditionnels français comme l'université ou les Écoles d'ingénieurs. Ces individus sont d'autant plus intéressants qu'ils évoluent souvent *out of the box*, en rupture avec la pensée traditionnelle en matière de S.I., ce qui facilite les évolutions nécessaires dans un contexte de concurrence internationale féroce.

Partant de ces constats, il semble opportun de disposer d'une nouvelle approche pour identifier chez nous les talents et les individus disposant des compétences utiles et nécessaires au maintien et à l'évolution du marché cyber en France, de préférence avant que les milieux internationaux ne le fassent. C'est d'autant plus approprié qu'un manque flagrant de compétences est actuellement observé sur le marché cyber en France, au moment même où les PME commencent à chercher du personnel qualifié, face aux nouvelles menaces qui les épargnaient jusqu'à présent.

Des dispositifs existent actuellement pour aider à identifier ceux qui disposent déjà de compétences avérées dans le domaine (ex : Hackathon). Il semble donc opportun de cibler ceux qui ne sont pas encore identifiés actuellement. Pour ce faire, il serait souhaitable d'identifier dès le plus jeune âge, dans l'enseignement secondaire et sans doute jusqu'à l'enseignement supérieur, les jeunes talents disposant de facilités naturelles dans le domaine cyber. Il est très souhaitable que les intervenants face à eux disposent de compétences réelles et suffisamment récentes pour pouvoir répondre comme il faut à un public jeune, dont le niveau de compétence moyen est parfois supérieur au leur…

Il serait sans doute aussi très prometteur de rajouter une composante de « test cyber » à la *Journée défense et citoyenneté.* On pourrait ainsi identifier les jeunes ayant des facilités

notables dans ce domaine et leur proposer un cursus adapté.[96] Le service national universel (SNU), bien qu'encore balbutiant et sujet à évolution, nous semble une excellente occasion de donner une touche cyber à un maximum de jeunes dans un minimum de temps et à moindre coût. En plus d'un test cyber quasi-systématique pour mieux identifier les talents spécifiques, on pourrait prévoir une à deux demi-journées de formation cyber-sécurité pour tous.

Au-delà de cette identification, il est également nécessaire d'accompagner ceux qui doivent entretenir leur compétence cyber. Cette formation continue, bien que souvent laissée au second plan dans le milieu professionnel, est absolument cruciale vu la vitesse d'évolution des technologies et les menaces afférentes. Notons l'adéquation des MOOC à cette finalité, en particulier celui de l'ANSSI : *SecNumacadémie*[97]. Tout à fait adapté, il fournit une attestation avec durée de validité. Ce type de formation pourrait avoir un caractère validant dans le cadre de cursus d'études secondaires ou supérieures (unités, crédits) pour encourager l'attractivité de ces compétences et propager l'intérêt pour le cyber- au sein de la communauté étudiante.

Un des éléments majeurs de rétention des compétences cyber dans les entreprises françaises, est la sensation de liberté et l'épanouissement professionnel : *« Ça n'a pas de sens d'embaucher des gens intelligents puis de leur dire quoi faire. Nous embauchons des gens intelligents afin qu'ils puissent nous dire ce qu'il faut faire » (Steve Jobs).* Il faut donc encourager dans les entreprises une plus grande flexibilité pour ceux qui ont des compétences cyber reconnues, par exemple que:

- leur accès aux conférences et formations adaptées soit encouragé ;
- les formations MOOC soient reconnues et plus faciles d'accès (pas de contraintes d'horaires et/ou de dates, avec évaluation automatique et instantanée, capacité à repasser les examens), tout en maintenant une simplicité d'inscription pour un coût faible à nul ;
- un temps régulier et conséquent en auto-formation soit prévu dès la définition du poste à pourvoir.

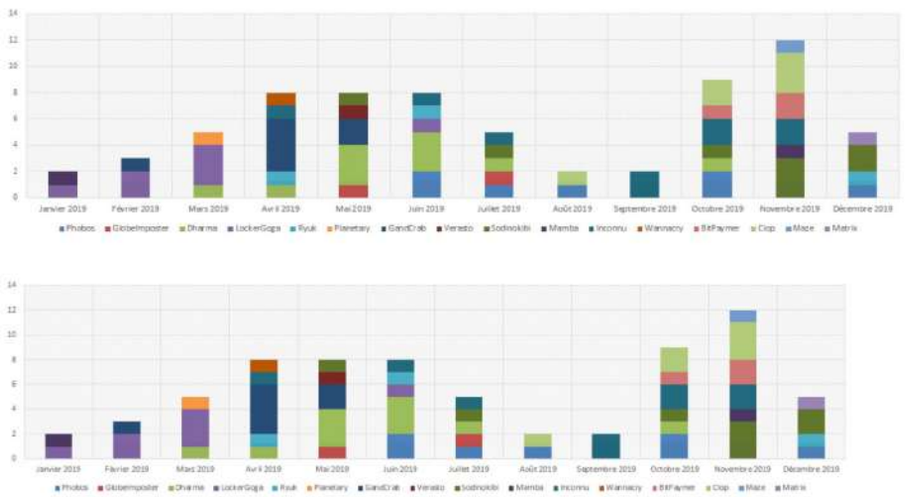
Dans cette logique, l'identification des intervenants pourrait cibler le vivier institutionnel (autorités), les professionnels extérieurs et bien entendu les auditeurs IHEDN, ces intervenants pouvant être classés selon le public visé :

- compétences générales (capable d'évoquer les grandes lignes) ;
- compétences approfondies (capable de répondre à un public averti) ;
- compétences d'expert (capable de répondre à un public d'experts).

Heureusement, peu d'entre nous ont été victimes de cyber-attaques, ou en tout cas en sont conscients. On dit souvent qu'il n'y a que deux catégories d'entreprises : celles qui ont subi une attaque de leur système d'information et celles qui ne savent pas qu'elles en ont été la cible.

96 De manière plus générale, ce test permettrait également d'identifier les personnes éprouvant des difficultés dans le domaine plus général de l'informatique, afin de leur proposer une adaptation de leur cursus, afin de réduire les risques d'exclusion du monde professionnel.

97 https://secnumacademie.gouv.fr/



Incidents rançongiciels traités par l'ANSSI en 2019

Source : ANSSI - ÉTAT DE LA MENACE RANÇONGICIEL[98]

NB : On consultera avec intérêt sur le site cybermalveillance.gouv.fr le parcours des victimes TPME/particuliers entre février et avril 2020 (hors arnaques au chantage webcam) qui sont devenues exponentielles entre le 8 et le 25 avril.

Plaisanterie mise à part, les media grand public estiment que 100 millions d'internautes européens ont été victimes d'une attaque cyber en 2018, estimation anxiogène qui amène le nombre de personnes touchées à ⅓ de la population. Ce chiffre englobe les multiples atteintes aux smartphones et aux objets connectés, qui se chiffrent en centaines de milliers de victimes à chaque occurrence. En France en 2017, plus de 19 millions de personnes auraient subi les conséquences d'actes de cyber-criminalité, soit 42 % de la population adulte en ligne. Les pertes financières atteindraient 6,1 milliards d'euros au cours des 12 derniers mois dans le seul Hexagone, chaque victime ayant par ailleurs perdu en moyenne 16 heures (soit deux jours ouvrés) pour réparer les dommages causés[99].

Toutefois, au niveau d'une association régionale IHEDN comme l'AR14 (région lyonnaise), deux « appels au secours » seulement sur près de 400 membres ont été reçus durant l'année passée. Nos pirates nationaux eux aussi sont assez peu actifs… ou peu doués pour masquer leur origine : seules 5 % des attaques informatiques étudiées à l'échelle mondiale proviennent d'adresses IP situées en France. L'Hexagone se positionne ainsi au 4e rang des pays d'origine présumés des cyber-attaques, dont le plus grand nombre serait initié depuis les États-Unis (22 %) et la Chine (13 %). Il reste que tout attaquant, comme tout internaute lambda, peut utiliser un VPN ou d'autres technologies pour brouiller les pistes[100]…

98 https://secnumacademie.gouv.fr/

99 Source : FIC 2019, étude Kaspersky - un éditeur de logiciels de protection subséquemment intéressé à publier les plus hauts chiffres possibles

100 Source : www.silicon.fr, 6 mai 2019

Au-delà de la statistique, ce qui nous intéresse ici c'est l'aspect psychologique de la chose. Qu'il s'agisse de particuliers ou d'entreprises, le contenu numérique a pris une telle importance dans l'esprit des gens que l'intrusion dans un système de données est vécue comme un véritable viol (carnets d'adresses personnels, photos, vidéos et accès aux courriels répandus sur la place publique pour les particuliers victimes). L'intimité numérique de la victime a été pénétrée, salie, volée, parfois diffusée à tort et à travers. De même, pour les données commerciales, comptables, financières ou RH d'organisations, qui les retrouvent bradées sur le *dark web* avec perte de réputation. Un viol donc — crime de lèse identité et de mise à jour du secret des affaires — d'autant plus mal vécu que la plupart du temps la victime ne sait pas vers qui se tourner pour nettoyer son système et éventuellement récupérer l'intégrité de ses données. Et pour couronner le tout, la loi vient maintenant sanctionner durement l'insuffisance de protection de données personnelles en cas de fuite.

Les grandes entreprises sont équipées humainement et techniquement pour limiter le risque cyber et réagir aussi vite que possible à tout type d'attaque. Les particuliers et les PME/ETI sont en revanche particulièrement démunis, puisque la sécurité représente un coût et que, comme l'assurance, elle est souvent jugée trop chère… jusqu'à la survenue du sinistre. D'où l'idée d'un SVP cyber, « guichet unique » d'aide aux victimes : ce serait un lieu où tout un chacun, particulier ou entreprise, pourrait trouver conseil, aide et soutien, mais aussi être aiguillé vers des prestataires de proximité susceptibles de l'aider à recouvrer sa santé numérique. On contribuerait ainsi à la résilience informatique de nos concitoyens et à celle de nos organisations nationales.

Une grande partie des fonctions souhaitables d'un SVP cyber existe déjà aujourd'hui dans le dispositif gouvernemental cyber-malveillance d'assistance aux victimes de telles agressions, accessible sans frais ni inscription sur le site internet cybermalveillance.gouv.fr. interministériel sous la houlette du Premier ministre et du SGDSN, ouvert à tous publics, professionnels comme particuliers, il offre ses services d'information, de conseil et d'aide aux victimes dans un esprit d'assistance et de prévention du risque numérique. On doit le faire connaître au plus grand nombre, en particulier du fait de sa légitimité. Toutefois, nos différentes expériences nous poussent à suggérer un élargissement de ses compétences, voire la mise en place d'une structure complémentaire, mieux adaptée pour synchroniser les efforts et visant à mettre en place une réelle solution de guichet unique simple, qui apporterait des réponses systématiques et rapides aux usagers. Du fait de leur activité personnelle ou professionnelle, plusieurs membres de la commission cyber-stratégie de l'Union-IHEDN ont en effet eu l'occasion, pour leur compte ou pour celui de clients, d'utiliser la plate-forme cyber-malveillance actuelle. Ces expériences de terrain ont été révélatrices de différents points sujets à améliorations, en particulier :

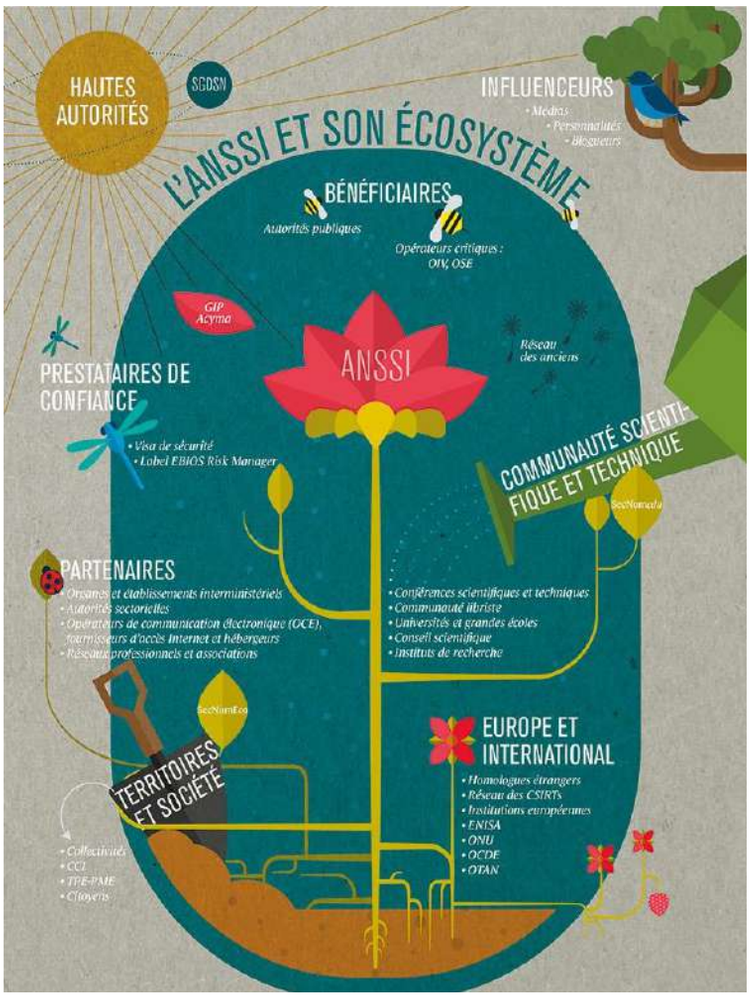
— **Effet ping-pong :** certaines attaques subies ont été soumises à la plate-forme, qui a traité la requête en la réorientant vers la CNIL ou la gendarmerie. Bien que ce type de réponse fasse sens, la nature souvent complexe des attaques subies a engendré un rejet de responsabilité entre les différents intervenants. Un exemple concret : le phishing sur une adresse mail ayant été traité par renvoi à l'ANSSI, celle-ci l'a considéré comme du spam et a donc

recommandé le transfert de la requête vers la CNIL, qui l'a traité comme une tentative d'arnaque et bouclé la boucle en recommandant un dépôt de plainte à la gendarmerie. L'incident s'est conclu au bout de quelques jours par un abandon pur et simple de la démarche, pour cause de lassitude de l'entreprise visée.

- **la non-réponse à un signalement :** plusieurs cas de hacking (cryptolocker) ont été signalés à la plate-forme, sans qu'une réponse particulière ait été émise. Bien qu'il soit souvent complexe, voire impossible de traiter de tels sujets, l'absence totale de réponse après une déclaration de la victime auprès de la plate-forme a eu pour effet une mauvaise perception de cette dernière, et donc son rejet par l'utilisateur.
- **le suivi des dossiers :** certaines entreprises ayant cherché à s'inscrire sur la plate-forme comme fournisseur de solutions se sont vues refuser le référencement, sans réponse claire ni motivée. Bien qu'ayant demandé des compléments d'information, puis ayant essayé de relancer le dossier par l'intermédiaire de l'interface en ligne prévue à cet effet, aucune réponse ne leur a été faite. Ces entreprises ont donc abandonné l'idée d'utiliser cette plate-forme. Même réaction chez une victime qui aura fourni ses informations de signalement à la plate-forme sans en recevoir un quelconque feedback à part un éventuel numéro d'ordre…

Pour être honnête, précisons quand-même que ces remarques concernent la plate-forme dans sa version à fin 2019 et sont peut-être attribuables à un manque de ressources. Des améliorations auraient toutefois été apportées, la nouvelle version étant prévue début 2020. En conclusion, si la plate-forme cyber-malveillance apporte déjà une première pierre importante (contenu « conseil » et « fiches pratiques ») à la mise en place d'un guichet unique pour les entreprises et les particuliers, elle reste toutefois à améliorer sur plusieurs points. Il faudrait en particulier :

- améliorer les interactions par un suivi de bout en bout des dossiers et des réponses correspondantes, peut-être en faisant appel à des associations bénévoles référencées ;
- réduire l'effet ping-pong, en affinant les questionnaires/interactions afin de mieux cerner les problématiques des utilisateurs ;
- mettre en place une structure transversale commune, permettant un suivi des dossiers cyber quelle que soit l'administration (CNIL, ANSSI, gendarmerie…) qui les prend en charge, afin de pouvoir répondre clairement aux entreprises et aux particuliers en les guidant, mais aussi en les accompagnant tout au long du traitement de leur dossier.



https://www.ssi.gouv.fr/agence/missions/nos-publics-et-nos-actions/

Source : ANSSI

SVP CYBER

En relation étroite avec le site.site cybermalveillance.gouv.fr, on peut donc imaginer un SVP cyber qui serait à la fois un espace de sensibilisation, d'information et de conseil, et qui pourrait s'articuler comme suit :

— *Une série de rubriques grand public,* volontairement rédigées en langage clair et simple, avec des informations accessibles au plus grand nombre, même et surtout aux non-spécialistes de l'informatique :
  - éviter les attaques par hameçonnage (phishing) ; faire face aux arnaques au faux support technique,
  - bien gérer ses mots de passe ; protéger ses appareils mobiles,
  - fichiers chiffrés avec demande de rançon : comment se protéger,
  - apprendre à séparer ses usages « pro » et « perso »,
  - se protéger contre une attaque en déni de service (DDoS), défiguration de site internet : que faire ?
  - mettre à jour ses appareils ; sauvegarder ses données ;

— *Un choix de publications, à caractère plus professionnel* : infographies, affiches (libres de droits) à reproduire et apposer en entreprise, vidéos, etc.
  - affiche de sensibilisation éditée par l'ANSSI rappelant les douze principes de base à respecter pour assurer sa cyber-sécurité : *« La sécurité numérique à portée de clic »*,
  - guide *« Anticiper et minimiser l'impact d'un cyber-risque »* de la FFA. Ce n'est plus optionnel pour les entreprises, quelle que soit leur taille. L'enjeu économique est vital : il s'agit pour elles de préserver leur savoir-faire,
  - guide des bonnes pratiques de l'informatique pour TPE/PME (ANSSI-CPME) : adoption de réflexes simples,
  - infographie *« Surfez Zen »* : à mettre entre toutes les mains. Cette infographie réalisée par l'ANSSI recense les principales menaces guettant les utilisateurs sur Internet et les bons réflexes à adopter sans attendre,
  - guide *« L'essentiel de la sécurité numérique pour les dirigeants »* du CEIDIG,
  - guide *« Réagir à une attaque informatique : 10 préconisations »* de la police nationale. Celles-ci constituent des repères essentiels pour aider les entreprises à appréhender la marche à suivre après un incident,
  - *« Guide de cyber-sécurité pour les PME »* (CCB-Belgique) qui fournit aux PME un aperçu des mesures de base et des plus avancées au plan cyber-sécurité,
  - vidéos de La *Hack Academy*, télé-crochet fictif où quatre personnages hauts en couleur démontrent par le contre-exemple et la dérision les risques auxquels chacun est exposé sur Internet (de quoi passer un bon moment…),
  - le kit de sensibilisation réalisé par cybermalveillance et ses membres (à télécharger absolument sur le site) a pour objet de sensibiliser aux questions de sécurité du numérique, de partager les bonnes pratiques dans les usages personnels et d'améliorer les usages dans le cadre professionnel. Les thématiques qu'il couvre sont : les mots de passe, les usages pro ou perso, les appareils mobiles, l'hameçonnage (Phishing), les Quiz, les mises à jour, les sauvegardes, les arnaques au faux support technique, les rançongiciels (Ransomware) et les réseaux sociaux ;
— *un fil d'actualités grand public ou professionnelles* sur le front de la cyber-malveillance, sur les attaques récentes et sur les moyens de défense. On y trouverait par exemple :
  - comment se prémunir d'une arnaque au faux support technique ?
  - avertissement sur les soldes : conseils pour affronter les cyber escroqueries ,
  - outil de déchiffrement du rançongiciel (ransomware) PyLocky versions 1 et 2,
  - comment identifier et supprimer un virus ?
  - Notre-Dame de Paris : campagnes d'arnaque en cours,
— force de frappe du dispositif SVP cyber, une mise à disposition des coordonnées des nombreux prestataires de service classés par spécialité/compétence et par localisation, donnant ainsi un accès facile aux professionnels sélectionnés en fonction du demandeur et de sa situation. Un menu permettrait à la victime de préciser son problème et son code postal, pour bénéficier immédiatement d'une liste des prestataires référencés avec leur adresse et numéro de téléphone. Le dispositif ne ferait pas de recommandation : la victime garderait son choix et devrait prendre directement contact avec les quelques prestataires

- proposés pour en savoir plus, consulter les avis clients, demander et comparer des devis…
- un système (le plus léger possible) de suivi d'incidents, qui permettrait à la fois un retour de type « satisfaction clients » vers la victime après un délai raisonnable et une évaluation qualitative des prestataires référencés, et serait aussi un outil statistique utile dans l'écosystème du risque cyber qui n'en est qu'à ses débuts.

On ne peut que souhaiter qu'un minimum de gens aient à se faire connaître comme victimes. Mais la lutte contre la cyber-malveillance est un enjeu de salut public, et on peut espérer qu'avec la création d'un SVP cyber on aura sous la main une réponse pratique, immédiate et quasi gratuite pour se faire aider à surmonter les attaques cyber.

Chapitre XI

Le projet CYBUNIH (Cyber union-ihedn)

L'Union-IHEDN s'appuie sur son maillage territorial et sectoriel d'auditeurs et d'associations pour soutenir les programmes de sensibilisation aux risques numériques et à la protection des systèmes d'information.

Les « relais CYBUNIH » s'interfacent avec les relais légitimes pour renforcer leur action dans les territoires et valoriser les contenus validés par les prescripteurs nationaux. Pour délivrer un message pratique et pertinent, ils sont formés et intégrés dans un schéma territorial coordonné avec les partenaires institutionnels.

Cette initiative sera traitée avec la légitimité, les atouts et les limites de l'Union-IHEDN, et s'appuiera sur son réseau d'auditeurs, force active et mobilisable dont les actions devront être coordonnées dans tous les territoires et pilotées au niveau national avec ses partenaires. Cela supposera des connaissances réactualisées et standardisées selon les meilleures pratiques, reconnues par les institutionnels publics et privés légitimes, et des moyens de référencement et communication centraux utilisés en commun par toutes les associations d'auditeurs.

Comment délivrer la sensibilisation sur le terrain

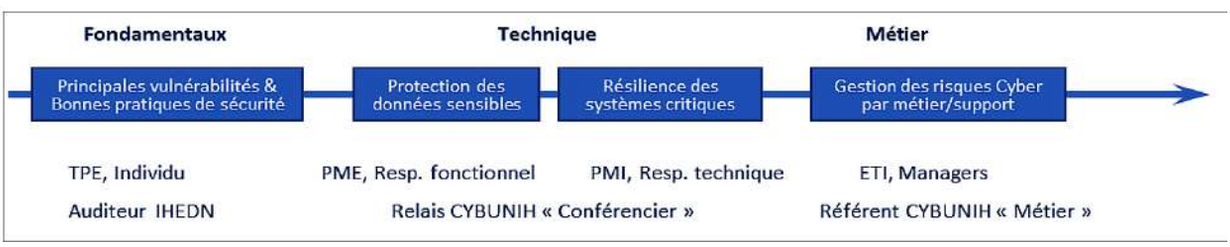
Même s'ils pouvaient être formés en nombre suffisant, les auditeurs IHEDN n'ont *a priori* guère de légitimité à aborder directement le sujet cyber-sécurité auprès de professionnels et dans les territoires. Ils peuvent, par contre, apporter leur soutien aux prescripteurs, services publics, prestataires de conseil et associations de professionnels légitimes. En effet, si les prescripteurs sont centralisés et très compétents, ils ne peuvent atteindre de manière fine tous les acteurs des territoires. À l'opposé, les prestataires de services et les fédérations de professionnels sont sur le terrain, mais, soit n'ont pas encore intégré le management des risques cyber, la sécurité des systèmes et la protection des informations dans leur prestation, soit n'ont pas de ressources compétentes en nombre suffisant pour satisfaire au cas par cas les besoins sur leur périmètre.

Par construction, les auditeurs IHEDN sont formés aux questions de défense, et souvent intégrés à des niveaux de management significatifs dans tous les secteurs : privé, administratif, associatif et de réserve militaire. Ils représentent donc une force d'accompagnement efficace tant de l'offre (mise en relation des porteurs, valorisation des initiatives) que pour la satisfaction

de la demande (information pertinente, sensibilisation, événementiels). La fonction de « Relais CYBUNIH » est donc créée pour faciliter en région l'identification des auditeurs IHEDN motivés, leur formation par les prescripteurs, leur coordination avec les relais professionnels légitimes, et leur emploi sur le terrain.

On peut envisager deux types d'intervenants :

- le « relais CYBUNIH » est un membre du comité directeur de chaque association régionale d'auditeurs IHEDN, nommé comme référent pour coordonner sur son périmètre géographique les volontaires, les auditeurs conférenciers, les partenaires, les actions et les événements, en interface avec la commission cyber-stratégie de l'Union-IHEDN dont il déploie le schéma national de formation et de pilotage territorial.
- le « conférencier CYBUNIH » est un auditeur IHEDN volontaire pour participer aux actions de sensibilisation organisées ou soutenues par son association régionale avec ses partenaires locaux (CPME, CLUSIR, Trinômes), référencé à ce titre par la commission cyber-stratégie de l'Union-IHEDN, et maîtrisant les contenus de référence (MOOC, guides, sites web, formation, etc. certifiés ANSSI).



Cette capacité d'un accompagnement « éclairé en central » et « coordonné sur le terrain » auprès des acteurs en place, constituera la force, la spécificité et la légitimité du réseau des « relais CYBUNIH ». Cette force de sensibilisation sur le terrain sera renforcée en amont au niveau national par une capacité d'animation et de formation des relais CYBUNIH, et de coordination territoriale et sectorielle avec les partenaires légitimes (pilotage dans chaque région administrative avec l'ANSSI, la réserve, les fédérations de professionnels et d'experts, etc).

Schéma national de formation et de pilotage CYBUNIH

Le « pilote régional CYBUNIH » est choisi parmi les relais CYBUNIH des associations régionales IHEDN relevant d'une même Région administrative (13 en Métropole et 5 en Outre-Mer), de préférence dans l'AR où se trouve la préfecture de Région. Il est nommé par la commission cyber-stratégie de l'Union-IHEDN, qu'il représente auprès des services régionaux de l'État et des partenaires (ANSSI, gendarmerie, Réserve cyber, CNIL, associations professionnelles, etc.) et participe aux comités de coordination des actions de sensibilisation. Idéalement membre d'une association partenaire ou de la Réserve cyber, le pilote eégional CYBUNIH doit maîtriser

les contenus de référence, s'impliquer activement dans les accords de partenariat, et assurer pour l'Union-IHEDN au niveau de la Région le rayonnement et l'animation cyber, tâches pour lesquelles il peut désigner un suppléant afin de l'assister.

Le « référent métier CYBUNIH » pilote au niveau national pour l'Union-IHEDN un des partenariats cyber établis avec un institutionnel ou une association professionnelle. Ces partenariats étant souvent issus d'une action en Région, les référents sont prioritairement choisis au sein de l'AR IHEDN qui a pris localement l'initiative de partenariat avec l'entité régionale, dont l'auditeur référent est généralement membre et donc bien informé de ses besoins. On peut ainsi améliorer la facilité d'organisation dans la région et généraliser le partenariat à tout le territoire en reproduisant les bonnes pratiques dans d'autres régions et en les valorisant au niveau national.

Le Comité de pilotage CYBUNIH regroupe les pilotes régionaux, les principaux référents métier et des membres désignés de la commission cyber-stratégie de l'Union-IHEDN. En application du schéma directeur CYBUNIH défini par la commission, il convient des modalités de relation avec les partenaires (prescripteurs, fédérations nationales), valide les contenus de référence et le processus de validation de leur maîtrise par les conférenciers (formations des relais cyber-IH), consolide et valorise les actions en Région (animation, annuaire, site web).

Schéma territorial de coordination CYBUNIH

Territoire Région administrative	A.R.	A.R PILOTE
Auvergne Rhône-Alpes	2, 8, 14	Région Lyonnaise
Bourgogne Franche-Comté	4, 10	Bourgogne
Bretagne	5, 6	Haute Bretagne
Centre-Val de Loire	7	Centre-Val de Loire
Corse	20	Corse
Grand Est	13, 22, 23	Alsace
Guadeloupe	31	Guadeloupe
Guyane	30	Guyane
Hauts de France	15, 24	Nord
Ile de France	16, 21	Paris- Ile de France
La Réunion - Mayotte	27	La Réunion - Mayotte
Martinique	26	Martinique
Normandie	3, 11	Normandie
Nouvelle Aquitaine	1, 18, 25	Aquitaine
Nouvelle Calédonie	32	Nouvelle Calédonie
Occitanie	12, 19	Midi-Pyrénées
Pays de Loire	17	Pays de Loire
Polynésie Française	28	Polynésie Française
Provence Alpes Côte-d'Azur	9, 20, 29	Provence

Des auditeurs et des contenus certifiés

La mise en place des relais CYBUNIH est un programme ambitieux qui nécessite des moyens de formation, d'animation et de communication. Leur compétence, leur capacité de coordination

territoriale et leur prise en charge de l'implication des associations régionales IHEDN sont les trois facteurs clés de succès.

a. Les relais CYBUNIH d'une association régionale IHEDN accompagnent les actions locales de sensibilisation.
b. Les référents métier CYBUNIH identifient et valorisent les supports et programmes des fédérations nationales.
c. Le Comité de pilotage CYBUNIH s'assure au niveau national de la qualité (certification) et valorise les contenus diffusés.
d. Le pilote régional CYBUNIH aide à cadrer l'initiative avec l'ANSSI, la réserve cyber- et les partenaires de la Région.
e. Les kits CYBUNIH (supports par cible : PME, PMI, ETI ; et par problématique : donnée, systèmes, risques) aident le conférencier à se former et à diffuser les messages les plus pertinents pour la manifestation qu'il anime.
   - fondamentaux : vulnérabilités et règles d'hygiène informatique,
   - techniques : protéger ses données sensibles et ses systèmes critiques,
   - métiers : réduire les risques numériques dans chaque fonction métier/support ;
f. Les kits auditeur permettront à chacun de pouvoir se former aux fondamentaux et devenir un conférencier CYBUNIH. Aujourd'hui, tout le monde peut se former gratuitement aux fondamentaux de la cyber-sécurité, et traiter sérieusement des problématiques et solutions qu'encore trop peu d'entreprises maîtrisent complètement. D'où la démarche proposée à tout auditeur motivé pour devenir Conférencier CYBUNIH.

Nous encourageons la mise en place dans l'annuaire Interne de l'Union-IHEDN par association régionale, d'une liste des auditeurs disposés à faire des interventions, que ce soit dans un cadre interne ou à l'extérieur. Bien que de nombreuses compétences et initiatives existent, elles sont trop souvent ignorées en dehors du périmètre des associations d'auditeurs. Pour être efficaces et reconnues, les actions cyber en Région doivent être partagées, soutenues et valorisées au niveau de l'Union-IHEDN. Les relais CYBUNIH doivent être formés, certifiés et proches du terrain. Des kits CYBUNIH « certifiés » seront élaborés à partir de contenus existants, sélectionnés et organisés pour garantir la qualité des interventions et leur pertinence par rapport à chaque besoin.

Des contenus certifiants pour devenir un intervenant CYBUNIH

L'ANSSI a produit de nombreux guides sur différentes thématiques plus ou moins techniques. Elle référence aussi, et certifie régulièrement, des guides produits par les fédérations professionnelles. Les auditeurs IHEDN souhaitant devenir des intervenants ou des conférenciers CYBUNIH se doivent de maîtriser la culture générale du MOOC de l'ANSSI et, selon l'expertise thématique ou le partenariat métier qu'ils souhaitent animer, les guides méthodologiques du partenaire métier (validé au préalable par l'ANSSI). *La production de nouveaux contenus ou le référencement de supports au contenu non certifié sont à proscrire.*

Formations certifiantes minimum pour un conférencier CYBUNIH **:** - MOOC de l'ANSSI (attestation pour 4 modules de 5h) - MOOC sur la protection des données à caractère personnel (atelier-rgpd.cnil.fr) - MOOC's complémentaires (UBS, CNAM, EPITA…) Pour les référents métier ajouter : - Le Guide d'hygiène informatique de l'ANSSI (a minima) - Les 20 guides thématiques référencés en annexe des kits CYBUNIH	

Démarrage et pilotage CYBUNIH

1) Mise en place des relais CYBUNIH au niveau des « AR » (associations régionales IHEDN)

- Présentation par l'Union-IHEDN de la stratégie CYBUNIH à tous les présidents d'AR IHEDN.
- Identification par chaque AR IHEDN du relais CYBUNIH qui fera partie de son comité directeur.
- Référencement des membres, des compétences et des actions cyber- de l'AR.
- Remontée de l'information à la commission cyber-stratégie de l'Union-IHEDN.
- Formation dans chaque AR des relais CYBUNIH (veille, kits conférenciers, certification).

2) Mise en place des pilotes régionaux et des référents métier CYBUNIH

- Validation des pilotes régionaux et des référents métier et formation au schéma directeur CYBUNIH.
- Autoformation certifiante aux contenus et kits de référence CYBUNIH.
- Présentation du schéma aux partenaires et mise en relation des correspondants régionaux.

3) Mise en place du Comité de pilotage et des moyens d'animation du réseau CYBUNIH

- Réunion bimestrielle du comité de pilotage CYBUNIH avec les pilotes, les relais et les référents CYBUNIH.
- Annuaire pour le référencement en ligne des relais CYBUNIH et de leur groupe cyber.
- Espace collaboratif (blog filtré) où partager les contenus, les événements et les acteurs de la cyber traités par les relais CYBUNIH de chaque AR IHEDN.
- Recrutement et formation de conférenciers CYBUNIH.
- Soutien à l'organisation d'évènements de sensibilisation (conférenciers, sponsor, kits…).
- Consolidation des rapports d'activités des AR IHEDN et partage auprès des partenaires.
- Rapport annuel et conférence de présentation consolidée des actions CYBUNIH

Journées cyber de l'Union-IHEDN

Le réseau des auditeurs IHEDN forme un maillage national et régional important, qui touche par nature tous les domaines de la société française, y compris au niveau décisionnel. Force est pourtant de constater que, bien que présent dans toutes les strates de la société française, le rayonnement de l'Union-IHEDN reste faible auprès du grand public. C'est vrai, en particulier, dans le milieu cyber, où peu d'entreprises et de start-ups se sentent concernées par la défense nationale, au sens le plus général du terme.

Il faut donc envisager un événement annuel cyber servant de référence à la communauté Union-IHEDN, et qui pourrait devenir du même coup une source de rayonnement notable vers les responsables de haut niveau, offrant au passage une tribune aux institutions qui nous accompagnent, ainsi qu'au milieu universitaire et de la recherche de haut niveau. On pourrait s'inspirer du modèle Forum Teratec[101], qui rayonne largement dans le milieu du calcul haute performance, tout en nouant des partenariats avec les institutions, les grands groupes, et les entreprises innovantes. L'événement cyber aurait pour objectifs la propagation du savoir, la reconnaissance des grands acteurs institutionnels du domaine, le rayonnement de l'Union-IHEDN et la mise en valeur de ses auditeurs. Il pourrait constituer le lancement du programme CYBUNIH et de la mobilisation des auditeurs IHEDN, en vue d'aider à sensibiliser au cyber les populations vulnérables de notre pays.

Ces Journées cyber de l'Union-IHEDN seraient composées pour une part de sessions plénières avec institutionnels et grands acteurs du domaine comme ANSSI, CNIL, ORANGE, mais aussi des présentations de nouvelles technologies et de projets innovants de start-ups. Sous la conduite de spécialistes et d'auditeurs IHEDN, il y aurait d'autre part des ateliers techniques et applicatifs : impact pour les collectivités d'une défense cyber, implication du RGPD pour les TPE, etc. Le financement de ces journées pourrait être assuré par des mécènes ou sponsors, auxquels on donnerait en contrepartie une certaine visibilité dans ce domaine porteur. Dans l'idéal il faudrait qu'un tel évènement soit « tournant », et prenne place chaque année dans une région différente pour couvrir le maximum de territoires, et partant d'entreprises, d'organisations, d'universités et de particuliers.

PILOTAGE DES RELAIS CYBUNIH

En accord avec la stratégie définie avec les prescripteurs (ANSSI, Comcyber, gndarmerie, CNIL) et partenaires (fédérations nationales), les relais CYBUNIH veilleront à ce que la sensibilisation des petites entreprises (PME, PMI, ETI) soit traitée au plus près de leurs besoins (études de cas, vidéos, guides, contacts locaux…) validés avec leurs fédérations professionnelles, en capitalisant sur les contenus certifiés (en priorité ceux de cybermalveillance.gouv.fr et les guides des relais « métiers » (CPME, Medef, Cigref, Captronic, CLUSIF/R…).

101 http://www.Teratec.eu/forum/

Avec ce schéma de pilotage national, les actions locales du programme CYBUNIH pourront être d'autant plus efficaces et légitimes qu'une coordination opérationnelle (date, lieu, intervenants, cibles, patronage…) au sein de chaque région administrative sera assurée par les pilotes régionaux CYBUNIH avec les triptyques régionaux ANSSI/Comcyber/gendarmerie, ainsi qu'avec les comités de pilotage régional des fédérations partenaires. L'appartenance de pilotes, de relais ou de référents CYBUNIH à la réserve cyber, à la réserve IHEDN ou à l'une des fédérations partenaires serait un facteur clé de succès.

PRESCRIPTEURS CYBER-SÉCURITÉ		RÉFÉRENTS MÉTIER	
ANSSI		CPME, CINOV-IT	
Com cyber		MEDEF	
ACYMA	CYBERMALVEILLANCE.GOUV.FR Assistance et prévention du risque numérique	CLUSIF	
Gendarmerie nationale		Cigref	
CNIL		DFCG	
Trînôme académique / SNU		AMRAE	
Réserve citoyenne (non cyber)	LA RÉSERVE CITOYENNE	CCI France, CAP TRONIC	

Rappel de quelques fondamentaux de la cyber-sécurité

Quelle que soit la taille de l'organisme, l'exposition aux menaces cyber repose souvent sur l'ignorance de principes de sécurité pourtant élémentaires et sur un manque de responsabilisation (la sécurité : ce n'est pas moi !) Il faut donc :

- identifier l'information sensible (valeur qu'elle revêt pour un attaquant, exigences légales…) ;
- protéger les mots de passe (qu'est-ce qu'un *bon* mot de passe, séparation des usages, comprendre les attaques par force brute, par ingénierie sociale, par défaut de protection dans les fichiers) ;
- protéger les appareils mobiles (PC portables, smartphones perso/ pro, clés USB…) ;
- déjouer les tentatives de manipulation psychologique (réseaux sociaux, *phishing*) ;
- utiliser des logiciels fiables ;
- veiller à les mettre à jour (les virus exploitent les erreurs de codage et de configuration) ;
- comprendre et repérer les attaques virales automatisées (*spam/phishing, ransomware*, faux site web) ;
- sauvegarder et savoir restaurer ses données en cas de perte/destruction de système.

Comprendre les fondamentaux de la cyber-sécurité requiert une explication simple et concrète :

- des types d'attaques, de leur fréquence, de leur origine et de la motivation des attaquants ;

— des vulnérabilités techniques et humaines exploitées par les hackers et les logiciels malveillants ;
— des manières simples de réduire son exposition au risque par quelques bonnes pratiques de sécurité.

Les sites web de l'ANSSI, de la CNIL et de cybermalveillance.gouv.fr regorgent d'articles sur ces sujets. Pour un débutant (auditeur, PME/PMI, enseignant) nous suggérons de commencer par :
— le portail cybermalveillance.gouv.fr dans son intégralité (statistiques, vidéos, fiches pratiques, contacts) ;
— quelques guides simples de l'ANSSI : passeport voyageur, posters, synthèse du mois de la cyber-sécurité ;
— l'histoire de la CNIL et ses publications Facebook (principes de protection, incidents, condamnations) ;
— des vidéos humoristiques sur les impacts d'attaques (Hackademy ; Pub Qwant ; Cigref).

Trame de conférence : sensibiliser aux risques et à la sécurité cyber

Le succès d'une action de sensibilisation réside dans la capacité à parler d'enjeux qui concernent directement l'auditoire : perte d'activité commerciale, de service, de production ; dans un langage concret (celui d'un manager qui couvre plusieurs fonctions opérationnelles et techniques) ; à mettre en évidence la réalité des menaces, à souligner la responsabilité de chaque collaborateur (vidéos, témoignages), et enfin à proposer de bonnes pratiques, faciles à mettre en place et réduisant au minimum les risques les plus courants :
— convaincre de la réalité des attaques (pertinence par rapport au secteur/territoire) :
  - présenter en mode interactif un cas fictif (vidéo ou témoignage d'intervenant),
  - présenter des statistiques et des exemples pertinents pour l'auditoire (géographie, activité…),
  - expliquer les principales vulnérabilités à l'origine des incidents et attaques,
  - présenter une ou deux vidéos de modes opératoires pertinents par rapport à l'auditoire,
  - présenter des catalogues plus larges (cyber-malveillance) à revisiter après la conférence,
— détailler l'impact d'une attaque (perte d'activité, confiance client, vol, rançon, procès…) :
  - rappeler le besoin de sécurité en termes de perte de disponibilité, de confidentialité ou d'intégrité,
  - illustrer l'explication avec un cas réel (vidéo) selon l'activité économique de l'auditoire :
    - PMI : indisponibilité opérationnelle (production, logistique, e-commerce, mail…),
    - PME : perte/fuite de données (commerciale, innovation, clients, personnelles, classifiées…),

- ETI : non-conformité légale, procès, campagne de presse (comptabilité, fraude, RGPD…) ;
- proposer de bonnes pratiques, simples et efficaces, face aux scénarios de risque exposés ;
- reprendre les scénarios et vulnérabilités précédemment exposés en montrant que ces incidents auraient pu être évités ou leurs conséquences réduites par le respect de bonnes pratiques simples :

- contrôle d'accès (droit d'en connaître, gestion des mots de passe, perte/vol de PC en voyage),
- prévention des virus (repérer un spam, installation/mise à jour de logiciel, clé USB/site web),
- continuité d'activité (sauvegarde sécurisées et testées, contrats de support, télétravail) ;

— communiquer sur les formations facilement accessibles (en lien avec les vulnérabilités) :
  - MOOC ANSSI, CNIL, UBS, CNAM…
  - stages de formations certifiées par l'ANSSI ;
— communiquer sur les procédures / prestataires utiles en cas d'incidents majeur :
  - contacts pour déclarer / vérifier une malveillance,
  - procédures pour initier une procédure judiciaire / enquête de police,
  - liste de prestataires (distinguer certifications ANSSI ou simple référencement) ;

— remettre un guide de synthèse (pertinence par rapport aux contenus présentés/présentiel) :
  - URL des sites de référence,
  - Guide imprimé (rédigé par un partenaire + validé par l'ANSSI/CNIL).

Retours d'expérience & témoignages

Témoignage de Véronique GUEVEL : Protéger les PME

Concernant les PME, mon constat est que leur niveau d'adoption et de compréhension est encore très insuffisant, en particulier pour la protection des données (dont celles à caractère personnel), malgré les partenariats possibles avec la CPME et la Réserve cyber de la gendarmerie. De mes nombreuses interventions depuis des années auprès d'associations de chefs d'entreprises, de la CPME, de syndicats, de maisons de l'emploi, forums, IHEDN, événements comme le cyber-Day, sur différents sujets couvrant le Cloud, le RGPD et la cyber-sécurité, plusieurs mots ressortent : temps, coût, complexité du sujet ; compliqué à mettre en œuvre, besoin d'adhésion de tous, impossibilité de le faire ; déjà subi un risque, risque humain, peur de la menace… Et pourtant la prise en compte du risque n'est guère au rendez-vous, même si l'on constate une prise de conscience du risque de tout perdre. Peu de retour d'ailleurs pour savoir si on a pris des mesures ou pas.

Présentation orale de 45 minutes (sans projection de support) expérimentée dernièrement et qui semble être bien reçue :

pour introduire le sujet, détailler et expliquer les risques retenus et pourquoi (contexte actuel incertain et à risque ; défi majeur : la confiance dans les acteurs, les sous-traitants) avec des exemples, et faire le lien avec les articles du RGPD pour lister certaines idées reçues (avec des chiffres à l'appui : nombre d'attaques, etc.) et les démolir : « Le RGPD c'est pour les GAFAM », « Mes données n'intéressent personne, je n'ai rien à cacher, je ne commercialise pas les données de mes clients, pourquoi devrais-je me mettre en conformité au RGPD ? »

développer ensuite en détail l'historique qui a conduit à la création de la CNIL et pourquoi le RGPD prend tout son sens. Illustrer par un exemple réel (un magasin avec la notion de contact humain) et virtuel (e-commerce) pour faire comprendre le mécanisme des aspects marketing (cookies) et les délais de conservation des données, avec la carte bancaire par exemple. Analyser les attaques types, et expliquer pourquoi les données ainsi que les infrastructures et les systèmes d'information des participants intéressent les hackeurs. Toujours avec des exemples et des témoignages vécus.

Conclure en disant comment réagir (gestion de l'incident, à qui je m'adresse : en réparation, en communication, les autorités compétentes), ce qu'il faut mettre en place (anticiper, avoir des processus), en soulignant l'intérêt du RGPD, la nécessité d'avoir une charte informatique et de sensibiliser, de former les personnes et de les responsabiliser, car elles peuvent/doivent aussi être sanctionnées en cas de non-respect (de la charte informatique, par exemple), en donnant des exemples concrets tirés de l'actualité : quand tout cela est dit clairement, les gens font bien plus attention aux outils qui leur sont confiés. Présenter les différents kits et citer les MOOC : ANSSI, CNIL etc). L'idée n'est pas de faire peur, mais de montrer que ça existe et que c'est bien réel. Cette approche est transposable et peut être adaptée selon la cible et le secteur d'activité car nous avons des exemples dans tous les domaines et pour tous les publics. Elle est en général très appréciée de l'auditoire, avec beaucoup de questions, des remerciements aussi, car le public témoigne qu'il a appris des choses. C'est d'autant plus important que, vu l'ampleur des attaques, véritable raz de marée, si les personnes directement concernées ne font rien, on risque une catastrophe économique et financière de grande envergure.

Mon stage à l'ANSSI m'a beaucoup aidé à structurer mon discours et ma présentation, pour expliquer, par exemple, ce qu'est une attaque cyber : attaquant(s), motivation(s), vecteur(s), finalité(s), alors que sur ces sujets, on voit beaucoup trop de gens qui se font passer pour des ***sachants***, mais qui ne maîtrisent pas du tout le sujet. On constate le même phénomène dans certains articles de presse. L'important est d'indiquer les bonnes pratiques et, encore une fois, de suivre le bon sens, et enfin de proposer des outils labélisés, des formations pour apprendre où et comment faire de la veille.

Témoignage de François GUYOT : sensibiliser PME/PMI et collectivités territoriales

Après les grands groupes industriels, le risque cyber s'abat sur les PME/PMI et les « petites » collectivités territoriales. Bien que réel, ce risque est méconnu par la plupart de leurs dirigeants. Toute action de sensibilisation doit donc commencer par celle du « top management », sans lequel aucune action dans la durée ne peut être sérieusement envisagée. La difficulté est bien sûr de réussir à joindre ces dirigeants surbookés par leurs sujets favoris (« client », « cash », « production »…) et peu disponibles pour s'intéresser à d'autres.

Pour atteindre l'objectif, une argumentation ***ad hoc*** doit être formulée en « face à face », lors d'un bon moment obtenu de façon « opportuniste ». Elle sera exprimée en termes de risques business, directs ou indirects, en schémas d'attaque sur une structure informatique et ses cibles potentielles (avec des exemples), et sur les conséquences opérationnelles pendant la phase de remédiation consécutive à un sinistre. Les cas de Saint-Gobain et du CHU de Rouen sont tout à fait adaptés pour illustrer ces divers points. Une fois réussie, cette première étape permettra d'élargir très vite la communication aux collaborateurs « en charge », pour les amener vers des partenaires professionnels qui pourront les aider à identifier, puis à dérouler, les séquences audit et plan d'action nécessaires.

La première difficulté à surmonter est donc d'obtenir ce contact « direct/face à face ». Pour favoriser cette démarche, plusieurs axes d'action sont à développer :

s'appuyer sur les institutionnels, interlocuteurs habituels du chef d'entreprise et du maire est un bon moyen : il a besoin d'eux et réciproquement. Qui sont-ils ? Les autorités (préfet, gendarmerie/police…), les élus déjà acquis à cette cause (députés, conseillers départementaux et régionaux, communauté d'agglomération, CESE), les organisations consulaires et professionnelles : CCI, MEDEF, CPME, U2P (Union des entreprises de proximité), AMF (Association des maires de France), CMA (Chambre de métiers et de l'artisanat), associations locales d'entreprises…

provoquer l'évènement autour d'un thème principal autre que la cyber-sécurité, mais présentant a minima quelques analogies ;

« imposer » une présence personnelle « non délégable » ;

disposer d'un outil de communication professionnel (avec contenu adaptable à la diversité des entreprises ciblées), qui soit aligné sur les recommandations de l'ANSSI, administration de référence en la matière ;

s'appuyer sur des intervenants « au bon niveau cyber », tant par leur capacité à s'adresser aux chefs d'entreprises que par leur maîtrise du sujet.

La première étape est de **mobiliser les acteurs consulaires et professionnels** du département et de la région, pour les convaincre de la pertinence de la démarche et de la qualité des intervenants (que la gendarmerie peut garantir). Il faudra ensuite identifier avec eux les « dirigeants cibles » à traiter en priorité, puis positionner des actions de sensibilisation en les intégrant dans le cadre d'évènements qui leur sont propres et qui touchent les dirigeants visés. Un essai en grandeur réelle est en préparation en Bourgogne Franche-Comté, avec le soutien de la gendarmerie nationale et des services de la préfecture.

Témoignage de Marie-Hélène PEBAYLE : sensibiliser les responsables financiers

J'ai une double expérience dans la sensibilisation des cibles les plus vulnérables à la cyber-sécurité :

comme directrice administrative et financière d'ETI et de collectivités territoriales depuis plus de vingt ans, membre à ce titre du réseau de décideurs financiers DFCG, je constate qu'outre le DSI, le garant de la valeur de l'entreprise est le DAF, car aujourd'hui cette valeur dépend de la sécurité de ses données et de ses systèmes d'information ;

comme réserviste citoyenne et auditeur IHEDN, référente des correspondants défense des communes du Var

Aujourd'hui, à travers les systèmes informatiques, les réseaux de smartphones ou encore les machines-outils communicantes, la technologie s'est insérée dans nos vies professionnelles et personnelles. La cyber-sécurité vise à protéger toutes ces données — tant du vol que de la modification —, mais aussi à faire en sorte qu'elles soient toujours disponibles lorsque nous en avons besoin, donc d'organiser leur résilience.

Selon le baromètre de PWC, une entreprise est en danger de mort en cas d'arrêt de sa production au bout de trois semaines. La cyber-sécurité ne peut être cantonnée aux fonctions de chacun, elle doit être portée par un processus transversal et collectif qui découle la gestion des risques.

Il n'y a pas d'entreprise qui échappe aujourd'hui à l'informatique, et nombreuses sont celles qui virtualisent tout leur patrimoine informationnel. Les entreprises « B to C » et celles dont les données revêtent un caractère stratégique (ex : transports), sont ainsi particulièrement vulnérables. L'IT représente en moyenne 5 % du budget d'une société. Mais, dans ce budget, la cyber-sécurité ne compte que pour 5 %, alors que les cyber-criminels ont montré ces dernières années leur réactivité et leur capacité à créer de nouveaux schémas de fraude.

Dans ce contexte, le directeur financier, qui a dans son ADN l'identification et l'appréhension du risque comme de la confidentialité, est un acteur clé et peut aider à transcrire en mots simples les enjeux et contraintes de ce sujet très technique. Il est aussi un acteur central de la cyber-sécurité dans l'entreprise, la direction financière étant en première ligne de la lutte contre la fraude (ciblée à 48 % sur la direction financière contre 19 % pour la direction générale). De par mon expérience des problémes de protection des données commerciales, financières, d'intégrité des comptes et de conformité légale, je suis en mesure de formaliser les besoins des entreprises en vulgarisant l'approche théorique, tout en m'attachant à prôner des solutions pragmatiques, et de sensibiliser aux exigences de sécurité avec les supports de sensibilisation et de méthodologie simples publiés par la CNIL ou l'ANSSI.

En tant que présidente de la DFCG Provence, je me suis engagée dans une démarche de sensibilisation à la cyber-sécurité des dirigeants financiers et de contrôle de gestion pour trois raisons principales :

la cyber-sécurité est une opportunité de développement, car elle s'attache à sécuriser le fonctionnement de l'entreprise et assurer sa pérennité ;

une cyber-sécurité intégrée au fonctionnement de l'entreprise permet de prendre les virages digitaux plus rapidement et avec moins d'investissement ;

la confiance devient une ressource valorisable pour les entreprises : investir dans la cyber-sécurité permet de renforcer la confiance et donc de fidéliser clients et consommateurs.

S'impliquer dans les réseaux professionnels DFCG permet d'augmenter la pertinence du discours pour mieux sensibiliser la profession aux risques et aux responsabilités ; nous avons ainsi organisé une manifestation reproductible en région dont vous trouverez ci-après une synthèse (soirée cyber à Marseille octobre 2019).

Exemple : première soirée cyber-sécurité de la DFCG Provence le 21 octobre 2019

Introduction et présentation du panorama cyber

Fabrice GARNIER DE LARBAREYRE, PwC

Le risque cyber devient la quatrième préoccupation des grandes entreprises, mais il est encore sous-estimé. Pourtant, c'est un enjeu vital. Une entreprise voit sa survie menacée après trois semaines de black-out. Chaque groupe devrait avoir un RSSI indépendant du DSI, car son rôle est d'alerter, de mettre en avant les failles de sécurité. De fait, le turnover des RSSI est de trois ans. Les dirigeants d'entreprises commencent à comprendre qu'ils sont aussi attendus sur ces sujets et que leur poste en dépend. Pour les mafias des pays de l'Est ou d'Afrique, la cyber-criminalité est bien moins dangereuse et plus rémunératrice. On estime le besoin en informaticiens spécialisés en cyber-sécurité à 2 millions dans le monde.

Table ronde : la cyber-sécurité une affaire de spécialistes ?

Moise MOYAL, délégué PACA Corse ANSSI

L'Agence nationale de la sécurité des systèmes d'information est chargée de proposer des règles à appliquer pour la protection des systèmes d'information de l'État et vérifier l'application des mesures adoptées. Dans le domaine de la défense des S.I., elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques. Elle apporte son expertise et son assistance technique aux administrations et aux entreprises, en particulier aux opérateurs d'importance vitale (OIV). Elle est enfin chargée de la promotion des technologies, produits et services de confiance, de sensibiliser le grand public aux enjeux de la sécurité des S.I. et de diffuser les bonnes pratiques.

Adrien MORANZONI, GSA Prado (Assurance)

Les compagnies d'assurance évoluent avec la technologie et les besoins des entreprises. Elles ne sont pas là pour pallier les lacunes des entreprises en termes de sécurité informatique, mais pour les

Chapitre XII

Trente propositions

1 Définir la sécurité cyber comme priorité stratégique nationale. Traduire cette volonté politique de souveraineté par la création d'une Autorité transversale du Numérique rattachée au Premier ministre. Chargée d'élaborer la doctrine cyber et ses grands axes, elle aurait aussi mission d'en animer le déploiement et d'en exercer le contrôle vis-à-vis de tous les ministères, dont en particulier ceux de l'économie, du commerce, de l'industrie, de la défense, de la recherche et de la santé .

2 Localiser sur le territoire national l'ensemble des processus critiques du cyber.

3 Organiser un *Grenelle du cyber* visant à prendre des décisions à long terme pour assurer un avenir cyber compatible avec nos valeurs, nos connaissances et nos moyens. Ces rencontres politiques réunissant dans leur diversité les forces vives de la Nation, il sera possible d'aligner les outils politiques, législatifs et économiques permettant de préparer l'avenir souhaitable. Il faut pour cela mobiliser nos connaissances et faire appel à nos valeurs, en dépassant le prisme purement technique pour porter cette réflexion au niveau moral et sociétal.

4 Fonder un *Observatoire du cyber* indépendant, multidisciplinaire, composé d'anciens et de plus jeunes, en lien avec le civil comme avec le militaire, chargé de réaliser d'année en année un état des lieux cyber, tableau de bord permettant de mesurer l'évolution de notre position par rapport à nos ambitions, et de guider ainsi notre pilotage politique, économique, technologique et sociétal.

5 Associer étroitement le secteur privé au projet national cyber piloté par la fonction publique, en réunissant autour d'un objectif commun la classe politique et le monde des affaires (où se trouvent les opportunités cyber et où en sont supportés les coûts), pour l'encourager celui-ci à y apporter ses importants moyens et à développer des solutions dont il sera un des bénéficiaires.

6 Déterminer les commandes de l'Administration en fonction de la stratégie cyber globale, en évitant de se focaliser uniquement sur le mieux disant.

7 Mettre en place pour les entreprises et pour les particuliers des mécanismes fiscaux encourageant les investissements dédiés au cyber.

8 Encourager la généralisation au niveau européen du modèle estonien d'identité numérique individuelle, tout en prenant les dispositions nécessaires pour préserver la confidentialité des données personnelles.

9 Vérifier l'aptitude de la technologie *blockchain* à constituer pour les systèmes d'information de santé un *tiers de confiance* neutre pour sécuriser les transferts de données entre les acteurs du système de santé, assurer la traçabilité des accès aux données médicales grâce à sa transparence et son inaltérabilité, garantir l'anonymat des patients grâce à son système de clés publiques et de clés privées, tout en réduisant les coûts de traitement informatique.

10 Identifier pour la ville intelligente quel acteur de confiance, privé ou public, national ou local, pourra être chargé de la récolte et du stockage des données de terrain et des données personnelles indispensables à son fonctionnement, en application de directives claires du Conseil constitutionnel pour éviter les dérives possibles.

11 Développer la « science participative » qui associe les citoyens à la production des savoirs (en particulier biologiques et écosystémiques), et permet à tout individu ou communauté d'utiliser des outils scientifiques pour collecter, analyser, interpréter et utiliser les informations disponibles de son environnement, accroissant ainsi les découvertes, leur impact et leur diffusion, et encourageant chacun à se sentir concerné.

12 Faire évoluer cybermalveillance.gouv.fr vers un guichet national unique *SVP cyber* en élargissant ses prestations actuelles d'aide aux entreprises ou particuliers victimes, pour leur apporter conseil et soutien de bout en bout. Que ce soit directement, ou en les aiguillant vers des prestataires de proximité susceptibles de les aider à recouvrer leur santé numérique. Et surtout en les accompagnant tout au long de leur dossier traité par la Gendarmerie, la CNIL, l'ANSSI ou d'autres.

13 Accroître l'attractivité et la lisibilité de la filière cyber-sécurité qui offre beaucoup de postes face à une pénurie mondiale de techniciens ou d'ingénieurs disponibles, en valorisant ses métiers auprès du grand public, en favorisant l'orientation des lycéens et des étudiants de bon profil vers une formation adaptée, en développant des lieux d'échange pour faciliter l'accès du plus grand nombre à la filière, en y adjoignant l'Intelligence artificielle comme priorité stratégique.

14 Instituer un module d'éducation cyber obligatoire à tous les stades de la scolarité : école, collège, lycée, université, grandes écoles et autres formations professionnelles, pour permettre à chacun d'acquérir les bases minimales nécessaires à la future vie du citoyen connecté.

15 Intégrer aux Journées défense et citoyenneté et au service national universel un dispositif d'identification et d'évaluation des compétences cyber, pour repérer les talents prometteurs et proposer aux jeunes talents un parcours de formation spécifique.

16 Favoriser la diversité des profils et des parcours dans le recrutement cyber- des filières d'excellence comme des entreprises, en veillant à autoriser une grande flexibilité vis-à-vis des « atypiques » ayant des compétences cyber reconnues : *« Ça n'a pas de sens d'embaucher des gens intelligents puis de leur dire quoi faire. Nous embauchons des gens intelligents afin qu'ils puissent nous dire ce qu'il faut faire »* (Steve Jobs)

17 Actualiser par la formation continue (MOOC de l'ANSSI par exemple) les compétences cyber des salariés, ne pas hésiter à en orienter les plus aptes vers une formation cyber qualifiante, renforcer leur sensibilisation et celle des dirigeants d'entreprises sur la cyber-sécurité, établir des règles de sécurité cyber connues de tous et dont le non-respect devrait être sanctionné.

18 Annexer au bilan comptable annuel un volet *Responsabilité cyber des entreprises* reprenant les 40 critères du guide d'hygiène de l'ANSSI selon une grille simple d'évaluation, permettant ainsi de suivre l'évolution de la prise de conscience cyber- dans cette entreprise et de son niveau de sécurité cyber.

19 Pousser les assureurs à élaborer une politique claire d'offre cyber pouvant s'inspirer des polices environnement. Elle comprendrait des questionnaires de c*ompliance cyber* pouvant servir de guide utile aux TPE/PME, et serait complétée par une série de mesures contraignantes : plan de prévention et de formation à mettre en œuvre comme condition préalable à la couverture de risques cyber, critères de déchéance d'indemnisation ou de hausse des primes, etc.

20 Adapter le droit au paradigme nouveau créé par le cyber : droit de la concurrence, en y autorisant le traçage de transactions illégales ; la propriété intellectuelle, en y révisant la qualification d'auteur ; droit pénal en y incorporant la notion d'arme numérique comme système ou objet virtuel utilisé pour tuer ou blesser.

21 Appuyer sur les organisations professionnelles (ordres, syndicats, CCI, organismes de formation, réseaux de grandes entreprises) le dispositif de déploiement territorial par les triptyques ANSSI-Comcyber-gendarmerie d'une campagne nationale de sensibilisation à la cyber-sécurité des TPE/PME/PMI/indépendants ou libéraux, avec des évènements adaptés au tissu économique local et qui pourraient être financés par des partenariats public/privé.

22 Fournir à l'Union-IHEDN les ressources nécessaires pour mettre en œuvre son projet CYBUNIH de renforcement de la vigilance cyber au sein de la population française, mobiliser à cet effet une partie de ses 10 000 auditeurs IHEDN formés aux questions de

défense, souvent intégrés à des niveaux de management significatifs dans tous les secteurs et représentant une force d'accompagnement efficace, et déployer sur le terrain dans la durée un programme national de sensibilisation cyber- à destination des segments de population les plus vulnérables : jeunes, PME/PMI/TPE, petits organismes territoriaux.

23 Conduire la création d'une *Europe cyber* faisant contrepoids aux États-Unis, à la Russie et à la Chine avec, comme en matière monétaire, une politique commune supranationale et totalement intégrée. À défaut d'une convergence des 27, créer une Communauté européenne du numérique regroupant les États ayant une vision et une volonté communes. Une première étape serait un partenariat stratégique bilatéral (par exemple franco-allemand) sur le modèle des programmes régionaux d'intégration pour les industries de défense. Si l'UE a sans doute perdu la bataille du *Hardware* et du *Software*, il lui reste un rôle à jouer dans la bataille des normes en tant que premier marché au monde.

24 Renforcer la juridiction européenne par un éventail de sanctions pouvant équilibrer l'arsenal des lois à portée extraterritoriale, essentiellement d'origine américaine. Mesure urgente et indispensable au regard des enjeux de pillage économique et d'espionnage industriel.

25 Élaborer au niveau de l'UE des conditions technologiques, juridiques et fiscales, favorisant l'émergence de groupes européens de taille mondiale en cyber- et en cyber-sécurité, véritablement concurrentiels face aux GAFAM et aux BATX, et dont le capital pourrait être réparti entre différents États ou groupes privés de l'UE.

26 Œuvrer au développement d'un cadre légal national et européen pour favoriser l'émergence de solutions et d'entreprises *blockchain*, avec pour objectif de susciter des leaders mondiaux de cette technologie appelée à révolutionner nos sociétés comme l'a fait internet.

27 Étendre la réglementation RGPD aux *personnes morales* afin de protéger les entreprises européennes contre la transmission de leurs données par leurs hébergeurs à des autorités étrangères.

28 Créer un *baromètre cyber* donnant au moyen d'indicateurs nationaux la maturité et la résilience cyber de chaque pays. Élaboré au départ par un groupe d'experts, sa mise à jour ultérieure pourrait être confiée à l'Insee.

29 Négocier l'entrée de la France en tant que leader européen dans le club fermé *Five Eyes* des services de renseignement électronique anglo-saxons.

30 Ajouter une septième commission «cyber » aux six commissions existantes de l'Assemblée génerale de l'ONU pour décharger celles-ci de la part de leur travaux sur le cyber-espace et regrouper les efforts.

Pour en savoir plus

Manuels pour PME / protection des données

ANSSI 	**Renforcer la sécurité de son système d'information en 42 mesures** I - Sensibiliser et former II - Connaître le système d'information III - Authentifier et contrôler les accès IV - Sécuriser les postes V - Sécuriser le réseau VI - Sécuriser l'administration VII - Gérer le nomadisme VIII - Maintenir le système d'information à jour IX - Superviser, auditer, réagir X - Pour aller plus loin
CPME/UNAPL 	**Pourquoi sécuriser son informatique?** 1 Choisir avec soin ses mots de passe 2 Mettre à jour régulièrement vos logiciels 3 Bien connaître ses utilisateurs et ses prestataires 4 Effectuer des sauvegardes régulières 5 Sécuriser l'accès Wi-Fi de votre entreprise 6 Être aussi prudent avec son smartphone ou sa tablette qu'avec son PC 7 Protéger ses données lors de ses déplacements 8 Être prudent lors de l'utilisation de sa messagerie 9 Télécharger ses programmes sur les sites officiels des éditeurs 10 Être vigilant lors d'un paiement sur Internet 11 Séparer les usages personnels des usages professionnels 12 Prendre soin de ses informations personnelles et professionnelles
ANSSI 	**Qu'est-ce qu'une cartographie ? Réaliser une cartographie de son SI.** 1) Initier la démarche (Enjeux et parties prenantes de la cartographie ; Définir le périmètre, la cible et la trajectoire de construction) 2) Modèles à adopter 3) Outils à utiliser 4) Construction pas à pas 5) Pérenniser ma cartographie Facteurs clés de réussite
Police Nationale 	**Réagir à une attaque informatique - 10 préconisations** 1 Définir la nature de l'incident ; les infractions spécifiques aux TIC 2 Une attaque informatique a eu lieu : Démarches techniques envisageables ? 3 Mesures conservatoires à prendre au sein du SI ; à qui confier ces missions ? 4 Préserver la preuve numérique, valider son authenticité, intégrité, probité ? 5 Quels sont les moyens techniques de collecte de la preuve numérique ? 6 Vers qui se tourner pour déposer plainte et remettre les preuves collectées ? 7 Faut-il un statut particulier pour déposer plainte ? Avec quels éléments? 8 Que se passe-t-il après le dépôt de plainte ? Attentes des enquêteurs ? 9 Suites judiciaires de l'enquête ? Comment obtenir réparation du préjudice ? 10 Anticiper, prévenir ; qu'est-il possible de faire pour améliorer la sécurité du SI afin de réduire les risques et menaces ? Quelques principes de base

MANUELS POUR PMI / SYSTÈMES CONNECTÉS

CIGREF 	**CYBERSÉCURITÉ — VISUALISER, COMPRENDRE, DÉCIDER** 1. Rapport et indicateurs du tableau de bord cyber-sécurité pour le COMEX 1.1. Décrire rapidement le SI et les activités les plus exposées 1.2. Donner les éléments sur la stratégie d'ouverture du SI 1.3. Evaluer l'état de la menace - Eléments d'actualité 1.4. Identifier les terrains de vulnérabilité de l'entreprise 1.5. Mettre en place le dispositif global d'analyse et pilotage des risques cyber 1.6. Expliciter les points-clés opérationnels 2. Gouvernance, méthode et sensibilisation 2.1. Acteurs à impliquer dans la stratégie de cyber-sécurité 2.2. Gouvernance du risque cyber 2.3. Importance de l'analyse de risques 2.4. Mutualisation de la veille cyber 2.5. Sensibilisation du COMEX aux risques cyber 2.6. La question de la confiance 2.7. Le dispositif normatif dans lequel s'inscrit la cybersécurité 3. cyber-attaque majeure : quelle organisation ? 3.1. Aspects géopolitiques 3.2. Points clés pour préparer l'action : Mesures d'urgence à mettre en place
DGE 	**BONNES PRATIQUES POUR ASSURER LA SÉCURITÉ DE VOS PRODUITS CONNECTÉS :** structurer votre démarche cyber-sécurité en vous posant les bonnes questions, comprendre les dimensions à considérer en matière de sécurité, donner un panorama des solutions existantes et des différents référentiels normatifs et juridiques, informer sur les partenaires pouvant vous aider. Contexte la sécurité créatrice de valeur Pourquoi ? quelles sont les attaches et risques potentiels Do,,éespersonnelles et RGPD : les nouveaux enjeux Comment ? quelle politique de sécurité adopter. Pratique : réalisation d'objets connectés sécurisés.
ANSSI 	**AGILITÉ ET SÉCURITÉ NUMÉRIQUE** 1 À qui s'adresse ce guide ? 2 La prise en compte incrémentale du risque 3 L'atrlier d'analyse de risque A4 Le preùier atelier 5 L''appréciation des risques : les bases à connaître et à transmetre. 6 Que faire après chaque atelier ? 7 Les ateliers suivants, itération après itération 8 Se préparer à une démarche d'homologation 9 Fchés mémo ? Structurer la politique de sécurité Les clés pour identifier les risques numériques critiques ; Le canevas de l'analyse de risque ; Un exemple complet
CNIL 	**ANALYSE D'IMPACT (RGPD) : LES OBJETS CONNECTÉS** 1 Étude du contexte : *Vue d'ensemble du traitement ; Données, processus et supports* 2 Étude des principes fondamentaux : *Mesures garantissant la proportionnalité et la nécessité du traitement ; Mesures protectrices des droits des personnes des personnes concernées; Évaluation du respect des principes fondamentaux* 3 Étude des risques liés à la sécurité des données : *Évaluation des mesures existantes ou prévues ; Appréciation des risques : les atteintes potentielles à la vie privée* 4 Validation du PIA : *Préparation des éléments utiles à la validation ; Validation formelle* Annexes : Mesures de minimisation des données ; Sources de risques ; Échelle de gravité et exemples d'impacts ; Échelle de vraisemblance et exemples de menaces ; Échelles pour le plan d'action ; Typologie d'objectifs pour traiter les risques

Nicol… Bail *Frantz Rublé*
Prés… Directeur général *Président*
Créd… Mutuel Alliance Fédérale *Euro-Information*

Manuels pour ETI / Fonctions impliquées dans la Gestion des risques

CEIDIG 	**L'essentiel de la sécurité numérique pour les dirigeants** 1) MIEUX COMPRENDRE LA RÉALITÉ DU RISQUE AUJOURD'HUI Qui est concerné ? Qui peut être ciblé ? Les principales menaces actuelles Des attaquants aux motivations multiples, Des attaques tous azimuts, Retour sur l'attaque de TV5 Monde, Lexique indispensable En France, l'État aussi s'organise et se dote de forces cyber 2) PROTÉGER SON ENTREPRISE : REPÈRES ET CONSEILS ESSENTIELS Les points clés : 10 questions pour mieux appréhender la cyber-sécurité Quelle organisation ? Comment définir le bon budget ? Quel tableau de bord ? Quels indicateurs suivre ? Point juridique flash 10 bons gestes pour se protéger 3) ZOOM SUR DES ENTREPRISES ET DES EXPERTS FRANÇAIS Les 10 conseils du CESIN pour appréhender le Cloud Sites utiles ; Les organismes qui peuvent vous aider Quiz
ANSSI 	**Bonnes pratiques à l'usage des professionnels en déplacement** (version 2019 du Passeport de conseil aux voyageurs) 9 bonnes pratiques de sécurité numérique, illustrées par l'exemple, à suivre AVANT, PENDANT et APRES un voyage
AMRAE 	**Maîtrise du risque numérique** COMPRENDRE LE RISQUE NUMÉRIQUE ET S'ORGANISER : (1) Définir un cadre de gouvernance du risque numérique (2) Comprendre son activité numérique (3) Connaître son seuil d'acceptation des risques (4) Construire ses pires scénarios de risque (5) Définir sa stratégie de sécurité numérique et de valorisation (6) Mettre en place des polices d'assurance adaptées BÂTIR SON SOCLE DE SÉCURITÉ (7) Placer l'humain au centre du jeu (8) Homologuer ses services numériques critiques (9) Bâtir sa protection (10) Orienter sa défense et anticiper sa réaction (11) Faire preuve de résilience en cas de cyberattaque PILOTER SON RISQUE NUMÉRIQUE ET VALORISER SA cyber-SÉCURITÉ : (12) Connaissance : de la veille à l'analyse (13) Engagement : de l'adhésion à l'action (14) Agilité : l'amélioration continue et la performance (15) Valorisation : la cyber-sécurité, un avantage compétitif BIBLIOGRAPHIE
FFA 	**Anticiper et minimiser l'impact d'un cyber risque sur votre entreprise** 04 Et si cela vous arrivait… 05 En quoi suis-je concerné ? 06 Protéger mon entreprise. 10 Assurer mon entreprise. 14 Que faire vis-à-vis de mon assureur ? 15 Que faire en cas d'incident informatique ? 18 Les questions fréquentes

Manuels pour experts (Gestion des risques numériques ; RGPD)

ANSSI	**EBIOS[9] RISK MANAGER (MÉTHODE D'APPRÉCIATION ET DE TRAITEMENT DES RISQUES NUMÉRIQUES)** qu'est-ce que la méthode ebios risk manager une démarche itérative en 5 ateliers différents états-unisges d'ebios risk manager atelier 1 – cadrage et socle de sécurité atelier 2 – sources de risque atelier 3 – scénarios stratégiques atelier 4 – scénarios opérationnels atelier 5 – traitement du risque bibliographie termes et définitions + fiches pratiques
AFAI / CIGREF 	**CIGREF – ENTREPRISE — LES CLÉS D'UNE APPLICATION RÉUSSIE DU RGPD** La protection des données personnelles: un double enjeu sociétal et économique «DPSI», une initiative pour accompagner les entreprises dans leur mise en conformité CHECK-LIST GDPR Quel est l'objectif de lacheck-list ? Démarche proposée ; Check-list GDPR RECOMMANDATIONS ET MESURES À METTRE EN PLACE POUR UN SI CONFORME Identifier les mesures à mettre en place pour un SI conforme ; Mesures potentiellement applicables sur les SI ; Mesures applicables pour se protéger des risques identifiés ; Illustration concrète de l'approche par le cas CRM MODE D'EMPLOI ET OUTILS DE CONFORMITE AVEC LE CADRE LEGISLATIF ET REGLEMENTAIRE Les outils de gouvernance ; Les principaux outils de confiance vis-à-vis des tiers et la présomption de conformité ; Les outils contractuels et les responsabilités ; Cas pratiques et exemples de clauses
CNIL 	**ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES** 1 Étude du contexte 1.1 Vue d'ensemble : Traitements considérés ; Référentiels applicables au traitement 1.2 Données, destinataires et durées de conservation ; Processus et supports 2 Étude des principes fondamentaux 2.1 Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement 2.2 Évaluation des mesures protectrices des droits des personnes 3 Étude des risques liés à la sécurité des données 3.1 Description et évaluation des mesures contribuant à traiter des risques liés à la sécurité des données (art.32), des mesures générales de sécurité et de gouvernance 3.2 Appréciation des risques « les atteintes potentielles à la vie privée » : Analyse et estimation des risques ; Évaluation des risques 4 Validation du PIA 4.1 Préparation des éléments utiles à la validation : synthèses relatives à la conformité [RGPD], aux bonnes pratiques liées à la sécurité des données, de la cartographie des risques, du plan d'action, Formalisation du conseil du DPO et de l'avis des personnes concernées 4.2 Validation formelle

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

L'ATELIER RGPD

https://www.cnil.fr/fr/PIA-privacy-impact-assessment

FUN MOOC CNAM Protection des données personnelles : le nouveau droit

RÉFÉRENCES DS DOCUMENTS CITÉS

Manuels pour PME / protection des données

https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique
/https://www.ssi.gouv.fr/particulier/guide/cartographie-du-systeme-dinformation/
https://www.interieur.gouv.fr/content/download/92418/720038/file/2016-10-preconisations-face-cybercriminalite.pdf

Manuels pour PMI / Systèmes connectés

https://www.cigref.fr/publication-cybersecurite-visualiser-comprendre-decider
https://www.captronic.fr/Sortie-du-guide-Cybersecurite-des-produits-connectes-a-destination-des-PME.html
https://www.ssi.gouv.fr/uploads/2018/11/guide-securite-numerique-agile-anssi-pa-v1.pdf
https://www.cnil.fr/fr/guides-aipd

Manuels pour ETI / Fonctions impliquées dans la Gestion des risques

https://www.amazon.fr/Lessentiel-s%C3%A9curit%C3%A9-num%C3%A9rique-pour-dirigeants-ebook/dp/B06X959GGD
https://www.ssi.gouv.fr/entreprise/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/
https://www.ssi.gouv.fr/actualite/confiance-numerique-lanssi-et-lamrae-publient-un-guide-sur-la-maitrise-du-risque-numerique-pour-les-dirigeants/
https://www.ffa-assurance.fr/infos-assures/anticiper-et-minimiser-impact-un-cyber-risque-sur-votre-entreprise-entreprises
https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/
https://www.cpme.fr/publications/guides/guide-des-bonnes-pratiques-de-linformatique

Manuels pour experts (Gestion des risques numériques ; RGPD)

https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/
https://www.cigref.fr/entreprise-cle-application-reussie-gdpr-livrable-cigref-afai-tech-in-france
https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd

Postface

« Respectueux de la vie privée de chacun, nous mettons la technologie et l'innovation au service de l'humain » : telle est une des missions que s'est fixée Crédit Mutuel Alliance Fédérale pour son futur statut d'entreprise à mission.

C'est à la lumière de cet engagement que nous sommes fiers de contribuer à la publication de ce livre blanc, fruit des travaux de la Commission cyberstratégie de l'UNION-IHEDN. Associant analyse rigoureuse et recommandations opérationnelles, il met bien en lumière les menaces et les enjeux de notre Monde Digital.

Bancassureur de premier plan en France et en Europe, présent au travers de près de 4 400 points de vente du Crédit Mutuel et du CIC au service de 26,3 millions de clients, Crédit Mutuel Alliance Fédérale propose une offre diversifiée de services à une clientèle de particuliers, de professionnels de proximité et entreprises de toutes tailles. Banque relationnelle de référence, il est ainsi un acteur engagé pour le développement de tous les territoires.

Les bénéfices de la digitalisation, confirmés lors de la crise sanitaire, ont permis aux sociétaires et clients de continuer à bénéficier des services et des conseils grâce à une offre de services bancassurances à distance et à une relation personnalisée avec leur chargé de clientèle.

Toutefois, dans ce Monde Digital où les menaces et la cybercriminalité se développent, Crédit Mutuel Alliance Fédérale a également la mission d'assurer la protection des données.

Alors que certaines entreprises ont construit leur modèle d'affaires autour de la collecte, de la valorisation et de l'exploitation des données à des fins commerciales, Crédit Mutuel Alliance Fédérale a fait un choix contraire, celui d'un usage respectueux de l'intimité numérique de ses clients.

L'économie numérique collecte, traite et structure un volume considérable d'informations sur les individus : habitudes de consommation, préférences, loisirs, déplacements, modes de transport, liens familiaux, associatifs, communautaires, profession, formation, données de santé, etc. Ces informations concernent l'identité de l'individu, sa vie privée et, pour certaines, son intimité.

En ce qui nous concerne, nous considérons que la connaissance du client doit servir exclusivement à lui apporter le service dont il a besoin, dans le cadre d'une relation de proximité et d'un pacte relationnel de confiance.

Nos développements informatiques respectent le principe de protection de la vie privée par conception et par défaut. Nos engagements sont clairement formalisés et publiés sur nos sites internet et adressés au client au moment de l'entrée en relation. Les droits du client lui sont exposés et des procédures internes ont été publiées pour en assurer l'effectivité, avec l'élaboration d'une politique des durées de conservation. La prospection commerciale s'appuie expressément sur le consentement du client.

Dans le cadre de notre plan stratégique, nous avons engagé des investissements très importants pour construire de nouvelles salles informatiques, disposant des exigences de continuité d'activité et de sécurité les plus avancées. Ce choix de développer notre Système d'Information avec un recours limité à la sous-traitance et une culture de l'expertise interne, mais aussi de construire et opérer nos architectures informatiques dans nos propres bâtiments, sans recourir au Cloud Public, nous apporte une nécessaire souveraineté, tout en disposant des dernières technologies disponibles via un Cloud privé. C'est un investissement très important, mais indispensable.

Deux exemples concrets : les échanges entre le chargé de clientèle et son client se font via des canaux sécurisés et maîtrisés : messagerie intégrée à la plateforme de banque à distance, hébergée en interne, avec des données stockées en interne, sans recours à des courriels publics, des sites de transfert de fichier dans le Cloud… Les rendez-vous en visioconférence sont réalisés sur nos plateformes techniques, via des logiciels installés dans nos Datacenters et non dans le Cloud public.

Les nouvelles technologies sont essentielles mais créent aussi des dépendances : nous avons besoin d'être connectés, à Internet, à nos clients par les différents canaux relationnels établis, à nos partenaires, à nos confrères, aux régulateurs, etc. D'où la priorité donnée à la sécurisation cyber avec l'acquisition et la mise en œuvre d'infrastructures techniques et de logiciels pour améliorer continuellement notre niveau de protection, le recrutement de nouveaux talents, la formation et l'information de nos équipes sur les techniques et menaces. Et, bien entendu, la collaboration avec des acteurs majeurs au niveau national et européen à travers des organismes de référence comme l'ANSSI ou les différents CERT privés et publics, permet de lutter contre ces menaces.

La cybersécurité est un choix collectif. Pour ce qui concerne le Crédit Mutuel Alliance Fédérale, le choix est clair : sécurité des systèmes et protection de l'intimité numérique des clients vont de pair.

Nicolas Théry
Président
Crédit Mutuel Alliance Fédérale

Daniel Baal
Directeur général
Crédit Mutuel Alliance Fédérale

Frantz Rublé
Président
Euro-Information

UNE BANQUE QUI APPARTIENT À SES CLIENTS, ÇA CHANGE TOUT.

Bancassureur de premier plan en France, présent au travers de près de 4 400 points de vente au service de 26,3 millions de clients, Crédit Mutuel Alliance Fédérale propose une offre diversifiée de services à une clientèle de particuliers, de professionnels de proximité et entreprises de toutes tailles.
Plus d'informations sur *creditmutuel.fr.*

Crédit Mutuel Alliance Fédérale regroupe les fédérations Centre Est Europe (Strasbourg), Sud-Est (Lyon), Ile-de-France (Paris), Savoie-Mont Blanc (Annecy), Midi-Atlantique (Toulouse), Loire-Atlantique et Centre-Ouest (Nantes), Centre (Orléans), Normandie (Caen), Dauphiné-Vivarais (Valence), Méditerranéen (Marseille), Anjou (Angers), Massif Central (Clermont-Ferrand) et Antilles-Guyane (Fort de France). Crédit Mutuel Alliance Fédérale regroupe également la Caisse Fédérale de Crédit Mutuel, la Banque Fédérative du Crédit Mutuel (BFCM) et l'ensemble de ses filiales, notamment le CIC, Euro-Information, les Assurances du Crédit Mutuel (ACM), Targobank, Cofidis, la Banque Européenne du Crédit Mutuel (BECM), la Banque Transatlantique, Homiris et CIC Iberbanco.

Crédit Mutuel
Alliance Fédérale

Le Crédit Mutuel, banque coopérative, appartient à ses 8 millions de clients-sociétaires.
Caisse Fédérale de Crédit Mutuel - RCS Strasbourg B 588 505 354.