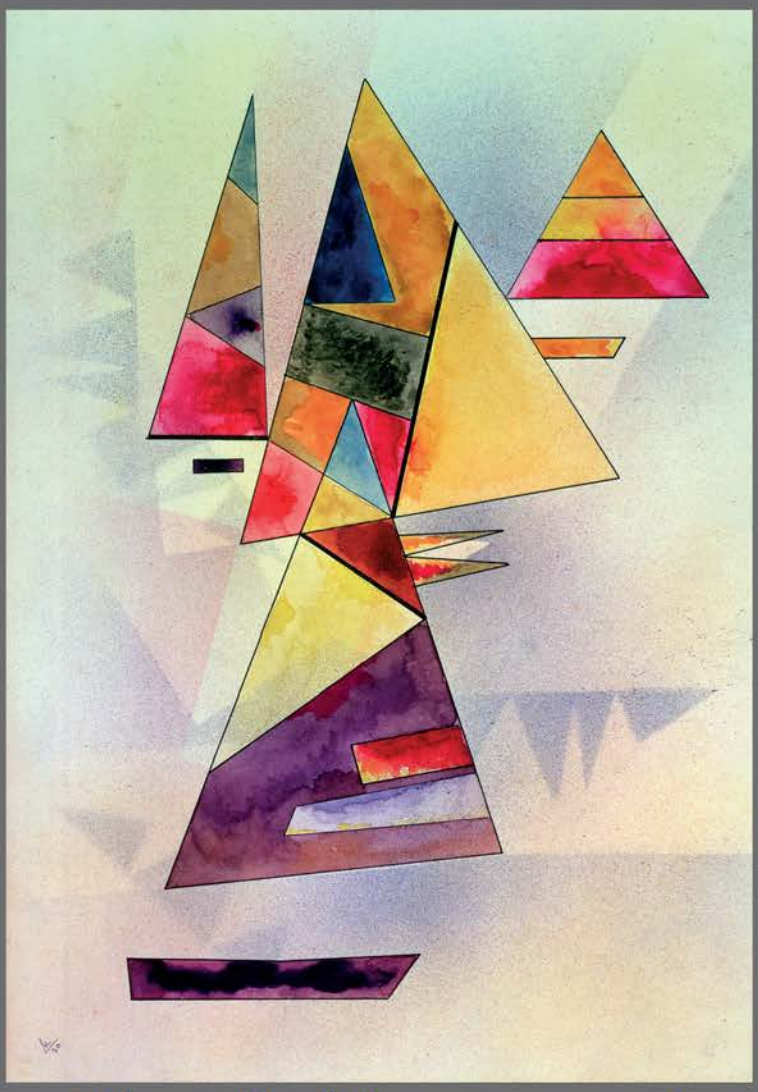
Enjeux numériques



Répondre à la menace cyber

UNE SÉRIE DES
ANNALES DES MINES
FONDÉES EN 1794

N° 8 - DÉCEMBRE 2019

Publié avec le soutien de l'Institut MinesTélécom

UNE SÉRIE DES
ANNALES DES MINES
FONDÉES EN 1794

ENJEUX NUMÉRIQUES

Série trimestrielle • N°8 - Décembre 2019

Rédaction
Conseil général de l'Économie,
ministère de l'Économie et des Finances
120, rue de Bercy - Télédoc 797
75572 PARIS Cedex 12
Tél. : 01 53 18 52 68
http://www.annales.org

François Valérian
Rédacteur en chef

Gérard Comby
Secrétaire général

Delphine Mantienne
Secrétaire générale adjointe

Liliane Crapanzano
Correctrice

Myriam Michaux
Webmestre et maquettiste

Photo de couverture :
Wassily Kandinsky (1866-1944),
Composition. Aquarelle et encre de Chine,
1930. Collection particulière.
Photo © BRIDGEMAN IMAGES

Iconographie
Christine de Coninck

Abonnements et ventes
COM & COM
Bâtiment Copernic - 20, avenue Édouard-Herriot
92350 LE PLESSIS-ROBINSON
Alain Bruel
Tél. : 01 40 94 22 22 - Fax : 01 40 94 22 32
a.bruel@cometcom.fr

Mise en page : Nadine Namer
Impression : Printcorp
N° ISSN : 2607-9984
Éditeur délégué :
FFE – 15, rue des Sablons - 75116 PARIS -
www.ffe.fr

Régie publicitaire : Belvédère Com
Fabrication : Aïda Pereira
aida.pereira@belvederecom.fr
Tél. : 01 53 36 20 46
Directeur de la publicité : Bruno Slama
Tél. : 01 40 09 66 17
bruno.slama@belvederecom.fr

Répondre à la menace cyber

04 Introduction
Côme BERBAIN

État de la menace

06 Le modèle français de cybersécurité : priorité à la défense
Guillaume POUPARD

11 La cybersécurité sort (enfin) de son ghetto technique
Nicolas ARPAGIAN

18 Que cherchent les hackers ?
Julie GOMMES

25 La sensibilisation : une arme défensive majeure
Jérôme NOTIN

29 Cyberdéfense : l'humain au cœur de l'efficacité opérationnelle
Vincent RIOU

33 Prévenir et détecter
Jacques DE LA RIVIÈRE

Les réponses publiques et privées

38 Souveraineté numérique et sécurité nationale
Claire LANDAIS et Julien BARNU

42 Protection des infrastructures critiques : 5 ans après la loi
Yves VERHOEVEN

47 Retour sur la genèse de la cyberdéfense militaire
Didier TISSEYRE

52 Nouveaux rôle et enjeux pour l'Etat dans la lutte contre la cybercriminalité
Thierry DELVILLE

57 À la poursuite des cyber-criminels
Jacques MARTINON

63 Innovation et startups cybersécurité en France : le début de l'embellie ?
Gérôme BILLOIS et Jules HADDAD

71 Le RGPD au service de la cybersécurité
Jean LESSI

75 Une agence au cœur de la cybersécurité européenne
Jean-Baptiste DEMAISON

80 Le cyber en assurance, un risque presque comme les autres ?
Benjamin DUCOS et Luc DE LIGNIÈRES

De nouveaux enjeux techniques comme politiques

88 Défis de la recherche scientifique en cybersécurité
Claude KIRCHNER et Ludovic MÉ

100 La confiance numérique, une condition *sine qua non* du succès de l'adoption du *cloud*
Marc DARMON et Olivier KERMAGORET

106 L'Internet des Objets modifie la cybersécurité : l'exemple de Linky
Hervé CHAMPENOIS

110 Quelle régulation pour les acteurs privés dans le cyberespace ?
Florian ESCUDIÉ

Hors dossier

115 Concurrence et numérique : entretien avec Bernard Benhamou
Propos recueillis par Jean-Pierre DARDAYROL et Delphine MANTIENNE

121 Vers une école du *risque numérique* ?
Jean-François CÉCI

132 Résumés
139 Abstracts
145 Contributeurs

Ce numéro est coordonné par Côme BERBAIN.

Introduction
Répondre à la menace cyber

Par **Côme BERBAIN**
Directeur de l'innovation et du véhicule autonome,
RATP

La vision commune de la menace cyber est aujourd'hui largement déformée. Hollywood s'est emparé il y a de nombreuses années du personnage du hacker : jeune homme blanc en sweat à capuche capable, à l'aide d'outils semi-magiques de contrôler les machines et de plonger le monde dans l'apocalypse, en arrêtant la production d'énergie d'un pays, en effaçant les données des banques ou en diffusant massivement de fausses informations. Dénué de la moindre conscience de ses actes, il est le plus souvent manipulé par un autre personnage, finalement plus humain car ses intentions sont plus compréhensibles.

Rien n'est à la fois plus loin de la réalité en ce qui concerne les intentions et les méthodes, et plus réaliste dans les conséquences potentielles. La transformation numérique à l'œuvre rend nos vies et nos sociétés dépendantes de données et de systèmes informatiques de plus en plus connectés et de plus en plus ouverts : que l'on pense aux comptes bancaires, aux hôpitaux dont les ordinateurs contiennent la seule trace de la liste des traitements à fournir chaque jour aux patients ou à la ville dont l'ensemble de l'éclairage est pilotable depuis un smartphone. Cette ouverture est source d'innovations qui font évoluer conjointement les technologies et les usages, eux-mêmes générateurs de nouvelles innovations dans des cycles rapides liés à la compétition internationale des États et des entreprises. Cette vitesse laisse bien peu de place à la maturation des technologies et à la compréhension fine des enjeux, ce qui pose un défi permanent en termes de régulation et de sécurité.

La sécurité de ce nouveau monde n'est pas une problématique entièrement nouvelle : elle s'inscrit au croisement des traditions historiques de la sécurité de l'information et des transmissions, du contre-espionnage et de la contrepropagande. Elle prend cependant une importance particulière en raison de l'étendue du champ d'action, de l'immaturité de la très grande majorité des entités publiques ou privées aussi bien sur les aspects techniques qu'organisationnels, et de la grande accessibilité des techniques offensives.

La cybersécurité, dont il est question dans ce numéro, est une des composantes de cette sécurité numérique. Elle s'attache à protéger les données et les systèmes d'information, à garantir leur confidentialité, leur intégrité, leur authenticité et leur disponibilité. Bien que reposant sur un substrat technique, elle intègre également les aspects humains, aussi bien individuels que collectifs. Il est fréquent d'entendre que la principale vulnérabilité d'un système informatique se trouve « entre la chaise et le clavier ».

Elle diffère néanmoins de la question de la protection des données personnelles ou de la manipulation des algorithmes ou des informations : la collecte illicite de données n'implique pas nécessairement la violation d'un système d'information particulier ; la diffusion de fausses informations sur un réseau social tel que Twitter relève du fonctionnement normal de ce réseau et ne nécessite pas d'attaquer les serveurs de Twitter. Cependant, ces questions ne sont pas sans liens et ces dernières années ont vu apparaître des attaques combinées d'une grande sophistication.

Ce numéro vise à présenter l'état de la réflexion et des évolutions en cours en matière de cybersécurité, au plus proche du terrain et des acteurs qui la pratiquent au quotidien, et bien loin des visions romancées. Il cherche à donner des clés de compréhension concrètes et des leviers actionnables aussi bien pour le citoyen, l'employé ou le décideur autour de plusieurs dimensions :

- « Voir et comprendre ». Il est difficile de se défendre contre un ennemi invisible. Si la médiatisation des attaques progresse autour de quelques cas emblématiques (TV5monde, Saint-Gobain, Airbus…), la majorité des victimes recherche la discrétion. La détection d'attaques reste l'indispensable première étape de la cybersécurité. Il est également nécessaire de comprendre la diversité des motivations, de la cybercriminalité des groupes mafieux aux actions prêtées aux Etats, ainsi que le caractère aussi bien local que systémique, de l'attaque ciblée d'un individu aux scénarios d'« ouragans cyber ».
- Le nécessaire équilibre entre prévention et réaction : à partir de la prise de conscience de la menace réelle, la tentation principale consiste à focaliser ses moyens sur la réaction, d'autant plus qu'il s'agit d'activités valorisantes. Cependant, à l'instar des risques incendies ou des risques industriels, ce seul travail ne peut suffire. Le long travail de standardisation et de certification des solutions, de sensibilisation et de formation des acteurs, et d'organisation et de régulation de l'écosystème, est nécessaire pour éviter que les « pompiers » cyber ne s'épuisent dans une course où l'attaquant possède toujours l'initiative et un avantage naturel, détruire étant toujours plus simple que construire ou réparer.
- Le dépassement de la technique : la complexité technique du sujet ne doit pas cacher les enjeux et les problématiques non techniques. Déjà entamée ces dernières années, l'intégration des questions de formation, d'organisation et de régulation doit venir se compléter de réflexions plus globales sur le rôle des États, la responsabilité des principaux acteurs numériques, les comportements des acteurs privés, les modalités et les périmètres de la régulation, ou encore l'adaptation à la cybersécurité d'activités existantes comme la justice.

Pour cela, ce numéro expose en premier lieu l'état de la menace, les motivations des acteurs et les enjeux de la détection, avant de présenter la palette de réponses possibles apportées aussi bien par le secteur public (État, Union européenne) que par le secteur privé. Compte tenu de l'enjeu de sécurité, l'État a naturellement investi le champ de la cybersécurité, aussi bien pour apporter une réponse aux attaques les plus importantes que pour fixer aux niveaux national et européen le cadre de la régulation des activités les plus essentielles au fonctionnement de notre société, ainsi que pour ses besoins propres. Aidé par quelques exemples fameux d'attaques qui sont aujourd'hui de plus en plus médiatisées, ce cadre a permis le développement du secteur privé, aussi bien dans les startups que dans les grands groupes, sous forme de produits, de services ou d'assurances. Dans ce domaine, la France reste dans la course mondiale et participe activement à la définition des cadres européens dont les détails auront des impacts de long terme sur la compétitivité de notre industrie.

Enfin, ce numéro évoquera les nouveaux enjeux de la cybersécurité : des défis techniques apportés par l'intelligence artificielle, le *cloud* ou les objets connectés mais aussi les défis de régulation des comportements des grands acteurs numériques ou des États.

Très bonne lecture !

Le modèle français de cybersécurité : priorité à la défense

Par **Guillaume POUPARD**
Agence nationale de la Sécurité des Systèmes d'information (ANSSI)

L'année 2019 marque la dixième année d'existence de l'Agence nationale de la Sécurité des Systèmes d'Information, l'ANSSI. Dix ans qui ont contribué à implanter durablement l'Agence dans l'écosystème français, européen et international de la cybersécurité. Dix ans aussi durant lesquels la menace numérique n'a cessé de croître, de s'adapter pour se faire toujours plus présente. Dix ans, enfin, qui ont permis de confirmer la pertinence du modèle français et le choix, audacieux, de ne pas cantonner la cybersécurité à un secteur tout en séparant strictement les activités défensives, confiées à l'ANSSI, des activités cyberoffensives.

Plus de dix ans après l'impulsion initiale, la cybersécurité est devenue une priorité stratégique majeure pour de nombreux États. C'est ainsi qu'on assiste, au niveau mondial, à la consolidation d'un « premier cercle » de puissances cyber, composé sans surprise des États-Unis, du Royaume-Uni, de la Chine, de la Russie et d'Israël. La dimension numérique est désormais pleinement intégrée dans les stratégies d'influence, d'ingérence ou de découragement des puissances étrangères. Le cyberespace est marqué par une montée des tensions, donnant lieu à une instabilité croissante, servies par des stratégies résolument offensives et, parfois, à visées hégémoniques.

Dans ce contexte, la France demeure une puissance cyber. Sa stratégie audacieuse lui a permis de rapidement développer des capacités autonomes. Elle reste l'une des rares nations capables de faire entendre une voix indépendante, équilibrée et forte, dans les instances européennes et internationales.

Cette place singulière tient pour beaucoup à son modèle d'organisation, qui nous a permis d'accompagner l'évolution de la menace tout en rendant possible le déploiement d'une véritable politique publique de la cybersécurité, condition d'une transformation numérique en confiance.

Une menace en constante évolution

C'est le quotidien du défenseur – plus généralement de quiconque évolue dans la gestion des risques – que d'être perçu comme un empêcheur de tourner en rond. On lui demande parfois d'arrêter de jouer les Cassandre (oubliant par ailleurs que celle-ci ne se trompait jamais). On lui reproche parfois de noircir le tableau ou de verser dans le catastrophisme pour précipiter une prise de conscience, voire justifier sa raison d'existence. Mais si le défenseur est condamné à parler au conditionnel, c'est bien pour ne pas avoir à parler au passé.

Nul besoin de grossir le trait en effet : l'activité de l'ANSSI ne cesse de démontrer que la menace numérique est tout sauf virtuelle, que les défis pour la sécurité du cyberespace restent immenses. Pour cause : la menace numérique est entrée dans une dimension nouvelle. Les attaques informatiques sont plus sophistiquées, mieux élaborées, plus destructrices. Elles touchent désormais toute la société, du citoyen à la grande entreprise jusqu'à nos institutions démocratiques. À la faveur d'une explosion des usages et d'une externalisation toujours plus importante, la surface d'attaque ne cesse d'augmenter, sans que cela ne se traduise mécaniquement par un accroissement de la sécurité – loin s'en faut.

Une recrudescence des attaques « par rebond »

Dans un environnement globalisé, synchronisé, externalisé, dans lequel les flux sont devenus tout aussi physiques que numériques, l'interdépendance croissante des acteurs expose chacun d'entre eux à la défaillance d'un des membres de leur écosystème. En cela, la *supply chain* – comprendre les liens de sous-traitance et d'externalisation entre les acteurs – constitue tout à la fois un puissant moteur de performance pour les entreprises et les administrations, mais également un véritable défi pour la sécurité du numérique.

Les attaquants l'ont bien compris. Ils exploitent désormais cette fragilité à leur profit, visant d'abord les prestataires d'entreprises pour atteindre leurs cibles principales. Cette tendance, particulièrement prégnante ces derniers mois, concerne notamment les entreprises de services du numérique (ESN) mais également un grand nombre de prestataires. Ces modes opératoires compliquent la mission du défenseur, qui doit surmonter les difficultés techniques et réglementaires induites par la nature de ces victimes et leur envergure souvent internationale.

Le risque (presque) nouveau du sabotage

En plus de l'espionnage numérique, qui continue de mobiliser une partie significative des ressources de l'ANSSI, les derniers mois ont été marqués par une menace nouvelle – pas tant par sa nature que par son impact potentiel : la menace du sabotage. Les conséquences humaines et économiques d'attaques de grande ampleur ou judicieusement ciblées pourraient en effet s'avérer catastrophiques. Imaginez : si vous coupez les transports en commun d'une capitale, toute l'activité économique du pays concerné pourrait être paralysée en quelques heures. Si, du jour au lendemain, les distributeurs de billets ne distribuent plus de billets, il y a fort à parier que cela donnerait lieu à d'importants troubles à l'ordre public.

Plus préoccupant encore : les infrastructures sensibles ou critiques semblent être de plus en plus ciblées par des actions de cartographie et de prépositionnement. Qu'il s'agisse d'États ou d'organisations criminelles, les attaquants s'attachent aujourd'hui à préparer les conflits ou les actions criminelles de demain. Ces attaques, dont les objectifs demeurent encore flous, pourraient constituer des opérations de reconnaissance en vue de préparer des actions de sabotage futures. Cette menace se fait plus prégnante à mesure que le contexte géopolitique se fait de plus en plus incertain.

Une prolifération des armes numériques et des vulnérabilités

La prolifération d'armes numériques et la divulgation de vulnérabilités informatiques, logicielles ou matérielles, favorisent la montée en compétence des attaquants. C'est ce qui a permis le franchissement d'un nouveau cap en 2017, avec des attaques inédites en termes d'échelle et de nocivité.

En paralysant de nombreuses entreprises, grandes et petites, mais également des acteurs comme des services hospitaliers, les attaques *WannaCry* et *NotPetya* ont démontré qu'il était possible de porter des atteintes considérables à des intérêts nationaux, sans pour autant que des infrastructures critiques soient forcément touchées. Elles obligent le défenseur à toujours élargir son périmètre de supervision, pour tenir compte d'une plus grande variété de victimes et d'attaquants. En outre, le réemploi d'outils malveillants favorise l'anonymat et complique le travail déjà délicat d'attribution par les services compétents. Les découvertes de failles critiques, matérielles ou logicielles, parfois médiatisées avant l'application de correctifs, offrent enfin aux attaquants de nouvelles possibilités d'agression plus massives et plus discrètes.

Des attaques de plus en plus lucratives

De plus en plus d'attaques ont pour finalité l'enrichissement des attaquants. Ceux-ci profitent en particulier des failles de sécurité pour compromettre un grand nombre d'équipements par le dépôt discret de « mineurs ». Il devient alors possible de se servir clandestinement de la puissance de calcul cumulée de ces systèmes pour générer des actifs de cryptomonnaies.

La préoccupation croissante des organisations à l'égard des enjeux de sécurité numérique et le renforcement parallèle de leurs capacités de défense amènent par ailleurs nombre d'attaquants à se tourner vers des cibles moins exposées, mais plus vulnérables. Ainsi, de nombreuses campagnes d'hameçonnage ciblant des collectivités territoriales ou des acteurs du secteur de la santé sont observées depuis 2018. Les objectifs de ces campagnes sont multiples mais comprennent généralement le vol de données personnelles, la demande de paiement d'une rançon après chiffrement des données, le minage de cryptomonnaies et la constitution de réseaux de machines zombies (*botnets*).

Face à cet accroissement de la menace, l'intuition stratégique française était la bonne

Cette évolution du risque numérique teste en permanence la résilience et la solidité de notre modèle de protection. Ce modèle s'organise autour d'une stricte séparation entre les activités cyberoffensives et les activités dédiées à la sécurité numérique –ces dernières étant en large partie confiées à l'ANSSI, autorité nationale à portée interministérielle.

Aux origines du modèle français

Le modèle français de cybersécurité est le résultat d'une succession de choix politiques ambitieux issus d'une prise de conscience : la transformation numérique de la société, de l'économie et de l'action publique devra se faire en confiance, ou elle ne se fera pas.

Quelques mois après l'attaque informatique majeure – la première du genre – ayant paralysé l'Estonie pendant plusieurs semaines [(1)], le *Livre blanc sur la défense et la sécurité nationale* de 2008 aboutissait à la création, en 2009, de l'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI), dans une visée strictement défensive et interministérielle. Cette création préfigurait un modèle original d'organisation nationale de cybersécurité, capable d'en accompagner les différents aspects.

En 2013, le nouveau *Livre blanc sur la défense et la sécurité nationale* élargissait le champ d'action de l'Agence aux acteurs privés les plus sensibles et stratégiques, dits « opérateurs d'importance vitale » (OIV). La *Stratégie nationale pour la sécurité du numérique* présentée publiquement par le Premier ministre en 2015 confirmait quant à elle l'ambition de porter une politique publique globale de la cybersécurité et de s'adresser au reste de la société, notamment les citoyens.

Enfin, les travaux stratégiques conduits en 2018 ont permis de réaliser un saut qualitatif important dans la gouvernance et le pilotage des activités de réponse aux attaques informatiques, notamment les plus sensibles. Ils ont en particulier permis d'expliciter les rôles des – désormais nombreux – acteurs institutionnels qui interviennent dans le champ de la sécurité numérique.

(1) L'attaque contre l'Estonie a en effet paralysé des activités essentielles au fonctionnement de ce pays pendant plusieurs semaines : s'appuyant sur la technique du DDoS, l'offensive a bloqué des sites Internet gouvernementaux ainsi que des médias, des partis politiques et des activités bancaires. Le gouvernement estonien avait alors accusé la Russie d'être à l'origine de l'attaque. Cette attaque a largement précipité une prise de conscience mondiale sur le risque numérique.

Contre-modèles

L'effort français en matière de cybersécurité s'inscrit dans une dynamique de développement capacitaire et de réflexion stratégique que l'on retrouve chez les autres principales puissances cyber. Ces dynamiques ont donné lieu à des organisations parfois très distinctes – le reflet d'autant de stratégies et de doctrines propres à chaque État. Certains pays, essentiellement guidés par des considérations pratiques et d'efficacité technique, tendent ainsi à regrouper les capacités défensives et offensives au sein de leurs appareils de défense ou de renseignement. C'est le cas, par exemple, des États-Unis. Le modèle américain présente l'avantage de mutualiser les compétences techniques nationales au sein d'un même pôle d'expertise, en l'espèce la *NSA*. Il pose cependant la question de l'acceptabilité, par le secteur privé, des interventions de l'État en matière de cybersécurité.

Par ailleurs, la concentration des capacités au sein des appareils militaires ou de renseignement peut rapidement déboucher sur une inclinaison naturelle à privilégier les aspects offensifs. Prenons l'exemple de la gestion des failles informatiques, qui sont recherchées par « le défenseur » à des fins de correction et par « l'attaquant » à des fins d'exploitation. La valeur de ces vulnérabilités ne cesse d'augmenter et le marché mondial connaît actuellement une forte inflation. Lorsque l'attaquant et le défenseur sont la même personne, on conçoit bien naturellement qu'il puisse être difficile de renoncer à un tel actif stratégique.

Enfin, faute de dispositif global de cybersécurité, certains pays en sont presque contraints à attaquer pour se défendre, de manière à neutraliser la menace à sa source, dans une forme de « fuite en avant » qui se traduit par des stratégies offensives préjudiciables à la stabilité du cyberespace.

Avantages du modèle français

Un peu plus de dix années après l'intuition initiale, le modèle français confirme toute sa pertinence. Mieux, il continue d'essaimer : des pays aussi divers que le Japon, Singapour, la Belgique ou Israël s'en inspirent parfois explicitement pour construire ou reconstruire leurs propres gouvernances.

Du point de vue de l'ANSSI, il présente en effet quelques indéniables avantages. À la différence d'un service de renseignement, le périmètre strictement défensif de l'Agence lui permet d'afficher une posture non ambiguë devant ses interlocuteurs, qu'il s'agisse d'entreprises ou d'administrations victimes, d'assemblées parlementaires, de chercheurs, de médias ou encore d'industriels. Ce modèle a rendu possible l'élaboration de législations très ambitieuses – souvent pionnières. Il en va ainsi du dispositif réglementaire de sécurisation des activités d'importance vitale, qui nous est envié (officieusement) par nombre de pays étrangers. Les récentes évolutions législatives ont également permis d'accroître significativement les capacités de détection de l'ANSSI ; elles sont également rendues possibles par ce modèle protecteur et rassurant.

D'autres pays ont cherché à élaborer un cadre contraignant pour leurs acteurs privés. À l'instar des États-Unis ou de la Russie, ces initiatives se sont souvent soldées par des échecs, les entreprises rechignant à collaborer activement avec les services de renseignement. Autre caractéristique propre au modèle français : l'ANSSI est un organisme interministériel, placé sous l'autorité du Premier ministre. Ce positionnement lui permet d'assurer la coordination interministérielle et la cohérence des positions. Il lui assure également un droit de regard et de contrôle sur les systèmes d'information des autres administrations, ce qui participe incontestablement du rehaussement de la sécurité de l'État.

C'est là un point essentiel de notre stratégie, ce qui fait sa force : le modèle français permet de déployer une politique globale de cybersécurité, c'est-à-dire une politique qui s'attacherait non seulement à défendre les infrastructures – publiques et privées – les plus critiques, mais aussi à parler au plus grand nombre, c'est-à-dire à l'ensemble des acteurs de la transformation numérique du pays.

Enfin, la séparation claire des missions, loin de les opposer, permet au contraire une répartition équilibrée des moyens mais également une coopération efficace au profit de la défense et de la sécurité nationale.

Tirer parti de toutes les opportunités offertes par notre modèle

Le risque numérique, accru par l'accélération technologique et le développement des usages, rend nécessaire une bien meilleure prise en compte des enjeux de sécurité par l'ensemble des acteurs de la transformation numérique. La sécurité doit sortir de son domaine réservé pour associer l'ensemble des architectes de la société numérique. Car au-delà des menaces sur la société, l'économie, la souveraineté et la stabilité du cyberespace, il en va du développement même des technologies.

L'État peut contribuer à créer les conditions de cette montée en puissance. Il s'agit en particulier de structurer un écosystème français de la cybersécurité, par la création de synergies entre les acteurs publics, économiques, de la recherche et de l'éducation. La vitalité de certains acteurs nationaux du secteur le montre : un marché français de la cybersécurité est en construction. Il est désormais nécessaire de l'accompagner.

D'autres pays ont mené cet effort structurant pour assurer la croissance de leurs industries de cybersécurité et ainsi garantir les moyens de leur souveraineté numérique. Israël constitue de ce point de vue un exemple particulièrement inspirant. L'État hébreu a en effet très tôt affirmé son ambition d'organiser son modèle autour de ces synergies. Cette ambition est caractérisée, pour Israël, par la création en 2016 du *CyberSpark*, qui réunit sur un même site des entreprises israéliennes et étrangères, des centres de recherche privés et publics et des unités spécialisées de l'armée israélienne.

La mission pour la création d'un « cyber campus », récemment confiée à Michel Van Den Berghe par le Premier ministre, participe de cet objectif de rapprocher des mondes qui ne se parlent pas suffisamment. De la même manière, l'ANSSI a récemment entrepris une démarche inédite d'ouverture auprès de son écosystème. Notre modèle nous le permet.

Cela passe par un changement de regard sur la cybersécurité. Celle-ci ne peut plus être appréhendée uniquement comme un poste de coût ou un patch appliqué en bout de course de l'innovation. Interrogez les experts de l'ANSSI : c'est un champ d'innovation passionnant, d'une grande richesse scientifique, profondément transdisciplinaire et associant une grande variété d'acteurs, privés et publics, en France comme à l'international. Elle pose des défis intellectuels majeurs pour les innovateurs de tous bords.

Si ces défis concernent naturellement les ingénieurs, les artisans des politiques publiques, du droit et des relations internationales ne sont pas en reste. Comment œuvrer à la stabilité du cyberespace ? Doit-on permettre aux acteurs privés de se faire justice eux-mêmes, de riposter aux attaques dans un contexte où les entreprises deviennent elles-mêmes des « champs de bataille » ? La stabilité du cyberespace est un sujet qui bouscule les habitudes politiques, diplomatiques et militaires. Les questions sont nombreuses et les perspectives excitantes, passionnantes, structurantes.

La cybersécurité sort (enfin) de son ghetto technique

Par **Nicolas ARPAGIAN**
Orange Cyberdefense

L'auteur s'exprime ici à titre personnel sans engager les institutions qu'il représente.

« On pense qu'il est temps pour vous de rejoindre la table des adultes. » D'une phrase familière, le caricaturiste (cf. Illustration 1) a qualifié la place nouvellement attribuée aux sujets de la cybersécurité au sein des comités de direction. L'enchaînement dans l'actualité médiatique des annonces de cyberattaques visant des entreprises et des administrations de toutes tailles, de tous les secteurs, sans épargner aucune région, a contribué à faire de cette matière technique un thème d'intérêt général. Elle ne relève plus désormais de la seule communauté des informaticiens car ses effets mettent en difficulté voire en péril l'usage des services numériques qui structurent notre quotidien personnel et professionnel.

La systématisation du recours aux technologies de l'information pour interagir avec la famille ou des amis, des collaborateurs, des partenaires, des clients, des donneurs d'ordres ou des décideurs institutionnels, a contribué à hausser le niveau de considération pour le bon fonctionnement de ces équipements et un accès continu aux données. C'est donc bien la généralisation de la consommation numérique qui a conduit à faire de la cybersécurité une priorité grandissante, bien au-delà des métiers informatiques.

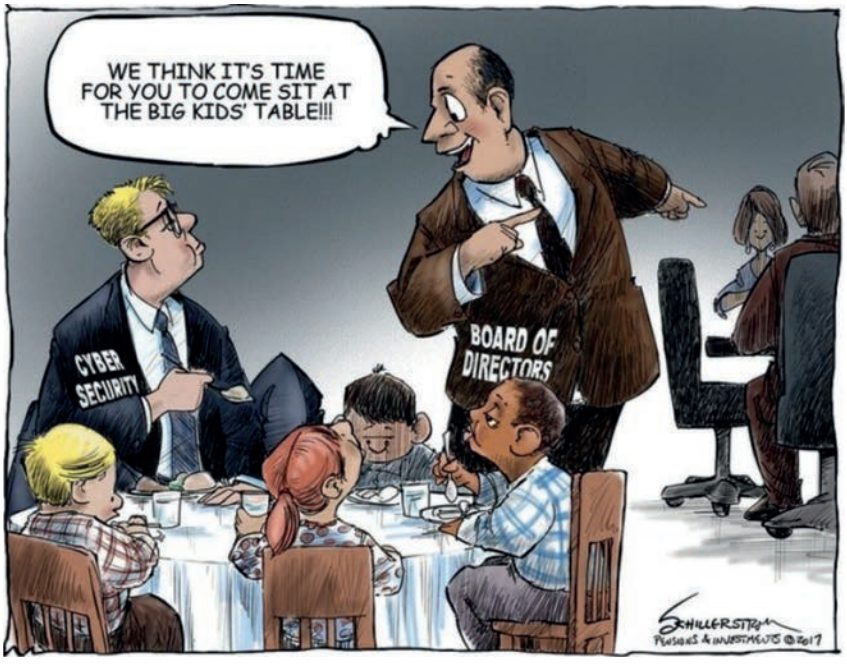


Illustration 1.

La question de la disponibilité des moyens de communication devient désormais une préoccupation de première importance. Si l'informatique ne fonctionne pas, la plupart des entreprises ne tardent pas à constater que leur activité est paralysée, et que leurs équipes ne sont pas en mesure de conduire leurs activités normales.

Une économie numérisée mais tangible

L'économie se définit rapidement comme la gestion de la rareté. Avec la bascule vers une économie de plus en plus dématérialisée qui s'appuie sur la collecte, la valorisation et la transmission d'informations, cette approche de rareté pouvait être rediscutée. Alors que les données sont désormais duplicables, stockables et transférables à l'envi, les consommateurs/utilisateurs de solutions informatiques peuvent avoir l'illusion de l'accessibilité constante des données qu'ils consomment au quotidien.

Le smartphone est devenu la porte d'accès aux services bancaires, aux messageries professionnelles et autres réseaux sociaux. C'est la fluidité des usages et la multitude des services rendus qui ont vite fait de convaincre les moins technophiles des internautes/mobinautes de l'importance de pouvoir accéder en permanence à ces précieux équipements [1] (cf. Illustration 2). C'est l'expérience du manque en cas de perte ou d'oubli de leurs appareils qui a tôt fait de familiariser avec les enjeux de cybersécurité. Les non-techniciens vont donc s'intéresser à la sécurité numérique pour sa capacité à garantir la continuité de service et l'accès à leur patrimoine numérisé : elle devra être présente pour assurer cette maîtrise de la machinerie informatique mais devra savoir se faire oublier pour ne pas gêner ou ralentir la navigation en ligne.

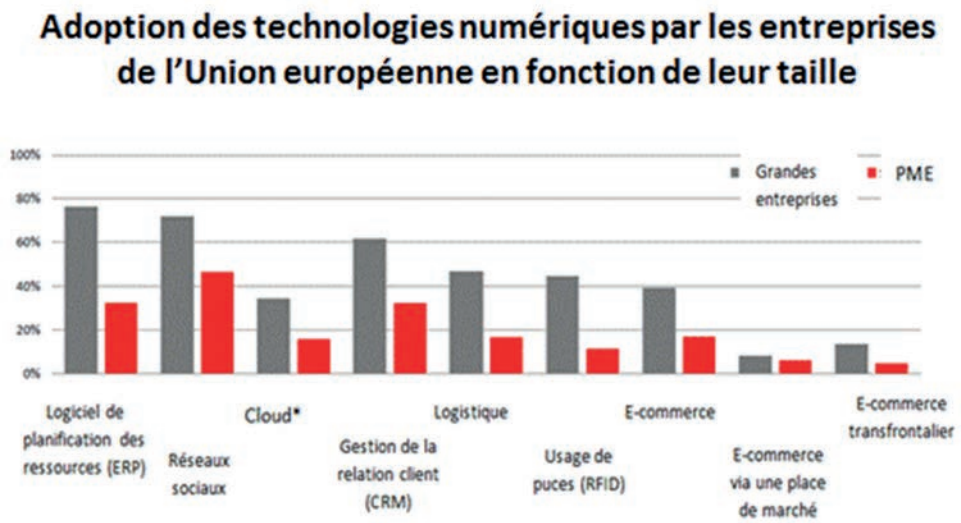


Illustration 2.

(1) « Accompagnement de la transition numérique des PME : comment la France peut-elle rattraper son retard ? » – Rapport d'information n°635 de Mme Pascale GRUNY, fait au nom de la Délégation aux entreprises du Sénat, déposé le 4 juillet 2019.

Une expertise qui se diffuse mais ne se partage pas toujours

L'expert cyber est devenu un personnage de roman et de nombreuses fictions télévisuelles ou cinématographiques lui ont fait une place de choix. Dans les médias, le terme de *hacker* est désormais synonyme de « pirate informatique ». À tort. Le *hacking* ne doit pas être considéré *a priori* comme une forme de piratage mais bien comme une capacité d'autonomie de la connaissance pour ne pas être enfermé dans le seul rôle de consommateur passif d'un outil technique [(2)].

Leur manière d'aborder les technologies peut s'avérer très profitable pour les équipes qui conçoivent ou commercialisent un produit. La compréhension des mécanismes IT et de leurs implications ne doit pas se cantonner aux seules directions techniques. L'application, en mai 2018, en Europe, du Règlement général sur la Protection des Données (RGPD [(3)]) a eu pour effet de valoriser ces informations présentes dans la plupart des entreprises et des organisations publiques. Au regard de l'importance des sanctions encourues en cas de perte ou de vol desdites données – jusqu'à 4 % du chiffre d'affaires mondial globalisé des entités responsables –, les états-majors ont œuvré pour que les services qui collectent, échangent ou produisent ces informations travaillent avec les juristes pour s'assurer de leur conformité à la règle de droit, tandis que tous ont coopéré avec les experts de la cybersécurité et de l'IT pour veiller à leur juste protection et à la traçabilité de leurs usages au sein de l'entreprise. La France a fait le choix dans le cadre de sa Loi de Programmation militaire (LPM) 2014-2019 de désigner plusieurs centaines d'Opérateurs d'Importance vitale (OIV), tandis que la directive *Network and Information Security* (NIS), entrée en application en mai 2018, à l'échelle européenne, établit des critères de protection pour les Opérateurs de Services essentiels (OSE). Ce sont ainsi des pans entiers de l'économie qui ont dû s'approprier la question cyber.

Ces ultimatums juridiques avec des dates d'entrée en vigueur annoncées à l'avance ont suscité *de facto* un partage d'expertises entre des spécialités qui s'ignoraient depuis longtemps. Cette expérience devrait pouvoir servir d'exemple pour dupliquer voire généraliser cette approche transverse qui correspond parfaitement à la diffusion continue de l'impact des technologies de l'information dans l'ensemble des branches du tissu économique. Cette intégration se traduit de manière très concrète : l'analyse des publications institutionnelles des sociétés qui composent les principaux indices boursiers (cf. Illustration 3) montre clairement que la quasi-totalité de ces compagnies doivent donner des gages de leur état de cybersécurité, en fournissant des preuves concrètes de leur engagement financier dans ce domaine et de leur adhésion à des règlementations sectorielles de plus en plus exigeantes.

Une individualisation des usages et donc des risques

Le cabinet Gartner estime que, dans les grandes organisations, 30 à 40 % des projets informatiques sont désormais conçus et pilotés sans impliquer les Directions des Systèmes d'Information (DSI). Ces pans technologiques, désignés sous le terme de « Shadow IT », sont donc aujourd'hui accessibles aux non-spécialistes de l'informatique. Les équipes métiers expriment un besoin et des éditeurs fournissent des solutions activables facilement et interopérables avec les infrastructrures et les logiciels déjà en place.

(2) ARPAGIAN N. (2013), « Les entreprises doivent se mettre au hacking », *Les Échos*, 21 août.
(3) Réforme des règles de l'UE en matière de protection des données : Site officiel de la Commission européenne https://ec.europa.eu/info/law/law-topic/data-protection/reform_fr

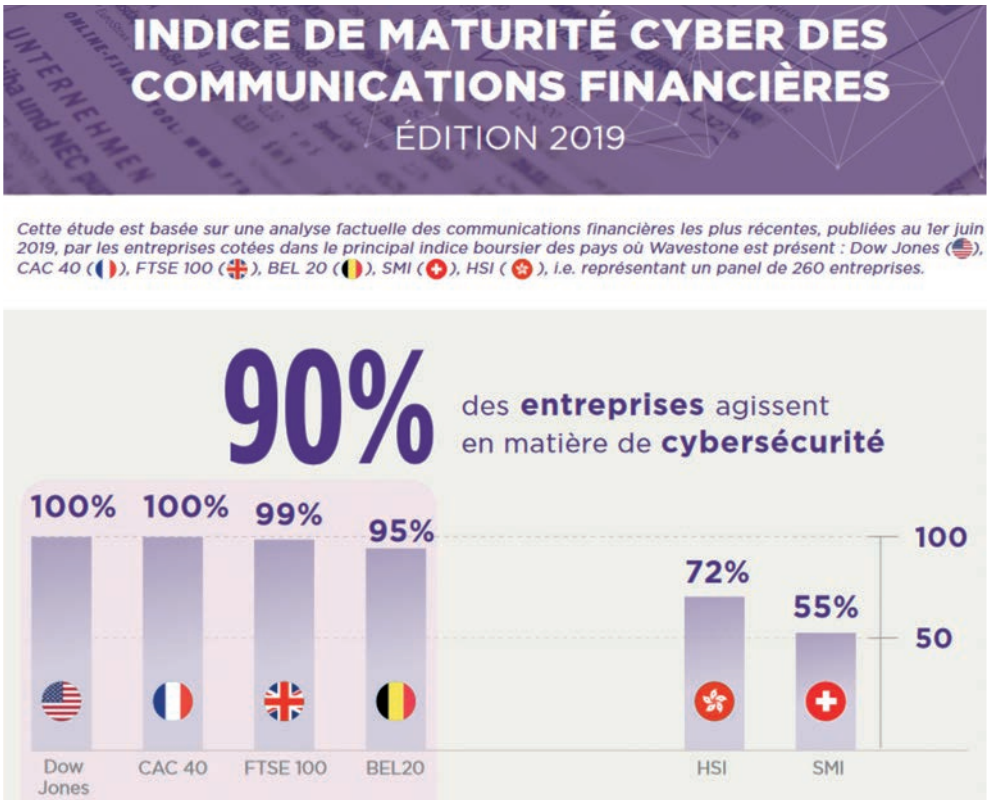


Illustration 3 : « Maturité cybersécurité dans les communications financières des grands indices boursiers », juillet 2019, Cabinet Wavestone.

Poussés par une intensification de la concurrence liée à l'émergence de nouveaux acteurs économiques et à une internationalisation des marchés, les managers se voient contraints de gagner chaque jour en agilité dans la conduite de leurs activités. Ils se doivent d'adapter en continu leurs processus : face à des startup, la pesanteur des machineries des grands groupes peut s'avérer fatale.

Or, les DSI n'étant pas forcément dotées de ressources humaines en nombre suffisant et ne disposant pas toutes d'une véritable culture de service auprès de leurs utilisateurs internes, elles n'ont pas toujours fait preuve d'une réactivité satisfaisante pour répondre aux besoins évolutifs des équipes métiers. De plus en plus, ces dernières ont été directement abordées par des fournisseurs prêts à livrer clés en main des serveurs et des applications immédiatement opérationnels – le respect des règles et des procédures de sécurité, voire la contradiction des obligations maison avec certaines clauses des conditions générales d'utilisation desdits fournisseurs, étant mis de côté dans l'enthousiasme du déploiement de la solution innovante tant attendue.

Un contexte qui explique que le cabinet Gartner [4] annonce qu'en 2020, un tiers des cyberattaques réussies menées contre les entreprises viseront précisément ces équipements de « Shadow IT ». Le slogan « Business First » redistribue le classement des priorités : il s'agit avant tout de tenir des positions commerciales ou de conquérir des marchés. Dans ces circonstances, la cohérence d'ensemble de l'informatique ou le respect scrupuleux des règles de sécurité peuvent aisément se retrouver remisés au second plan. C'est alors que l'engagement de la Direction générale en faveur

(4) Gartner's Top 10 Security Predictions 2016
https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/?cm_mmc=social-_-rm-_-gart-_-swg

de la cybersécurité de l'organisation, gage de sa durabilité, fera la différence, à l'occasion d'arbitrages entre les vertus respectives de la spontanéité des uns et de l'approche sécuritaire des autres.

Vers une financiarisation d'un domaine technique

L'architecture informatique sur laquelle repose la capacité d'une entreprise à demeurer agile et en croissance constitue donc également un point de faiblesse potentielle. Ce sont les deux faces d'un même Janus numérique. Et les experts de l'analyse financière ne s'y sont pas trompés. En effet, les agences internationales de notation Standard & Poors [5] et Moodys [6] ont désormais intégré les métriques de la cybersécurité dans leurs modèles d'évaluation de la valeur d'une entreprise. Aux États-Unis, en mai 2019, Equifax est la première société à voir sa note financière dégradée [7] en raison de sa gestion d'une cyberattaque massive survenue en 2017. L'entreprise doit être en mesure de montrer qu'elle a su s'approprier la flexibilité de la technologie mais que cette bascule numérique ne vient pas fragiliser sa viabilité ou celle de son écosystème (partenaires, sous-traitants, salariés, clients…). L'entrée en vigueur de réglementations sectorielles fixe des obligations supplémentaires. Par exemple, aux États-Unis, l'autorité des marchés financiers, la *Securities and Exchange Commission* (SEC) [8], sanctionne désormais les entreprises qui ne pourront pas démontrer leur prise en compte effective des règles de cybersécurité. Et certains territoires tiennent à préserver leurs habitants en établissant un corpus juridique particulièrement exigeant, à l'instar de l'État de New York qui a adopté en mai 2019 le *Stop Hacks and Improve Electronic Data Security (SHIELD) Act* [9] qui renforce les droits de ses citoyens à voir leurs données protégées. Même si ce déploiement s'effectue sous la menace de sanction, il n'en est pas moins une réalité. Chacun est ainsi davantage informé du risque numérique, et peut orienter, même dans sa vie quotidienne, son choix de prestataires ou de services numériques en fonction de la confiance qu'il/elle portera à la plateforme qui gérera, stockera ou partagera ses données. L'ignorance ne peut plus être invoquée pour se désintéresser des sujets de sécurité numérique.

L'absence de confiance peut-elle s'avérer fatale aux entreprises ?

Dans l'économie numérisée qui valorise les données, la question du niveau de cybersécurité s'imposerait donc comme une condition indispensable à la confiance qui doit unir un client à son fournisseur. En principe certainement. Toutefois, il existe un contre-exemple notable avec Facebook, qui fait partie des acteurs économiques les plus souvent et profondément mis en cause pour leur gestion défaillante de la confidentialité des données. Ainsi le régulateur étatsunien, la FTC, a condamné la firme californienne à 5 Md$ d'amende au printemps 2019 au titre de divers manquements à la confidentialité des données personnelles de ses membres. En 2018, le scandale Cambridge Analytica avait établi l'usage dévoyé à des fins politiques des capacités de profilage des utilisateurs du réseau social. En septembre 2019, le site spécialisé TechCrunch révélait

(5) "S&P Global Ratings360™ to Include Cyber Risk Insights from Guidewire Software's Cyence Risk Analytics", 16 février 2018
https://www.guidewire.com/about-us/news-and-events/press-releases/20180216/sp-global-ratings360%E2%84%A2-include-cyber-risk-insights
(6) FAZZINI K. (2018), "Moody's is going to start building the risk of a business-ending hack into its credit ratings", CNBC, 12 novembre.
(7) "Rating Action: Moody's affirms Equifax sr uns at Baa1, revises outlook to negative from stable", 17 mai 2019, Moody's Investors Service
https://www.moodys.com/research/Moodys-affirms-Equifax-sr-uns-at-Baa1-revises-outlook-to--PR_400804
(8) Securities Exchange Act of 1934 – Release N°84429 / 16 October 2018. Report of Investigation pursuant to Section 21(a) of the Securities Exchange Act of 1934 regarding certain
Cyber-Related Frauds perpetrated against Public companies and related internal accounting controls requirements
(9) Senate Bill S5575B du 7 mai 2019 – https://www.nysenate.gov/legislation/bills/2019/s5575

en outre que Facebook stockait sans aucune précaution – en l'espèce aucun mot de passe – les dossiers de 419 millions de personnes à travers le monde, soit environ un utilisateur sur six. Parmi les données sensibles figuraient le numéro de téléphone associé au profil, mais aussi le sexe et la localisation géographique pour certains comptes. N'importe qui pouvait donc y accéder. Malgré cet enchaînement de mauvaises pratiques, les consommateurs continuent à s'inscrire et à participer à cette communauté planétaire. Et lorsque la FTC a annoncé à l'été 2019 son amende record à l'encontre de Facebook, Wall Street s'est emballé : l'action a atteint son plus haut de l'année pour finir à près de 205 dollars. Ces scores s'expliquent sans doute aussi par la dépendance des consommateurs aux services de la plateforme, notamment la fonction Facebook Connect qui permet d'accéder à de nombreuses interfaces annexes au réseau social. Le cas Facebook illustre les compromis acceptés par le grand public et la communauté financière au nom de l'appréciation générale du service rendu. Au classement des priorités, ici, les consommateurs et les investisseurs ont fait le choix du risque.

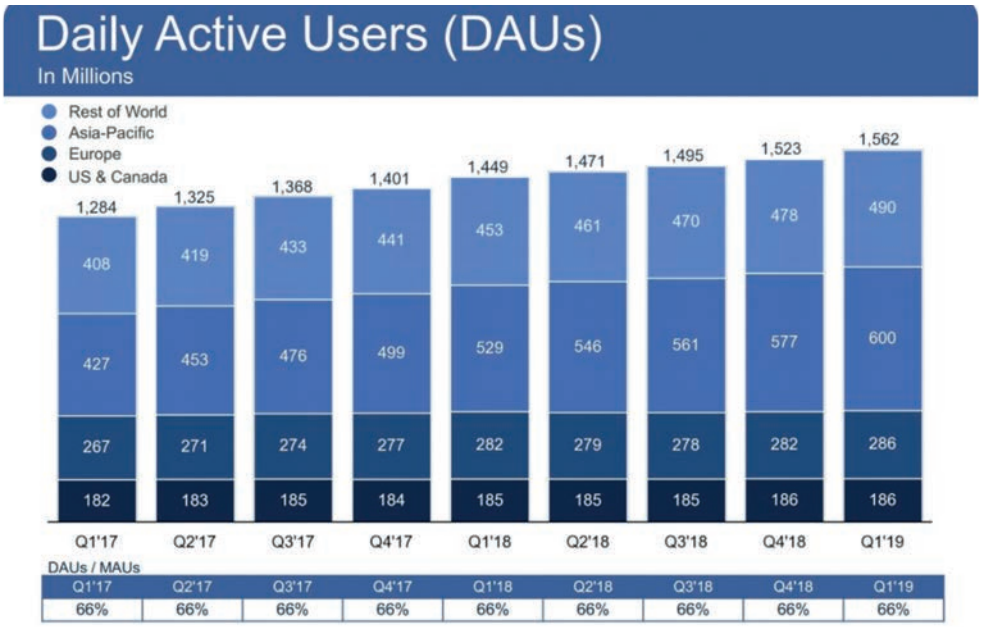


Illustration 4 : Nombre d'utilisateurs actifs de Facebook. Source : Facebook.

Conclusion

La numérisation croissante des modes de production, de commercialisation et de communication de l'ensemble des activités administratives ou économiques a conduit à banaliser les technologies de l'information qui accompagnent intimement chacune de nos activités personnelles et professionnelles. En prenant conscience de notre dépendance numérique et de la valeur des données, les utilisateurs des systèmes informatiques sont de plus en plus exigeants en ce qui concerne la disponibilité, l'intégrité et la confidentialité de leur capital informationnel et de leurs équipements IT. L'actualité médiatique – qui a mis sur le devant de la scène les pillages de bases de données, l'exploitation à des fins malveillantes des profils de réseaux sociaux ou le blocage d'informations sensibles par des rançongiciels – a contribué à l'appropriation des enjeux de cybersécurité bien au-delà des professionnels de l'informatique. On demande des comptes à ses fournisseurs tandis que des prestataires communiquent sur le fait qu'ils n'exploitent pas les données qui leur sont confiées. L'éducation au risque numérique progresse et c'est l'occasion pour les clients – consommateurs ou grands donneurs d'ordres – de mettre au clair leurs priorités dans leurs choix technologiques :

solutions préservant la vie privée, priorité aux éditeurs souverains, choix de logiciels pouvant faire l'objet d'un audit… Autant de décisions qui reposent sur une base technique mais qui s'appuient aussi sur des exigences juridiques, politiques, stratégiques qui dépassent les seuls experts de l'IT. Cette tendance forte de la part des consommateurs finaux de technologies finira-t-elle par influer de manière conséquente sur les politiques des grands groupes ? Si cela devait se vérifier, d'autres critères que la performance et le prix pourraient venir s'ajouter aux éléments de sélection d'un outil ou d'un partenaire, la question de la finalité des usages et de la traçabilité des modes opératoires devenant alors un des éléments différenciateurs entre concurrents.

Bibliographie

Monographies

ARPAGIAN N. (2018), *La Cybersécurité*, Paris, PUF, « Que Sais-Je ? »

ARPAGIAN N. (2018), *Quelles menaces numériques dans un monde hyperconnecté* ?, Paris, Institut Diderot.

ARPAGIAN N. (2009), *L'Avenir de la cybersécurité*, Paris, Institut Diderot.

Collectif (2018), « Assurer le risque cyber », Paris, Club des Juristes.

ROUHAN I. (2019), Les métiers du futur, Paris, F1RST Editions.

SCHWAB K. (2017), *La Quatrième révolution industrielle*, Paris, Dunod.

Rapports / Articles de périodiques

ARPAGIAN N. (2016), « L'Europe de la sécurité numérique : très juridique, mais guère technologique, et encore insuffisamment économique », *Annales des Mines - Réalités Industrielles*, 2016/3, pp.51-54.

ARPAGIAN N. (2017), « Vers une cyberguerre froide entre Moscou, Washington…et la Silicon Valley », *Revue des Deux Mondes*, Septembre 2017, pp. 70-76.

ARPAGIAN N (2018), « Cyberguerre : longtemps annoncée, désormais réalité ? », *Rapport RAMSES*, IFRI-Dunod, pp. 156-161.

ARPAGIAN N. (2018), « Vers une société numérisée, de plus en plus surveillée », *Constructif*, N°51, pp.66-69.

ARPAGIAN N. (2019), « A quoi ressemblera l'Homo Numericus ? », *LES ECHOS*, 9 octobre 2019.

DANESI R & HARRIBEY L. (2018), « La cybersécurité : un pilier robuste pour l'Europe numérique », Commission des Affaires européennes, Sénat.

ENISA, (2019), « Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity ».

GRUNY P. (2019), « Accompagnement de la transition numérique des pme : comment la France peut-elle rattraper son retard ? », Rapport n°635, Sénat, Délégation aux entreprises.

LACHAUD B. & VALETTA-ARDISSON A. (2018), « La Cyberdéfense », Commission de la Défense nationale et des Forces armées, Assemblée Nationale.

MINISTERE DE L'INTERIEUR, (2019), « Etat de la menace liée au numérique en 2019 ».

SCIENTIFIC ADVICE MECHANISM (2017), « Cybersecurity in the European Digital Single Market », European Commission.

SGDSN-ANSSI (2018), Rapport annuel.

Que cherchent les hackers ?

Par **Julie GOMMES**
Cognizant

Introduction

Internet est devenu un nouveau territoire de combats internationaux, fragmenté, disséminé sur des millions de serveurs ; des entreprises et commerces ont pignon sur rue dans ce que Quemener et Ferry appellent des « cyberparadis ». Nous sommes bien loin de l'Internet imaginé par Perry Barlow en 1996, qui espérait ce territoire déconnecté de toute activité physique et obéissant à ses propres règles, définies et changeant au gré des choix des utilisateurs. Ce territoire, miroir déformé du monde physique, est aussi peuplé de personnes qui en connaissent les codes, à tous les sens du terme, et capables de s'en accommoder, voire de s'allier pour en tirer profit, peu importent leurs motivations.

La frontière historique entre *blackhats* (les mauvais hackers) et *whitehats* (les gentils hackers) n'a jamais été aussi poreuse. Il est parfois difficile de cartographier qui sont et surtout ce que veulent ces hackers : au sein de chacun des groupes que nous avons identifiés, évoluent des personnes aux compétences, aux idéaux et aux niveaux techniques variés. Ce n'est plus une frontière manichéenne qui différencie les pirates, ni leur niveau de compétence, mais leurs motivations.

Des motivations bien distinctes

L'appât du gain

Les criminels sont les pirates qui ont fait beaucoup parler d'eux ces dernières années, retombées médiatiques obligent. Ils piratent avant tout pour le profit.

L'argent

De grosses sommes

L'attaque dite de la « fraude au président » est une des plus communes ces dernières années. Les hackers jouent souvent de ce que l'on appelle le Social Engineering[(1)], l'ingénierie sociale, comprenez les techniques de hacking adaptées au mode physique. L'attaquant, souvent après plusieurs mois de recherche d'informations sur l'entreprise et de contacts variés avec des employés, appelle le service comptabilité en se faisant passer pour le chef d'entreprise. Là, il demande un virement en urgence sur un compte hébergé à l'étranger ou la modification des coordonnées bancaires d'un prestataire. Pris par l'urgence de la demande, stressé par le comportement anxiogène du faux président, le comptable transfère l'argent… qui ne restera pas longtemps sur le compte et sera rapidement blanchi ailleurs, grâce à la coopération de certaines banques en ligne (Gueye, 2018). Entre 2010 et 2016, 2300 plaintes relatives à ce type d'attaque ont été déposées en France et le ministère de l'Intérieur estime leur préjudice sur cette période à 485 millions d'euros. De grands comptes français tels que Michelin (1,6 M€) ou Pathé (19 M€) ont d'ailleurs été victimes de ces criminels, mais les attaquants s'en prennent aussi à de petites structures.

(1) Les pratiques d'ingénierie sociale exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles des individus ou des organisations pour obtenir quelque chose frauduleusement (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.).

(Beaucoup) de petites sommes

Autre extorsion dans l'air du temps, les cryptolockers [2] permettent à des hackers de demander des rançons sous forme de très petites sommes en Bitcoin, pouvant aller de 5 à 50 euros, contre la promesse d'un déchiffrement des serveurs et ordinateurs de l'entreprise ou du particulier attaqué.

Ces malwares [3] circulent au gré des pièces jointes ou fausses publicités en ligne sur lesquelles nous cliquons sans faire attention. Ils se répandent vite et facilement et certains chefs d'entreprise voient l'ensemble de leur parc bloqué et croient ne pas avoir d'autre choix que de payer. Or, dans la plupart des cas, l'attaquant récupère l'argent intraçable et n'envoie jamais la clé de déchiffrement permettant de retrouver ses données.

À l'été 2017, une vague de cryptolockers a même bloqué la production de plusieurs grandes entreprises : Vodafone sera touché par WannaCry, à l'instar de FedEx, Renault, Telefónica et la Deutsche Bahn.

Les données

Des numéros de sécurité sociale aux États-Unis, permettant d'ouvrir un compte au nom de la personne et de récupérer à sa place le trop-perçu des impôts, aux numéros de visa en passant par un plan d'aéroport ou la notice de fonctionnement de machines servant à l'extraction du pétrole, les données sont le nouvel or noir des criminels. Pas besoin de grandes qualités techniques pour trouver le plan d'un aéroport ou le dernier *business plan* d'une entreprise cotée. Même si des entreprises gèrent leur sécurité de manière efficiente, des tiers (entreprise de communication, plombier, prestataires divers…) peuvent laisser leur serveur ou un simple disque dur de stockage connecté à Internet, parfois sans le savoir, et sans protection basique de type mot de passe. Des outils qui « scannent » l'Internet à la recherche d'objets connectés de type disques durs, NAS [4], clés USB, serveurs non protégés sont facilement et gratuitement accessibles en ligne. Les hackers n'ont alors qu'à les installer et les laisser tourner pour télécharger et revendre la documentation récupérée à la concurrence, dans le cas de l'espionnage industriel, ou au plus offrant, sur le darknet [5], où des forums donnent accès à d'autres forums et ainsi de suite, jusqu'à atterrir sur les plateformes où se font les échanges les plus importants.

La hiérarchisation des infractions est de moins en moins visible tant au niveau de la gravité que de leur nature juridique (Gueye, 2018) et c'est aussi sur ces plateformes que sont revendues les données volées *via* piratage et nécessitant des compétences plus étendues (intrusion sur un site et vol de la base de données, récupération des informations contenues dans une boîte email, intrusion sur un serveur suite au cassage d'un mot de passe…).

La déstabilisation d'un État

Il est d'autant plus difficile d'anticiper les attaques visant à déstabiliser un État que les modèles de menaces se diversifient. Les attaquants se présentent souvent sous les traits de hackers nationalistes ou ne font pas part de leur motivation réelle, comme dans le cas de Stuxnet [6], le virus destiné à retarder le programme nucléaire iranien (Bonnemaison et Dosse, 2014).

(2) Logiciels malveillants verrouillant les ordinateurs à des fins de demande de rançon.
(3) Logiciels malveillants développés dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.
(4) NAS (de l'anglais Network Attached Storage) est un serveur de fichiers autonome, relié à un réseau, dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes.
(5) Les darknets sont distincts des autres réseaux pair à pair distribués car le partage y est anonyme (c'est-à-dire que les adresses IP ne sont pas dévoilées publiquement) et que les utilisateurs peuvent donc communiquer anonymement. Plus généralement, le « Darknet » peut désigner toutes les technologies et communications web underground, plus communément associées aux activités illégales ou dissidentes.
(6) Stuxnet est un ver informatique découvert en juin 2010 qui aurait été conçu par la NSA en collaboration avec l'unité israélienne 8200 pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium.

Il est toutefois difficile d'établir clairement les liens entre États et groupes de hackers, même si Bannelier et Christakis (2017) affirment, sans les nommer, que certains États entretiennent des liens avec des groupes non étatiques, utilisés comme intermédiaires dans le but de réaliser des actions malveillantes contre un autre État.

Gueye (2018) détaille les impacts de telles attaques (économiques, sociaux, environnementaux ou vitaux) et souligne un « effet dévastateur pour un pays non préparé » en cas de blocage total de la distribution de billets, d'essence ou de produits frais. Faire vaciller un État sans envoyer un seul missile ou sans tirer un seul coup de feu est donc aujourd'hui possible, d'autant plus que l'avènement des télécommunications civiles et d'Internet a permis de transformer un combat asymétrique (7) en combat symétrique sur le terrain cyber.

Ingérence russe

À ce jeu, l'Europe de l'Est est devenue la boîte de Petri de la Russie, ou du moins de hackers nationalistes se revendiquant proches du Kremlin. Les attaques se multiplient et ce, depuis longtemps (Huvert et Razon, 2019) :

- En avril 2007, lorsque le gouvernement estonien a proposé de déplacer la statue d'un soldat symbole de l'ère soviétique, les sites gouvernementaux, ceux de partis politiques, de médias et de banques du pays, subissent des attaques par déni de service (8), rendant par ailleurs les numéros des urgences (pompiers, police) injoignables quelques temps.
- En juillet 2008, c'est la présidence et le parlement géorgien qui sont visés dans l'attaque de 54 sites Internet de partis politiques et de la finance.
- En 2015, les Russes réalisent une cartographie de centrales électriques ukrainiennes qui servira l'année suivante à lancer l'attaque BlackEnergy : les hackers utilisent alors les backdoors (9) laissées sur le système et, pendant une heure, l'électricité est coupée dans la ville de Kiev.
- En mars 2018, des hackers russes, autoproclamés proches du pouvoir, du groupe « ATP28 » aussi appelé FancyBear, ont été identifiés sur le réseau informatique de l'administration fédérale allemande. Les services secrets avaient alors souligné que ces pirates auraient infiltré le réseau un an auparavant et seraient restés sous les radars afin d'accumuler des informations.

Les pirates d'ex-URSS ont souvent le même profil : des ingénieurs, souvent très bien formés, qui ne souhaitent pas travailler en étant sous-payés par rapport à leur niveau de qualification. Ils se tournent donc rapidement vers une manière moins orthodoxe d'utiliser leurs compétences techniques pour gagner leur vie. En Europe, ce sont souvent des jeunes issus de Roumanie, de Russie ou d'Ukraine qui raflent les premières places des "war games" et "capture the flag". Ces compétitions de hacking sont organisées en marge des conférences de cybersécurité. C'est là qu'ils sont repérés par des ministères ou services de renseignement.

La guerre Inde/Pakistan

Les hackers patriotes russes ne sont pas les seuls à reproduire en ligne des conflits existants : Indiens et Pakistanais se livrent une guerre électronique sans fin autour du Cachemire. Ces dernières années ont d'ailleurs été l'occasion de voir certains d'entre eux monter en compétences.

(7) Une guerre asymétrique oppose la force armée d'un État à des combattants matériellement insignifiants. Les guerres asymétriques englobent notamment les guerres d'indépendance, le terrorisme ou la guérilla et se distinguent des guerres entre États.

(8) Une attaque par déni de service (DoS attack pour Denial of Service) est une attaque informatique ayant pour but de rendre indisponible un service. L'attaque par déni de service peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web ou empêcher la distribution de courriels dans une entreprise.

(9) Dans un logiciel ou un système d'information, une backdoor (porte dérobée) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel ou au système.

C'est le cas du hacker indien Godzilla :

- En 2012, il commence par des défacements [10] grossiers de sites, plus ou moins faciles à attaquer. C'est souvent un exercice pour les débutants et une manière de constituer son "book", montrer ce que l'on sait faire.
- En 2013, il met hors ligne les sites des ministères pakistanais des Chemins de fer, de l'Économie, de l'Intérieur, des Affaires religieuses, de l'Environnement et bien d'autres, publiant au passage la vulnérabilité qui lui avait permis de réaliser cette attaque : trois administrateurs géraient tous les sites gouvernementaux clés, utilisant une base de données commune, accessible *via* le mot de passe « 111111 ».
- En 2014, il rend hors d'usage plusieurs sites officiels pakistanais, ceux du gouvernement, du ministère de la Défense et de la présidence, en attaquant non pas les sites directement mais l'infrastructure qui supporte ces sites. Il a aussi attaqué à quelques reprises le Bangladesh et, à n'en pas douter, il sera à l'origine d'attaques contre les pays qui, à l'avenir, viendraient à se positionner en ennemis de l'Inde.

Le militantisme

Les « hacktivistes » militent pour des sujets politiques depuis les années 1960, rappelle Gicquel (2014), qui cite notamment les Allemands du Chaos Computer Club [11], le L0pht Heavy Industries [12] ou les écrits de Perry Barlow [13]. De nos jours encore, divers groupes militants se servent des techniques de hacking pour porter leurs causes, le hacking n'est donc pas le but recherché, comme pour les nationalistes, mais un moyen de communiquer ou de collecter de l'information.

Anonymous

Le mouvement Anonymous est né en 2006 sur le site 4Chan, mélange de forum, de tchat et de site de partage d'images. Il ne s'agit pas d'un groupe à proprement parler, avec ses codes et ses règles, comme peuvent l'être les nationalistes ou les malfrats, mais d'un mouvement auquel chacun peut se référer (Coleman, 2014). Manquant de cohésion à ses débuts, Anonymous s'est fait connaître *via* de petites attaques :

- En 2006 et 2007, notamment contre le parti nationaliste américain.
- En 2011, des hacktivistes publient les noms de pédophiles en se revendiquant du mouvement et en invitant d'autres hackers à faire de même. L'appel est suivi, il permettra la dénonciation de 1 589 pédophiles.

Gabriela Coleman définit le groupe comme « une myriade de relations, de structures et de positions morales » ayant pour mission l'attaque systématique de qui causerait du tort à l'humain (services de renseignements, Église de Scientologie, etc.).

Au fil du temps, le mouvement s'est recentré sur la communication. Communiquer vite et bien devient un des principaux objectifs : « Anonymous produit autant de contenus que ses membres ont de compétences créatives » (Gicquel, 2014), une capacité mise en œuvre en 2008 contre l'Église de Scientologie ou en 2010, alors que les dons à Wikileaks sont bloqués : Anonymous crée alors

(10) Un défacement est un anglicisme désignant la modification non sollicitée de la présentation d'un site web, à la suite du piratage de ce site. Par exemple, afficher le drapeau d'un pays sur la page d'accueil du site gouvernemental d'un autre pays.
(11) Le Chaos Computer Club, que l'on désigne souvent par le sigle CCC, est l'une des organisations de hackers les plus influentes en Europe.
(12) L0pht Heavy Industries (prononcer loft) était un groupe de hackers réputé, basé à Boston, aux États-Unis, entre 1992 et 2000.
(13) Essayiste, militant libertarien, John Perry Barlow (1947-2018) était un des membres fondateurs de *Electronic Frontier Foundation et de Freedom of the Press Foundation*.

des sites miroirs pour diffuser les informations, traduit des câbles diplomatiques pour leur assurer une visibilité plus large et attaque par déni de service les sites de Visa et Mastercard.

Et ces nombreux groupes, travaillant par pôles idéologiques sous la bannière Anonymous, vont faire éclater le mouvement à l'été 2011. En ressortiront de multiples îlots de hackers indépendants, foyers de résistances idéologiques allant de l'opposition à la censure en Tunisie à la lutte contre la culture du viol aux États-Unis. L'infiltration sur les systèmes d'information d'entreprises ne fait plus partie des incontournables *modus operandi* comme au début du mouvement.

Telecomix

Le groupe d'hacktivistes qui s'était constitué autour de la lutte contre le Paquet Télécom au niveau européen en 2009 a toujours eu une forte implication au niveau politique.

En 2011, ils aident les ressortissants des pays du Maghreb et du Moyen-Orient à communiquer pendant les révolutions alors que les connexions Internet sont impossibles :

- En Égypte, alors que les lignes analogiques ne sont pas coupées (l'armée se servant des téléphones fixes pour communiquer), ils ouvrent des lignes analogiques avec l'opérateur français FDN et envoient les numéros et codes d'accès sur plusieurs centaines de fax en Égypte, accompagnés d'une note explicative sur comment s'y connecter avec d'anciens modems 56k [(14)].
- En Syrie, l'idée de départ était de fournir une boîte à outils numériques pour permettre aux révolutionnaires syriens d'améliorer leur anonymat et leur sécurité en ligne.
  - Ils informent dans un premier temps les Syriens par mail, six mille adresses, en leur donnant des liens vers différents outils tels que le proxy Tor.
  - Le lien vers un salon de tchat est aussi partagé, Telecomix les invitant à aller y poser des questions sur l'utilisation des outils d'anonymat.
  - Suivront plusieurs mois d'échanges avec des Syriens pour les aider à communiquer avec l'extérieur et sécuriser leurs communications.
- En parallèle, Telecomix publie des informations techniques sur la surveillance de masse en Syrie et en Libye et organise des campagnes d'envois de modems 56K en prévision d'une future coupure de l'Internet en Syrie (Guiton, 2013).

Des intérêts parfois communs

Entre les « hacktivistes » aux idées libertaires, les criminels cherchant le profit, si possible immédiat, et les nationalistes qui souhaitent aider à asseoir l'influence de leur pays, il peut sembler que d'épais murs se dressent. Toutefois, ces acteurs peuvent « travailler ensemble » à l'occasion de différentes attaques, comme ce fut parfois le cas :

L'attaque de la Géorgie (2008)

L'attaque de la Géorgie [(15)] était attribuée à la Russie, contexte géopolitique oblige. On retrouvait alors :

- une discipline militaire dans l'organisation de l'attaque, attribuée aux nationalistes ;
- le savoir-faire de criminels, payés pour exécuter vite et bien certaines attaques ;
- l'expérience de groupes activistes en termes de communication.

(14) Modems analogiques.

(15) En août 2008, plusieurs sites géorgiens sont bloqués, d'autres piratés. Le site du ministère des Affaires étrangères géorgien affichait alors une caricature du président Mikheïl Saakachvili sous les traits d'Adolf Hitler.

Il est alors très difficile, même si les nationalistes Russes ont géré l'opération, de savoir comment cette attaque a pu débuter. Et ce modèle d'attaque se rapproche de ce que nous voyons de plus en plus. La piste la plus probable reste toutefois le fait que les premiers ont engagé des criminels pour réaliser leur attaque.

Les attaques croisées post-attentat (2015)

La bataille en ligne entre hackers des pays du Moyen-Orient et hackers occidentaux a éclaté très vite suite à l'attentat de 2015 dans les locaux du journal *Charlie Hebdo* et s'est déroulée en plusieurs temps :

- Une première vague de hackers occidentaux a visé des sites en langue arabe, pris au hasard, surtout *via* des attaques de type DDOS [16] ou de défacement sous la bannière Anonymous. Présentées comme un "fight back", ces attaques ne nécessitaient pas de grandes compétences techniques : elles pouvaient être réalisées grâce à des outils disponibles en ligne et dont l'usage est bien documenté.
- Dans un second temps, des attaquants du Moyen-Orient s'en sont pris à des sites en français vulnérables (campings, mairies de villages, petits commerces), souvent développés par des agences de communication ou des développeurs indépendants qui ne prennent pas toujours suffisamment en compte la sécurité. En façade, on observait des attaques assez symétriques avec ce qui avait pu être observé du côté occidental. Or, il ne s'agissait là que d'une première ligne. Une fois les sites Internet infectés, les serveurs rendus accessibles, un autre groupe de pirates, très expérimentés et n'étant pas originaires du Moyen-Orient, allaient plus loin et dérobaient les données afin d'en organiser la revente sur le *black market* [17] (accès à des serveurs, numéros de cartes bancaires…).

Nous avions alors affaire à des attaquants plus chevronnés mais impossible de savoir si l'occasion leur a permis de commettre leurs larcins ou si, en prévision de ce type d'événement, ils avaient déjà « recruté » des hackers moins expérimentés afin de couvrir leurs délits, les techniciens étant occupés à refaire fonctionner les sites ou enlever les traces de défacement au lieu de surveiller les activités suspectes sur les serveurs.

Que voudront les hackers demain ?

Les guerres de demain

Cette association entre hackers aux objectifs différents sur des projets communs a tendance à se développer, ce qui ne facilitera pas le travail des armées. L'OTAN a changé de paradigme et reconnaît depuis la mi-juin le cyber comme un nouveau territoire de guerre, ce qui l'inclut de fait, au même titre que l'aérien, le maritime et le terrestre, dans les zones sur lesquelles les États peuvent attaquer, se défendre ou défendre un autre pays membre de l'organisation. Une décision mûrement réfléchie puisque, en 2014, les chefs d'État des différents pays de l'OTAN pointaient déjà du doigt les déstabilisations qui pourraient survenir dans le monde physique suite à une attaque en ligne. Des hackers pourraient alors jouer différents rôles :

- Un rôle déstabilisateur, à l'instar des actions en Géorgie ou en Ukraine.
- Un rôle recruteur, afin de faire appel de temps à autres à des *script kiddies* [18] pour créer un

(16) Attaque DOS (voir note 8) réalisée à partir de plusieurs sources de type machines zombies. On parle ici de déni de service distribué (en anglais, *Distributed Denial of Service attack*).
(17) Synonyme de *Darknet* (voir note 5).
(18) Un *script kiddie* est un terme péjoratif d'origine anglaise désignant les néophytes qui passent l'essentiel de leur temps à essayer d'infiltrer des systèmes, en utilisant des scripts ou programmes mis au point par d'autres.

écran de fumée ou à des criminels leur permettant de bénéficier, contre rémunération, de leurs compétences techniques.

Un rôle diversif, permettant d'attribuer des attaques à d'autres (*via* proxys [19], commentaires de codes dans une langue bien particulière…) et ainsi détourner le regard d'un adversaire vers un autre pays.

L'information demain

Les capacités techniques des hackers leur permettent d'organiser rapidement et facilement des campagnes d'information ou de désinformation *via* notamment le défacement de sites web alors que d'autres vont se rapprocher de journalistes et transmettre des données permettant de faire la lumière sur des pratiques plus ou moins légales, à l'instar des révélations d'Edward Snowden ou le partage d'informations recueillies par des hackers avec un consortium international de journalistes ayant lancé l'affaire des Panama Papers [20].

Bibliographie

OTAN (1949, mis à jour le 25/11/2015), Traité de l'Atlantique Nord, Washington
https://www.nato.int/cps/fr/natohq/official_texts_17120.htm

PERRY BARLOW J. (1976), *Déclaration d'indépendance du cyberespace*, Electronic Frontier Fondation
https://www.cairn.info/libres-enfants-du-savoir-numerique--9782841620432-page-47.htm#

HUVERT E. & RAZON B. (2019), *Les Nouvelles Guerres, sur la piste des hackers russes,* Paris, Arte Éditions / Stock.

GICQUEL C. (2014), Anonymous, la fabrique d'un mythe contemporain, Paris, Fyp Éditions.

GUEYE P. (Dr) (2018), *Criminalité organisée, Terrorisme et cybercriminalité : réponses de politiques cybercriminelles,* Dakar, L'Harmattan Sénégal.

QUEMENER M. & FERRY J. (2009), *Cybercriminalité : Défi mondial,* Paris, Economica.

BONNEMAISON A. & DOSSE S. (2014), *Attention : Cyber ! Vers le combat cyber*-électroniquen, Paris, Economica, Collection Cyberstratégie.

BANNELIER K. & CHRISTAKIS T. (2017), « Construire la paix et la sécurité internationales de la société numérique. Acteurs publics, acteurs privés : rôle et responsabilités », Paris, *Les Cahiers de la Revue Défense nationale.*

COLEMAN G. (2014), *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous,* Québec, Lux éditeur.

GUITON A. (2013), *Hackers : Au cœur de la résistance numérique,* Paris, éditions Au diable Vauvert.

(19) Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.
(20) Fuite de plus de 11,5 millions de documents confidentiels issus du cabinet d'avocats panaméen Mossack Fonseca, détaillant des informations sur plus de deux cent quatorze mille sociétés offshore et leurs actionnaires de ces sociétés incluant des hommes politiques, des milliardaires, des sportifs de haut niveau ou des célébrités.

La sensibilisation : une arme défensive majeure

Par **Jérôme NOTIN**
GIP ACYMA

Lancé en octobre 2017, le dispositif national d'assistance aux victimes Cybermalveillance.gouv.fr est issu de la stratégie numérique du gouvernement présentée en juin 2015 et dont les objectifs ont ensuite été détaillés dans la *Stratégie nationale pour la sécurité numérique* rendue publique en octobre 2015.

Cybermalveillance.gouv.fr a ainsi reçu une triple mission :

- la sensibilisation et la prévention par la diffusion de bonnes pratiques en cybersécurité et potentiellement la diffusion d'alertes contextualisées ;
- l'assistance aux victimes par une aide au diagnostic du problème, des conseils simples et adaptés, une orientation vers les services compétents, voire vers des prestataires spécialisés de proximité susceptibles de les assister ;
- l'observation de la menace afin de détecter les phénomènes émergents pour pouvoir les anticiper et y répondre.

Les publics du dispositif sont les particuliers, les entreprises, les collectivités et les associations, hors opérateurs d'importance vitale.

Il s'est organisé sous la forme d'un groupement d'intérêt public, le GIP ACYMA. Ce partenariat public-privé rassemble donc les acteurs de l'État et de la société civile engagés dans sa mission d'intérêt public de lutte contre la cyber-malveillance. On peut ainsi citer l'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI), qui relève des services du Premier ministre, et le ministère de l'Intérieur qui ont copiloté sa conception, ainsi que le ministère de la Justice, le ministère de l'Économie et des Finances et le secrétariat d'État en charge du numérique. À leurs côtés travaillent de nombreux acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles de type fédération ou syndicat, des assureurs, des opérateurs, des constructeurs, des éditeurs… En juillet 2019, le groupement d'intérêt public est fort d'une quarantaine de membres. Outre leur soutien financier, ces membres renforcent et démultiplient les actions du dispositif.

Au fil du développement de son action, le dispositif Cybermalveillance.gouv.fr a pu démontrer, par son originalité et les services qu'il apporte, sa capacité à pouvoir répondre à une réelle attente de ses publics. En effet, près de 29 000 personnes sont venues rechercher de l'assistance sur la plateforme en 2018. Ce nombre de sollicitations a été multiplié par quatre entre les premiers mois et les derniers mois de cette année 2018, passant de 500 en janvier 2018 à près de 4 000 en fin d'année. Et sur les six premiers mois de l'année 2019, le dispositif a déjà assisté plus de 60 000 victimes. Cela représente donc le double de victimes par rapport à l'ensemble de l'année 2018 pour une durée divisée par deux. Cette très forte augmentation s'explique principalement par le fait que les publics concernés par le dispositif commencent à en connaître l'existence.

L'analyse de ces sollicitations et les échanges que le dispositif peut avoir avec son écosystème lui permettent d'adapter son action aux attentes et aux réalités du terrain, et en particulier sur ses actions de sensibilisation et d'alerte sur des menaces émergentes.

L'originalité du dispositif réside également dans le fait qu'il intervient généralement en amont des autres services de l'État lorsque la victime rencontre un incident. Il est en cela un capteur très intéressant pour les pouvoirs publics d'une certaine réalité de la cyber-malveillance pour des victimes qui n'envisagent pas en première intention de déposer plainte, soit parce qu'elles n'ont pas conscience que leur mésaventure pourrait faire l'objet de poursuites, soit parce qu'elles pensent que les poursuites dans la sphère cyber ont peu de chances d'aboutir et que leur démarche ne serait qu'une perte de temps, soit enfin parce qu'elles ont honte d'être victimes ou craignent pour leur image. Le dispositif intervient en incitant systématiquement la victime à déposer plainte chaque fois qu'une infraction pourrait être retenue, mais aussi en l'aidant dans sa démarche au travers des conseils prodigués qui sont élaborés en collaboration étroite avec le ministère de l'Intérieur.

Une des forces du dispositif est ainsi sa capacité à identifier des phénomènes à partir d'événements qui, parfois pris séparément, peuvent être considérés comme marginaux mais dont le rassemblement met en évidence le caractère sériel. C'est ainsi que le dispositif a pu contribuer à l'identification du phénomène cybercriminel de masse qu'est « l'arnaque au faux support technique » dès ses premiers mois de fonctionnement, au travers des rapports techniques d'intervention qui lui sont remontés par ses prestataires référencés. Dans la grande majorité des cas, si les victimes avaient bien eu l'impression à un moment ou un autre de s'être fait arnaquer, elles n'envisageaient généralement pas pour autant de déposer plainte, pour les raisons évoquées précédemment.

L'identification de ce phénomène cybercriminel et les échanges opérationnels qui ont pu être menés avec les services des ministères de l'Intérieur et de la Justice ont conduit à l'ouverture d'une enquête par la section de lutte contre la cybercriminalité du parquet de Paris en mars 2018. Cette enquête, confiée au centre de lutte contre les criminalités numériques (C3N) du pôle judiciaire de la gendarmerie nationale, a conduit à l'interpellation et à la mise en examen d'un réseau de trois individus ayant fait près de 8 000 victimes et à la saisie de près de 2 millions d'euros début février 2019.

Cette possibilité d'identification des menaces au plus près de leur apparition permet également au dispositif d'alerter les populations sur son site Internet et/ou ses réseaux sociaux (Twitter, Facebook, LinkedIn). Grâce au relais et à l'appui de ses membres, plusieurs alertes émises par le dispositif ont été largement reprises par les médias grand public (JT de 20h00), démultipliant ainsi les capacités d'atteindre le plus grand nombre de victimes potentielles.

Les TPE-PME : cibles de choix des cybercriminels

Même si elles ne sont pas exonérées du risque de subir des cyberattaques très variées, les grandes entreprises ou les grandes administrations se sont souvent armées pour y faire face, tant en matière de compétences qu'en moyens techniques. Il n'en est malheureusement pas toujours de même pour les petites et moyennes entreprises, ou les collectivités territoriales. Ces plus petites structures représentent donc une cible de choix pour les cybercriminels qui cherchent évidemment toujours à maximiser leurs profits avec un minimum d'efforts. Les conséquences de ces attaques peuvent être dramatiques pour ces plus petites organisations qui y jouent parfois leur survie économique.

On peut aisément admettre que la priorité d'une entreprise réside dans la réalisation de son activité, dont les systèmes d'information ne sont généralement considérés que comme le simple support. La numérisation des activités en fait pourtant une composante particulièrement critique pour les entreprises. Sans leur système d'information, la plupart des organisations ne peuvent tout simplement plus fonctionner et voient donc leur activité s'arrêter.

Pourtant, les services autour du système d'information sont souvent externalisés auprès de prestataires qui se livrent une concurrence féroce en tirant les prix vers le bas, ce qui est

évidemment toujours un argument très regardé par leurs clients. Cette logique économique va souvent de pair avec un niveau des prestations qui peut s'avérer amoindri, notamment en ce qui concerne le domaine de la sécurité.

De leur côté, les cybercriminels ont bien conscience de cette réalité et des vulnérabilités induites pour ces entreprises qu'ils vont pouvoir exploiter afin d'en tirer profit. Le temps est aujourd'hui révolu (ou presque) du stéréotype du « pirate » marginal, qui s'attaquait seul depuis sa chambre d'étudiant à une multinationale. Les entreprises doivent aujourd'hui faire face à un écosystème cybercriminel qui se structure et se spécialise en expertise et domaines de compétences. Certains groupes criminels se sont ainsi spécialisés dans la réalisation d'outils d'attaques de haut niveau, d'autres dans la recherche de failles ou d'accès dans les systèmes, d'autres encore les achètent pour les mettre en œuvre, d'autres enfin vont exploiter les résultats des attaques. Et sur le fameux *Darknet* dans lequel gravitent ces cybercriminels, tout se vend et tout s'achète.

Au travers des échanges qu'il peut avoir avec les victimes ou ses prestataires référencés, le dispositif Cybermalveillance.gouv.fr constate que les attaques conduites par les groupes cybercriminels sont de plus en plus « professionnelles » et que les dommages qu'elles occasionnent sont de plus en plus conséquents pour les structures qui les subissent.

Parmi ces attaques, celles par rançongiciels (*ransomware*) sont une bonne illustration de l'évolution des techniques et des capacités cybercriminelles. Si, initialement, ces attaques étaient généralement déclenchées à partir de simples pièces jointes ou liens malveillants contenus dans des messages d'hameçonnage (*phishing*) plus ou moins ciblés et mal rédigés, aujourd'hui les entreprises qui en sont victimes voient des modes opératoires radicalement différents les frapper.

Désormais, les cybercriminels cherchent par exemple à pénétrer directement les entreprises par leurs accès extérieurs, que ce soit par les accès de travail à distance ou de télémaintenance. Ils y parviennent soit en exploitant une faille logicielle non corrigée, soit en arrivant à « casser » des mots de passe insuffisamment solides.

Une fois dans la place, les cybercriminels peuvent parfois rester plusieurs jours dans le réseau de l'entreprise victime. Durant cette période de reconnaissance, ils vont cartographier le réseau pour repérer tous les actifs numériques importants. Dans certains cas, et si les cybercriminels y voient un intérêt, ces actifs peuvent être dérobés au passage pour être revendus à d'autres qui sauront en faire usage.

Une fois cette cartographie réalisée, les cybercriminels lancent la partie visible de leur attaque. Celle-ci se déroule généralement en dehors des heures ouvrées de l'entreprise qu'ils ont pu appréhender en l'observant. Ils commencent alors à chiffrer les données de l'entreprise en démarrant par… ses sauvegardes. Les cybercriminels ont bien compris que chaque entreprise a aujourd'hui peu ou prou des sauvegardes. Mais aussi que ces sauvegardes sont généralement, et par facilité, directement accessibles en ligne sur le réseau de l'entreprise qui n'a d'ailleurs souvent aucune autre copie récente de ses données.

À l'ouverture des bureaux de l'entreprise, toutes ses données sont chiffrées et les sauvegardes inaccessibles. Un message de demande de rançon l'attend. Cette rançon représente généralement une portion « acceptable » du chiffre d'affaires de l'entreprise au regard du préjudice qu'elle subit. De quelques centaines d'euros pour une TPE à plusieurs milliers d'euros pour des collectivités, et jusqu'à des centaines de milliers d'euros pour des PME de taille plus importante. Cette variabilité des rançons demandées en fonction des capacités de paiement de sa cible démontre bien que le cybercriminel qui commet l'attaque ne frappe plus au hasard, et qu'en amont et une fois dans la place, il a cherché à savoir quel montant maximal il pouvait extorquer à sa victime.

Les conséquences de ces attaques par rançongiciels ne se limitent pas à la perte financière de la seule rançon, que certaines victimes pourraient être enclines à payer. Il faut en effet toujours y ajouter le coût de la perte de production parfois durant plusieurs jours, liée à l'indisponibilité du système d'information de la victime, ainsi que celui des travaux de remise en état.

Ces exemples montrent qu'une entreprise logiquement focalisée sur son cœur de métier et sur sa réactivité opérationnelle peut se retrouver insuffisamment préparée à subir de telles attaques. Elle peut alors se retrouver désemparée quand elle tombe sous le joug de cybercriminels qui sont pour leur part de plus en plus « professionnels » dans leurs actions.

La sensibilisation : une arme défensive majeure

La sensibilisation reste la meilleure arme des entreprises et des collectivités pour éviter les cyberattaques. Dans le milieu professionnel, cette sensibilisation des employés aux cybermenaces et aux bonnes pratiques à adopter pour les détecter et les éviter est donc primordiale. Or, cela reste souvent un exercice difficile, car les sujets de sécurité numérique sont généralement ressentis comme rébarbatifs, peu parlants et sources de contraintes pour les utilisateurs. Et ce, quel que soit leur niveau dans l'entreprise : du dirigeant à l'employé, en passant par le cadre ou même « l'informaticien ».

C'est partant de ce constat issu des travaux conduits avec ses membres que le dispositif Cybermalveillance.gouv.fr a réalisé en 2018 le premier volet de son kit de sensibilisation pour les collaborateurs, le plus facile d'accès possible. Le kit complet a été finalisé en juin 2019. Il peut être téléchargé gratuitement sur la plateforme du dispositif [1]. Il comprend différents types de supports (courtes vidéos, infographies, fiches pratiques, mémos…). Il s'adresse au collaborateur à propos de ses usages personnels de manière pédagogique et illustrée, sur des sujets qui peuvent également intéresser l'entreprise dans ses usages professionnels. Par exemple, si un collaborateur sait détecter et réagir à un message d'hameçonnage (*phishing*) dans ses usages personnels, il saura également le faire dans ses usages professionnels. Dans ce kit, différents thèmes sont abordés : l'hameçonnage qui est le principal vecteur d'attaque aujourd'hui ; la bonne gestion des mots de passe qui reste une des principales protections des systèmes ; la sécurité des appareils mobiles (smartphones, tablettes) qui présentent des vulnérabilités spécifiques importantes ; la différenciation des usages professionnels et personnels, etc.

Un choix fort a été de le publier sous licence Etalab 2.0. Cette licence permet à toute entité de le modifier, et donc d'ajouter ou de supprimer du contenu. Beaucoup de structures ont par exemple simplement ajouté le logo de leur entité afin que l'adhésion des collaborateurs soit encore plus forte.

Enfin, au titre de la prévention et de la sensibilisation, on peut également citer la préparation à la gestion de la crise qu'engendre pour une entreprise toute attaque informatique majeure. Force est de constater que les entreprises, surtout les plus petites, sont généralement insuffisamment préparées pour affronter ces situations difficiles et pour elles exceptionnelles. De nombreux conseils en première intention sont disponibles sur la plateforme Cybermalveillance.gouv.fr sur les principaux types d'attaques.

La question pour une entreprise n'est donc plus aujourd'hui de savoir si elle sera attaquée, mais quand ?, et si elle est suffisamment préparée pour l'empêcher ou y faire face. Car malheureusement, la cybermalveillance, cela n'arrive pas qu'aux autres.

(1) https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/.

Cyberdéfense : l'humain au cœur de l'efficacité opérationnelle

Mettre à l'épreuve son dispositif de défense est indispensable pour progresser

Par **Vincent RIOU**
Directeur associé Cybersécurité, CEIS

Mais comment se fait-il que les meilleures technologies de détection et de prévention des attaques, combinées avec les meilleures sources de Threat Intelligence, le tout utilisé par une équipe de lutte informatique défensive dédiée échouent encore et encore à stopper des attaques avancées ? Comment se fait-il que nous assistions à une explosion des vols de données massifs alors que les budgets cyber ne cessent d'augmenter ? La réponse est simple. Dans un contexte de cyberguerre totalement asymétrique, le défenseur sera mis en échec si, après avoir arrêté des milliers d'attaques, il n'en laisse passer ne serait-ce qu'une seule. À l'inverse, l'attaquant, après avoir été bloqué des centaines de fois, sera gagnant pour une seule attaque réussie. Le jeu est totalement déséquilibré.

Dès lors, faut-il encore et encore augmenter son budget cyber et accumuler dans son réseau les « boîtes magiques » tant vantées par le marketing des éditeurs ? Le nombre de sociétés ayant subi une attaque majeure malgré des millions d'euros dépensés en outils de sécurité divers montre qu'il ne suffit pas de dépenser plus pour limiter son risque. Il faut dépenser mieux. Pour vous en convaincre, engagez une équipe de *Red Team* et observez par où ils rentrent dans vos réseaux (certainement pas par la grande porte blindée !), comment ils bougent latéralement, comment ils effacent leurs traces, comment ils leurrent vos *cyber magic tools* achetés à grands frais, le tout sans se faire une seule fois détecter par le SOC[(1)]… Pendant ces tests *Red Team*, les outils du SOC reçoivent des dizaines d'alertes, voire des centaines. Le problème est que ce sont principalement des faux positifs, ou des leurres sciemment orchestrés par l'attaquant pour faire « sonner » le SOC et occuper l'attention des équipes en dehors des zones privilégiées par l'attaquant. Ces faux positifs créent dans les équipes du SOC une fatigue latente et une baisse d'attention et de motivation, qui conduisent inexorablement à l'inefficacité d'un dispositif censé traiter des attaques « avancées ».

Dès lors, posons-nous la question. Avant de réinvestir dans de nouveaux outils miracles, n'est-il pas grand temps d'apprendre à utiliser à pleine capacité les moyens dont nous disposons déjà ? L'importance de l'entraînement et de la préparation des troupes, de la connaissance de ses forces et de ses faiblesses, l'anticipation des stratégies de l'ennemi, la dissimulation, le leurrage… Tout est dans *L'Art de la guerre.* Ouvrage toujours cité, rarement appliqué…

Se mettre à l'épreuve pour progresser

Plus qu'en suivant des principes normatifs génériques, il faut appréhender sa cybersécurité du point de vue de l'attaquant : *Red Team,* entraînement opérationnel, exercice de crise. Cela demande du courage à une organisation de se mettre à l'épreuve, mais c'est la clé du succès.

(1) *Security Operation Center* ou Centre d'Opérations de Sécurité.

Les conséquences d'une attaque informatique réussie sont dramatiques : image écornée, pertes financières, rançonnage, vol de données, arrêt d'une exploitation, voire danger majeur pour les populations, si l'attaque vise une infrastructure sensible. Cette tribune n'a pas vocation à égrener les chiffres, ils sont connus. Elle s'attellera à ouvrir une piste fondamentale pour circonscrire le phénomène : la mise à l'épreuve et l'entraînement.

À un premier niveau, des opérations de sensibilisation en entreprise permettent aux employés, quelles que soient leurs compétences techniques, de connaître les fondamentaux des comportements à adopter. C'est ce que l'ANSSI appelle l'« hygiène informatique ». À l'image des règles de sécurité sanitaire, un entraînement régulier s'impose, afin de créer des automatismes. Ainsi, il conviendrait de créer de manière récurrente des exercices de crise cyber touchant une large part des employés, afin de les sensibiliser aux risques. Un employé averti en vaut deux, et le coût du montage de tels exercices est largement amorti par la diminution du risque induit par les bons réflexes créés à tous les niveaux de l'entreprise.

L'entraînement des professionnels de la cybersécurité d'une entreprise ou société de service spécialisée doit, lui, aller bien plus loin. Afin d'acquérir et de conserver les réflexes indispensables à ces métiers, les professionnels doivent se former, puis s'entraîner en permanence. Dans un parallèle avec la sécurité physique, on n'imagine pas le GIGN ou le RAID partir en mission sans un entraînement préalable d'une intensité telle qu'elle amène ses personnels à agir de manière réflexe, avec une extrême efficience une fois sur le terrain. Ils évaluent l'ensemble des comportements possibles de l'attaquant et préparent la contre-offensive en fonction. Confrontées à une attaque de grande ampleur, les équipes de réponse aux incidents informatiques doivent, elles aussi, être préparées. Plus que des fiches réflexes, il faut des actes réflexes.

Formation *vs* entraînement

On distingue la formation de l'entraînement par le caractère immersif de ce dernier. La formation va permettre de développer des compétences théoriques selon une démarche pédagogique adaptée. L'entraînement, quant à lui, consiste à effectuer une mise en situation dont le niveau de difficulté sera corrélé au niveau de compétence du professionnel. Là où la formation permet de connaître les techniques de base composant la boîte à outils du cyber-défenseur, l'entraînement permet de les maîtriser par la mise en pratique, afin d'augmenter la qualité et la vitesse d'exécution et de diminuer le stress en situation réelle. C'est l'entraînement qui permet d'acquérir les réflexes vitaux en cas d'agression et d'augmenter son efficacité.

« Plus je m'entraîne et plus j'ai de la chance », disait Arnold Palmer. En effet, l'efficacité opérationnelle ne dépend pas seulement de la somme de connaissances amassée souvent de manière trop théorique. Elle résulte, au contraire, de mécanismes réflexes qui ne peuvent s'acquérir que par la pratique intensive. Le vocabulaire et les modes d'actions de la cyberdéfense s'apparentent beaucoup aux sports de combat : attaque, défense, parades, feintes, anticipation, réflexes, endurance… Un parallèle également évident avec le monde militaire, où nos soldats doivent maîtriser armement, tactiques et modes opératoires sur le bout des doigts avant de partir en opération. Ceci est d'autant plus vrai que les moyens de cyberdéfense, évoluant au rythme des nouvelles techniques d'attaque et des avancées technologiques, deviennent de plus en plus complexes et donc difficiles à maîtriser, ce qui renforce le besoin d'un entraînement régulier.

On peut, dès lors, faire le lien avec les qualités nécessaires à un compétiteur sportif, ces qualités devant s'acquérir par un entraînement régulier :

- Le relâchement : conserver son sang-froid est indispensable quand l'attaque survient. Toute crispation est synonyme d'une baisse d'efficacité. Le relâchement permet de diminuer la

pression et le stress, permettant un état d'esprit propice à la diminution du temps de réaction et à l'augmentation de la qualité des réponses aux attaques.

- Des techniques adaptées : souplesse, vivacité, adaptation au contexte. La réponse à incident nécessite une palette de techniques large, qu'il faut acquérir préalablement à la survenue d'un incident important. Celle-ci doit être la plus exhaustive possible. D'où la nécessité d'une mise à jour de ses capacités de défense régulière par des entraînements et des stages ciblés, en environnement simulé.
- La diminution du temps de réaction : outre l'expérience du terrain, seul un entraînement réaliste permet de diminuer ce temps de réaction, crucial pour la qualité d'une réponse à une attaque et la limitation des dégâts induits. Au-delà des connaissances théoriques, la mise en pratique répétée permet d'automatiser la réaction, jusqu'à arriver à des actions « réflexes ».
- La multiplication des oppositions : un boxeur ne progressera plus s'il s'entraîne constamment avec le même partenaire. Au contraire, sa courbe de progression sera maximale s'il varie les entraînements (sac de frappe, musculation, cibles mobiles, partenaires différents, travail de vitesse…). Il en va de même en cyberdéfense. Il faut se confronter à des attaques larges et variées, dans des contextes opérationnels différents, avec des outils différents, pour aiguiser ses sens et optimiser une réaction qui se veut avant tout humaine, même si elle est fortement soutenue par la technologie.
- La focalisation de son attention : en opération, lorsqu'une attaque survient, il est essentiel de pouvoir faire abstraction des stimuli parasites, de gérer son effort, et de bien réagir aux commandements de la chaîne de décision. Cela ne s'acquiert pas en théorie, mais bien par la pratique.

À ces qualités personnelles, il convient de rajouter les qualités collectives, car la cyberdéfense est un travail d'équipe. Chaque acteur de la chaîne de défense a un rôle particulier et complémentaire. On peut faire le parallèle avec les qualités d'une équipe de rugby ou de football. Les qualités individuelles s'additionnent alors par la mise en œuvre de stratégies collectives, par la solidarité et l'entraide, l'optimisation de la chaîne de décision, l'initiative au service du collectif, la qualité du reporting, le respect des rôles et des règles…

Pour être efficaces, ces entraînements collectifs et individuels doivent être réguliers. En effet, les menaces informatiques sont en constante évolution, et un « expert » du domaine ne le reste jamais longtemps s'il se repose sur ses acquis. De nouvelles techniques d'attaques sont perpétuellement développées dans le monde cybercriminel. Il faut donc en permanence se préparer pour limiter l'effet de surprise et les dégâts induits par les attaques. Le rôle de la *Cyber Threat Intelligence* est alors mis en avant, à raison. Encore ne faut-il pas se contenter d'intégrer les tactiques et procédures d'attaque constatées par le passé, mais anticiper comment elles pourraient être adaptées par l'ennemi.

La formation et l'entraînement s'adaptent ainsi au niveau et aux besoins requis, de la sensibilisation à l'entraînement intensif, des « gestes qui sauvent » en cas d'agression, à l'entraînement d'un « cyberdéfenseur » professionnel.

Une entreprise peut décider de mettre en place un processus de formation et d'entraînement interne, basé sur les compétences à sa disposition, ou choisir de faire appel à un centre professionnel de formation et d'entraînement à la cyberdéfense, à l'image de *bluecyforce* en France, qui dispose de moyens très importants d'immersion dans le réalisme d'une cyber-crise et de méthodes pédagogiques adaptées.

En effet, bien s'entraîner impose de disposer de moyens importants pour renforcer le réalisme de l'immersion. On ne progresse efficacement que par l'action. Reprenons notre parallèle sportif. Pour améliorer ses performances, le boxeur amateur va s'inscrire dans une salle, où il trouvera

l'ensemble du matériel adapté à sa pratique : rings, sacs de frappe, poire de vitesse, partenaires d'entraînement, professeurs… Les cours seront adaptés à son niveau, le faisant progresser d'étape en étape, par la confrontation avec des adversaires de plus en plus forts. Le tout dans une ambiance ludique et agréable, mêlant challenge physique, mise sous pression puis détente, afin d'améliorer autant le mental que le physique.

Il en va de même pour la formation et l'entraînement à la cyberdéfense.

Le ring et tous les accessoires d'entraînement ? Un environnement fermé et contrôlé, intégrant de larges topologies réseaux, des flux de données réalistes et des systèmes d'information simulés, permettant de mener des attaques de tous niveaux d'intensité, en toute sécurité, sans risque de propagation incontrôlée.

Les partenaires d'entraînement ? Une *Red Team,* hackers éthiques professionnels et expérimentés, dont le niveau des attaques s'adaptera au niveau des stagiaires, afin de ne pas les « noyer sous les coups » mais, au contraire, de les faire progresser.

Les poings, les gants, les yeux, les muscles du boxeur ? L'ensemble de moyens techniques de la chaîne de lutte informatique défensive : WAF, SIEM, EDR, firewalls, sondes de détection, outils de forensique… Autant de moyens qu'il ne faut pas se contenter d'implémenter dans leur environnement informatique, mais bien de maîtriser dans un contexte d'ensemble cohérent.

À tout cela s'ajoute un paramètre essentiel de l'entraînement : la « ludification ». Sous forme de jeux, l'entraînement doit aboutir à une implication totale, à la provocation d'une montée de stress qu'il faudra apprendre à contrôler, à des enjeux forts qu'il faudra défendre. La qualité des scénarios proposés est donc partie intégrante de la pédagogie, tout comme la complémentarité des profils des « entraîneurs » des futurs champions de la cyberdéfense.

Leurrer l'ennemi : la cybersécurité déceptive

L'épreuve des équipes de défense face à une *Red Team* aguerrie nous amène naturellement à définir de nouvelles stratégies de réponse. Comment combattre un ennemi furtif, agile, qui s'adapte, qui n'a à suivre aucun carcan légal ou règlementaire ? Les actions contre-offensives étant interdites dans notre législation, il faut piéger l'ennemi. C'est le concept de Cybersécurité déceptive. Leurrage, dissimulation, déception… autant de stratégies de contre-mesures bien connues du monde de la Guerre électronique, qu'il nous faut nous réapproprier dans le cyberespace, afin de ne pas laisser l'attaquant serein par une posture de défense passive, uniquement basée sur la détection et la remédiation des incidents. Pour le moment, nos entreprises les plus matures se croient à l'abri derrière de hautes murailles, tandis que l'ennemi apprend à voler…

L'entraînement des équipes opérationnelles, les exercices de crise et la confrontation à une équipe *Red Team* sont de véritables épreuves du feu. Elles seules sont en mesure de qualifier l'efficacité réelle d'une stratégie de cybersécurité, tout en faisant progresser l'ensemble de la chaîne de défense.

Se confronter, se réadapter, ne pas se contenter de suivre les normes, ne pas faire confiance aux seuls outils de cybersécurité pour se défense. À tous niveaux, l'humain est au cœur de l'efficacité opérationnelle.

Prévenir et détecter

Par **Jacques DE LA RIVIÈRE**
Gatewatcher

L'hétérogénéité des systèmes d'information, la migration des données dans le *Cloud* ou encore le nomadisme sont autant de paramètres qui rendent difficile la définition du périmètre de protection des entreprises. À cela s'ajoute la professionnalisation de la cybercriminalité qui rend les menaces plus nombreuses et polymorphes.

Dans cet environnement sinueux, et alors que les analystes des Centres d'Opérations de Sécurité (SOC) et experts de la sécurité du *Cloud* sont des denrées rares, il est logique de vouloir utiliser la technologie pour automatiser des tâches de détection, d'évaluation et de réponse.

Plusieurs solutions se dessinent aujourd'hui, à la fois innovantes et complémentaires, mais chacune avec des limites : le SOAR (*Security Orchestration, Automation and Response*), la CTI (*Cyber Threat Intelligence*) et enfin l'intelligence artificielle et plus spécifiquement le *machine learning*.

Les enjeux de l'automatisation et de l'orchestration dans la cybersécurité

À l'heure où les volumes d'alertes et d'informations sont parfois trop importants à traiter pour l'humain, l'orchestration et l'automatisation de la gestion des incidents sont devenues incontournables.

L'acronyme SOAR rassemble toutes les technologies qui permettent de collecter les données et alertes de sécurité à partir de multiples sources et, surtout, aident à industrialiser l'analyse et le triage des incidents. L'idée est ici de combiner les apports de l'humain et de l'informatique pour définir, hiérarchiser et intégrer des activités de réponse à incident dans un processus standardisé.

Si les entreprises s'intéressent à ces outils, c'est notamment pour essayer d'améliorer la productivité de leurs équipes en charge de la sécurité, alors que le budget manque pour en gonfler les effectifs, ou que les tentatives de recrutement se heurtent à la pénurie de compétences. Et si le recours à des prestataires de services extérieurs peut être une solution, faire appel à des outils d'orchestration et d'automatisation peut en constituer une autre.

Outre les gains de productivité, les outils de SOAR peuvent également aider à réduire les délais de réponse aux incidents de confinement et de remédiation, mais aussi à libérer les analystes de certaines tâches routinières, parfois redondantes, et souvent chronophages. Et celles-ci ne manquent pas de peser sur la motivation des équipes des SOC. Cela concerne notamment tout le travail de triage initial des alertes, parmi lesquelles, souvent, de nombreux faux positifs. Les outils de SOAR enrichissent automatiquement les alertes, ajoutent des informations de contexte clé, pour permettre un triage automatisé ou, *a minima,* un triage manuel plus rapide et plus simple.

L'optimisation du triage peut dès lors permettre d'améliorer les capacités de détection en limitant le risque de voir des alertes significatives passer inaperçues. Et cela vaut aussi pour tout le travail de documentation des processus et d'audit, le suivi des performances du SOC, ou encore pour le temps de formation initiale des analystes.

L'automatisation et l'orchestration en sécurité sont rendues possibles par la multiplication des API nécessaires à l'intégration. Fut un temps où quelques outils proposaient des API, mais peu d'entre elles étaient aussi standardisées et simples que les API Rest qu'on utilise aujourd'hui. L'automatisation totale des processus de sécurité nécessitera encore du temps, si tant est qu'elle soit possible. En attendant, les outils de SOAR peuvent apporter beaucoup dans de nombreux domaines.

Cela commence notamment par la gestion des alertes remontées par le système de gestion des informations et des événements de sécurité (SIEM). Là, les outils de SOAR permettent d'automatiser des tâches d'enrichissement, comme la recherche d'informations supplémentaires sur des indicateurs de compromission, ou la soumission d'échantillons suspects à des systèmes d'analyse externes. Les tickets correspondant à des alertes simples, ne relevant pas d'une menace réelle, peuvent être fermés automatiquement.

Des outils d'EDR [(1)] peuvent également être mis à contribution de manière transparente pour la collecte de données supplémentaires sur les hôtes concernés et la recherche de corrélation avec le trafic réseau peut ainsi être lancée. Concrètement, il peut être question de traitement de courriels suspectés de relever d'une tentative de *phishing*, et d'enrichissement d'une alerte générée par le SIEM à l'aide d'une plateforme de gestion du renseignement sur les menaces. On peut aussi se pencher sur les outils de gestion de tickets et plus généralement de services IT (ITSM), mais aussi de travail collaboratif, comme Slack, ou encore d'administration de systèmes, comme SCCM et SSH.

Le principe de la *Security Automatisation,* et non de l'IA, est bel et bien de remplacer le travail de l'analyste par celui d'une machine. La machine collecte les informations, les agrège en les confrontant à une base de suspicions connues pour enclencher *in fine* les protocoles de remédiation et la communication aux utilisateurs, dès lors évidemment que la réponse à ce type d'alertes est d'ores et déjà identifiée.

Zoom sur la *Cyber Threat Intelligence*

La *Cyber Threat Intelligence* a pour but de collecter et d'organiser toutes les informations liées aux cybermenaces afin de dresser un portrait des attaquants et d'en dégager des tendances (méthodes et techniques d'exploitation, secteurs touchés…). La CTI permet de connaître, de mieux se défendre et d'anticiper pour détecter les prémices d'une attaque.

Le terme *Threat Intelligence* est apparu début 2011, lorsque les premières APT (*Advanced Persistent Threats*) ont été largement médiatisées. Certaines organisations et entités étatiques utilisent ce concept depuis plus longtemps.

Les informations collectées peuvent être de différentes natures : marqueurs, IOC (indicateurs de compromissions tels que des *hash,* des noms de domaines ou des adresses IP), historiques d'attaques, réutilisation d'architecture ou de platement ayant servi antérieurement, utilisation de services, techniques et méthodes spécifiques (signatures communes, registrant identique).

Les moyens de collecte existants sont nombreux. On retrouve notamment le renseignement *Open Source* (OSINT), la *Social Media Intelligence* (SMI ou SOCMINT), les flux de données commerciaux et communautaires, les informations provenant du *Deep* ou du *Dark Web*, ou encore le renseignement d'origine humaine et la capacité d'analyse et de corrélation (HUMINT).

(1) *Endpoint Detection and Response.*

Dans une volonté globale de développer des standards réutilisables par le plus grand nombre, les moyens d'échanges ont tendance à s'harmoniser. De nombreuses initiatives, notamment *Open Source*, ont vu le jour pour favoriser la communication des informations CTI : STIX (*Structured Threat Information Expression*), MISP (*Malware Information Sharing Platform*), TAXII (*Trusted Automated eXchange of Indicator Information*). Cette transmission d'information permet également de générer des règles de détection pour des outils de supervision tels que les IPS.

L'intérêt d'implémenter un programme de *Cyber Threat Intelligence* au sein de son entreprise ou organisation est donc réel. Mais il faut tout d'abord se poser les bonnes questions. En effet, toutes les données ne sont pas significatives, il faut donc cadrer le programme de renseignements sur les cybermenaces en amont du projet. Il faut dans un premier temps définir les enjeux et les conséquences d'une atteinte à la sécurité de l'entreprise : qu'est-ce qui doit être protégé ? Quelles informations un attaquant voudrait-il obtenir ou détruire ? Lorsque les réponses à ces questions ont été formalisées, il faut déterminer les objectifs liés à la mise en place d'un programme de CTI au sein de son organisation. Ils doivent être clairs et réalisables, mais doivent également être facilement mesurables grâce à des indicateurs et des critères fixés au préalable.

Une fois les besoins exprimés et les objectifs fixés, vient le temps de la collecte des données avec la mise en place de différents « capteurs », en exploitant par exemple des sources ouvertes accessibles sur Internet (OSINT).

Il faut ensuite passer sur la phase de traitement des données pour simplifier leur exploitation par les analystes. Toutes les informations collectées (IOC, *malwares*, contexte géopolitique, méthodes de groupes d'attaquants) doivent être contextualisées et enrichies pour se transformer en véritable renseignement. C'est à ce moment-là que nous entrons dans la phase d'analyse, qui repose encore aujourd'hui en grande partie sur l'expertise de l'analyste. À l'issue de son travail, il produira un rapport, qu'il conviendra de diffuser aux bonnes personnes, au bon moment et dans le bon format.

Les équipes qui peuvent être intéressées par la CTI sont multiples :

- la direction générale, les RSSI ou le DSI, doivent être alimentés par du renseignement stratégique sur les cybermenaces de leur secteur d'activité ;
- le *Risk Manager* et ses équipes doivent avoir une vision globale des véritables menaces cyber qui pèsent sur les différents métiers de leur organisation ;
- le *Security Operation Center* (SOC) a besoin de renseignement très opérationnel et contextualisé sur les dernières cybermenaces, sous forme d'IOC, de règles de détection / corrélation voire de stratégies de réponse / remédiation adaptées (bloquer telle IP, lancer une investigation sur tel périmètre, bloquer ce protocole vulnérable, etc.) ;
- le CERT/CSIRT (interne ou externe) aura tant besoin de renseignements stratégiques qu'opérationnels très contextualisés sur les groupes d'attaquants ciblant son organisation ou ses clients, afin d'accélérer ses investigations et ses réponses aux incidents de sécurité.

L'intelligence artificielle : le futur de la détection ?

Commençons cette dernière partie avec un peu de théorie, en définissant ce qui se cache derrière le terme « intelligence artificielle ». On peut la définir comme un ensemble de concepts, de théories et de techniques permettant de résoudre des problèmes à forte complexité logique ou algorithmique. On trouve plusieurs disciplines associées, comme la neurobiologie computationnelle, la logique mathématique ou l'informatique. Tout cela peut sembler complexe mais comme avec toutes les technologies, il faut se reconcentrer sur les besoins et exploiter l'IA à bon escient.

Zoomons sur les possibilités offertes par le *machine learning* pour la sécurité et la détection des menaces. Il y a eu de nombreux débats sur les différences entre *deep learning* et *machine learning*. Nous avons fait le choix du *machine learning*. Cela nous a semblé être une bonne solution pour la résolution de problèmes considérés comme insolubles par des algorithmes classiques.

Le *machine learning* nous aide à modéliser la normalité : c'est ce qu'on appelle une intelligence artificielle supervisée. L'algorithme va permettre de qualifier une situation donnée et d'en déterminer la distance par rapport à la normalité. Si l'écart est trop important, il faut qualifier cette « anormalité ». Cela peut donner lieu à une alerte (incident de sécurité ou fraude par exemple) ou à un faux-positif. L'avantage du *machine learning* réside dans le traitement des faux-positifs : on va apprendre à la machine que c'est un cas « normal » et que le modèle de normalité doit être enrichi pour éviter de faire deux fois l'erreur.

Les apports de l'intelligence artificielle et plus spécifiquement du *machine learning* sont multiples.

L'IA peut être utilisée pour mettre à jour les bases de données de sécurité. L'analyse des journaux provenant de plusieurs sources permet à l'intelligence artificielle de détecter de nouvelles menaces imminentes. Autrement dit, l'intelligence artificielle est capable de collecter des données exhaustives à partir de plusieurs journaux et enregistrements, et de faire les rapprochements qui permettent d'identifier de nouvelles menaces diffusées par les pirates.

Côté logiciels malveillants et logiciels espions, l'intelligence artificielle peut également identifier les tendances en analysant les données de plusieurs canaux. Grâce à la détection plus rapide des nouveaux systèmes malveillants, l'intelligence artificielle empêche les dommages de prendre une ampleur démesurée. On dispose ainsi de plus de temps pour rechercher les méthodes de prévention qui permettent de corriger les bogues ou les failles de sécurité susceptibles d'être exploités par le *malware* ou le virus.

Hormis la détection des transferts de *malwares* à grande échelle, l'intelligence artificielle peut également être utilisée pour analyser un système afin d'y détecter toute activité anormale. Le fait d'analyser un système en permanence permet de recueillir suffisamment de données permettant de conclure au caractère anormal de certaines activités et de créer un modèle de normalité.

Les utilisateurs peuvent être surveillés en permanence afin de détecter tout accès non autorisé. Si le système repère une activité anormale, l'IA peut exploiter certains paramètres pour déterminer en amont si la menace est réelle ou pas afin de la signaler.

Le *machine learning* peut être utilisé pour aider l'intelligence artificielle à distinguer ce qui doit être considéré comme une activité « normale » d'une activité « anormale ». Plus le *machine learning* se perfectionne, plus l'IA gagne en efficacité pour déceler de légères anomalies potentiellement révélatrices d'un problème. Comme évoqué plus haut, l'important est de pouvoir faire les rapprochements nécessaires. Certaines anomalies mineures paraîtront insignifiantes en soi, mais prises ensemble, elles permettent de se faire une idée plus complète des causes sous-jacentes. L'IA est capable d'effectuer une analyse permanente d'un système, d'analyser plusieurs activités différentes et de les comparer, et de déclencher des alertes. L'intelligence artificielle met l'accent sur l'identification des points faibles, des bogues et des failles de sécurité potentiels. L'apprentissage machine peut, par exemple, être utilisé pour détecter à quel moment des données non fiables sont envoyées par une application. Les vulnérabilités de type « Injection SQL » sont l'une des failles les plus couramment exploitées par les logiciels malveillants et les virus pour dérober des données et accéder aux systèmes. Autre faiblesse que l'intelligence artificielle peut aider à détecter : le débordement de mémoire tampon ou transfert d'un volume de données inhabituellement élevé par une application dans une mémoire tampon. L'intelligence artificielle peut aussi avoir son utilité pour limiter l'erreur humaine. En effet, l'une des principales causes de violation de

la protection des données reste l'erreur commise par certains collaborateurs : l'IA permet d'en prévenir les dommages.

L'intelligence artificielle peut plus globalement déterminer les éventuelles vulnérabilités du système en effectuant un suivi des menaces actuelles, et notamment des *malwares*. En évoluant, l'intelligence artificielle ne détecte pas seulement les défauts d'un système ou d'une mise à jour en particulier, mais elle empêche aussi automatiquement l'exploitation de ces failles. Qu'il s'agisse d'ajouter des pare-feux supplémentaires ou de corriger des erreurs de codage à l'origine de vulnérabilités, l'IA offre un excellent moyen de prévention des problèmes.

Si la réponse peut ressembler à la prévention, cette phase a lieu ultérieurement : au moment où les logiciels malveillants se sont déjà introduits dans le système. Comme évoqué plus haut, l'intelligence artificielle peut être utilisée pour détecter les comportements anormaux et établir des corrélations afin de déterminer le profil d'un *malware* ou d'un virus dans le système.

Cette étape consiste à mettre en place la réponse appropriée face au *malware* ou au virus. Il s'agit de maîtriser les dommages, d'éliminer le virus du système, de corriger les éventuelles failles de sécurité et de mettre en place des protections supplémentaires pour éviter que le virus n'infecte à nouveau le système.

Si l'IA présente de nombreux avantages pour la cybersécurité, il y a encore une certaine marge de progression. La détection des anomalies empêche certes les accès non autorisés à un compte ou détecte les logiciels malveillants dès les prémices d'une attaque, mais elle peut également produire des faux positifs. L'intelligence artificielle peut réellement s'améliorer pour mieux repérer les activités vraiment anormales (car une connexion à partir d'un nouvel emplacement peut tout simplement signifier que l'utilisateur est en déplacement).

Les sociétés de sécurité et les éditeurs de logiciels continueront néanmoins à s'appuyer sur l'apprentissage machine pour réduire les délais de détection, augmenter les taux de détection, empêcher la propagation des logiciels malveillants, protéger les systèmes et accroître la sécurité des clients. Et si l'IA a encore beaucoup de chemin à parcourir, son impact commence à être tangible dans le domaine de la cybersécurité.

Souveraineté numérique et sécurité nationale

Par **Claire LANDAIS**
SGDSN
et **Julien BARNU**
Conseiller industrie et numérique

Notre souveraineté numérique, autrement dit notre capacité à rester maîtres de nos choix et de nos valeurs dans une société numérisée, recouvre trois enjeux complémentaires :

- préserver les composantes traditionnelles de notre souveraineté, à une époque où le numérique tend à remettre en question les monopoles régaliens – ce qu'on pourrait appeler la « souveraineté à l'ère du numérique » ;
- disposer dans le cyberespace d'une capacité autonome d'appréciation, de décision et d'action : il s'agit ici d'une « souveraineté dans l'espace numérique » ;
- maîtriser nos réseaux, nos communications électroniques et nos données, ce que l'on pourrait qualifier de « souveraineté sur les outils du numérique ».

Souveraineté à l'ère du numérique

Les nouvelles technologies ont progressivement permis à des acteurs privés de rivaliser avec les États, en assumant des fonctions faisant historiquement l'objet de monopoles régaliens. Cette tendance, en partie irréversible, doit conduire chaque État à arbitrer entre les attributs de souveraineté qu'il choisit de préserver en priorité, et ceux qu'il peut accepter de déléguer à la sphère privée, le cas échéant de façon encadrée. On peut citer, de façon non exhaustive :

- Identifier les personnes : les réseaux sociaux, au premier rang desquels Facebook avec Facebook Connect, jouent dorénavant le rôle de fournisseurs d'identité. Les services d'identification qu'ils proposent sont déjà largement utilisés, à ce stade par des sites Internet privés et pour des utilisations non sensibles. Sans réponse des États, de telles solutions pourraient, à moyen terme, devenir de fait les identités numériques d'usage. L'Europe et la France ont cependant apporté une réponse consistant à :
  – encadrer la fourniture d'identité numérique par le secteur privé : la loi pour une République numérique de 2016 prévoit que seules les solutions d'identité numérique répondant à un cahier des charges établi par l'Agence nationale de la Sécurité des Systèmes d'Information peuvent être présumées fiables ;
  – développer une identité numérique souveraine, avec le projet AliceM du ministère de l'Intérieur, en attendant le déploiement du parcours d'identification numérique qui fait actuellement l'objet d'une mission interministérielle, et mettre en place une plateforme – France Connect, conçue et opérée par la direction interministérielle du numérique – permettant de fédérer différents fournisseurs d'identité, privés comme publics, pour l'accès en ligne aux services publics ou à des services tiers ;
  – au niveau européen, introduire un cadre juridique commun (le règlement européen dit « eIDAS ») qui prévoit la reconnaissance entre les États membres et l'interopérabilité des identifications numériques nationales.

- Attaquer et défendre : face à une menace cyber qui ne cesse de croître, certains acteurs, essentiellement étatsuniens, remettent en cause le monopole des États dans l'usage de la violence légitime et font la promotion d'une doctrine offensive de réponse aux attaques, autorisant une riposte par les acteurs privés eux-mêmes (*hack back*) qui se fonde sur une interprétation discutable du droit à la légitime défense. Le risque de légalisation de pratiques de *hack back* dans certains pays et de leur diffusion au niveau international est bien réel. Or, permettre à des acteurs privés de mener des actions offensives est de nature à aggraver l'instabilité du cyberespace, notamment au regard du risque qu'une action de riposte non encadrée prenne pour cible un tiers innocent ou engendre des dommages collatéraux. Dans ce contexte, la France a choisi de maintenir l'interdiction actuellement en vigueur de cette pratique en droit français et de prôner activement son interdiction au niveau international. Ainsi, l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, rendu public par le ministre de l'Europe et des Affaires étrangères le 12 novembre 2018 au Forum de Paris sur la Paix, et soutenu par le président de la République à l'occasion de son discours à l'UNESCO devant le Forum sur la gouvernance de l'Internet, a été l'occasion de réaffirmer le monopole étatique de la violence légitime. Cette initiative se décline aujourd'hui de façon opérationnelle dans différents forums, notamment à l'OCDE et à l'ONU ;
- Assurer la sécurité intérieure : l'efficacité de nos services d'enquête judiciaire et de renseignement repose dorénavant sur des technologies numériques pour lesquelles les offres nationale et européenne sont lacunaires, ce qui nous conduit à dépendre d'offres étrangères, par exemple pour le traitement de données massives. Il est donc essentiel que l'État travaille de concert avec l'industrie pour faire émerger des solutions nationales ou européennes. C'est dans la poursuite de cet objectif que le Conseil de l'innovation d'avril 2019 a retenu un grand défi sur l'application de l'intelligence artificielle à la cybersécurité : « Comment automatiser la cybersécurité pour rendre nos systèmes durablement résilients aux cyberattaques ? ». Ce grand défi doit déboucher sur des solutions novatrices au profit des entreprises pour détecter des intrusions informatiques sophistiquées et corriger automatiquement des failles.

D'autres tendances de cette nature pourraient être évoquées ici, comme la remise en cause par les cryptomonnaies du monopole régalien à battre monnaie, mais cette question sort du champ de compétence du SGDSN.

Souveraineté dans l'espace numérique

La seconde facette de notre souveraineté numérique est le maintien de la capacité de l'État et, dans un certain sens, de nos entreprises et citoyens, à disposer d'une autonomie d'appréciation, de décision et d'action dans le cyberespace.

En ce qui concerne l'État, la France a choisi de se donner les moyens de conserver une autonomie de décision en matière de défense et de sécurité du cyberespace. L'atteinte de cet objectif repose sur :

- une capacité souveraine à détecter les attaques informatiques qui affectent l'État et les infrastructures critiques. Ainsi, l'ANSSI développe ses propres systèmes de détection pour la supervision des administrations, et des travaux ont permis de faire émerger des solutions industrielles de confiance pour la France au profit des entreprises. L'ANSSI a ainsi qualifié en avril 2019 les sondes de détection de deux industriels français. En outre, nos capacités nationales de détection ont été significativement renforcées par la loi de programmation militaire pour 2019-2025, qui permet aux opérateurs télécoms de mettre en œuvre des dispositifs de détection au sein de leur réseau et à l'ANSSI de déployer une sonde sur le réseau d'un hébergeur infecté par un attaquant. Ce mécanisme entre désormais dans une phase de mise en œuvre pratique ;

- une capacité souveraine à attribuer les cyberattaques. Le choix de développer et de maintenir une telle capacité est un choix d'engagement majeur. La maîtrise de telles capacités ne sera accessible à terme qu'à un nombre très limité de pays qui auront fait le choix stratégique de les détenir ;
- une doctrine nationale de découragement et de réaction, reposant sur :
  – une méthode nationale d'évaluation de la gravité d'une cyberattaque, intégrant nos normes juridiques (Code pénal, Code de la défense, Règlement général sur la Protection des Données, etc.). Appelé par la « Revue stratégique de cyberdéfense », un schéma de classement des cyberattaques a ainsi été préparé par l'ensemble des acteurs de la cyberdéfense ;
  – une doctrine nationale de réponse, fondée sur le principe que la réponse résulte d'une décision politique formulée au cas par cas à la lumière des critères établis par le droit international. La réponse peut se traduire par une attribution publique, par l'adoption de contre-mesures voire, dans la mesure où il n'est pas exclu qu'une cyberattaque puisse atteindre le seuil de l'agression armée, par le recours à la légitime défense au sens de l'article 51 de la Charte des Nations Unies ;
- des capacités offensives permettant, face au risque d'agression armée, de disposer d'options de réponse de nature militaire dans le milieu cyber comme dans les autres milieux. L'arme cyber est aujourd'hui pleinement intégrée parmi les capacités opérationnelles des armées, et fait l'objet d'une doctrine qui encadre son emploi dans les opérations militaires sur les théâtres d'opérations extérieurs, dans le respect du droit international ;
- la promotion à l'international de notre vision selon laquelle (i) le droit international est applicable au cyberespace, et (ii) l'attribution publique est une décision politique qui relève de la souveraineté et ne peut être faite par une structure interalliée comme l'OTAN.

Pour nos entreprises, il s'agit de préserver une capacité à innover, dans un contexte d'hégémonie, des géants américains du numérique – là encore, ce domaine sort du champ de compétence du SGDSN.

Enfin, l'autonomie d'appréciation et de décision de nos citoyens passe par la sincérité du débat démocratique, face au phénomène émergent de manipulation de l'information par des puissances étrangères. Le rôle de l'État, s'il reste prépondérant pour lutter contre ces manipulations (régulation, impulsion, coopération internationale, etc.), doit bénéficier de relais dans la société civile et avoir pour objectif essentiel de renforcer les « anticorps » de la démocratie : intelligence du débat public, transparence du fonctionnement des plateformes, éducation aux médias, soutien au pluralisme.

Souveraineté sur les outils du numérique

Notre souveraineté numérique passe enfin par notre capacité à protéger nos réseaux de télécommunications, et les données qui y transitent, des actions d'espionnage et de sabotage.

En matière de sécurité et de résilience des réseaux, des dispositions législatives existent depuis plusieurs années et permettent un contrôle des équipements qui constituent le cœur des réseaux. Toutefois, au regard de l'importance croissante prise par les réseaux mobiles, et notamment dans le futur par la 5G et les nouveaux usages qu'elle permettra, il a été jugé nécessaire d'apporter des évolutions au cadre juridique actuel. C'est dans ce contexte qu'a été adoptée la loi n°2019-810 du 1er août 2019 soumettant à autorisation préalable du Premier ministre l'exploitation de certains équipements des réseaux mobiles pour les opérateurs télécoms qui sont opérateurs d'importance vitale.

De façon complémentaire, la maîtrise de nos réseaux passe par la protection de nos câbles sous-marins de télécommunications, essentiels au bon fonctionnement de notre économie. Au-delà du renforcement de leur protection, le gouvernement conduit une politique ambitieuse d'attractivité

de notre territoire pour la pose de câbles : la multiplication de leurs atterrages en France permettra d'accroître la résilience de nos flux de télécommunications internationaux.

En matière de protection des données et des communications de l'État, des entreprises et des citoyens, la diversité des enjeux nous conduit à décliner le niveau d'ambition de la France en différentes sphères :

- Pour les données et communications classifiées, nous devons viser une obligation de résultat, garantissant leur protection contre des attaques ciblées des adversaires les plus compétents. Cette ambition implique la maîtrise nationale de certaines technologies, au premier rang desquelles le chiffrement des communications. La France possède dans ce domaine une industrie de confiance, apte à fournir des équipements de très haut niveau de sécurité, agréés pour protéger les données échangées de niveau de classification Secret Défense. Le maintien d'une industrie nationale à la pointe dans ce domaine est une absolue priorité ;
- Pour le champ plus étendu des données et communications sensibles, nous devons fixer les contraintes auxquelles doivent se plier les solutions numériques utilisées par l'État et les opérateurs critiques. Il est illusoire de chercher à répondre à l'ensemble de ces besoins par des solutions purement nationales. Sans exclure fondamentalement des fournisseurs étrangers, cet objectif nécessite de disposer en France d'un tissu industriel de confiance, capable de produire des briques élémentaires de sécurité, mais aussi de concevoir des systèmes complexes en y intégrant des briques étrangères ;
- Pour le champ plus large de la sécurité économique des entreprises non vitales et de la protection des usages numériques des citoyens, l'État doit préserver sa capacité d'influence des choix numériques des acteurs concernés, en identifiant des solutions de qualité sans les imposer. À cette fin, l'ANSSI généralisera progressivement son dispositif de labellisation à l'ensemble des solutions numériques, afin d'encourager le recours aux meilleures solutions. Ce dispositif gagnera en pertinence économique grâce à son extension à l'échelon européen, permise par le *Cybersecurity Act* adopté le 12 mars dernier par le Parlement européen.

Cette déclinaison en trois sphères s'applique pleinement à la question du *cloud*. Ainsi, pour ses données classifiées, l'État aura recours exclusivement à un *cloud* interne. En revanche, pour d'autres données publiques et pour les besoins des entreprises, la qualification des *clouds* par l'ANSSI permettra d'identifier les offres – pas nécessairement nationales – qui apportent des garanties suffisantes vis-à-vis des risques tant techniques (risque d'attaque informatique) que juridiques (contraintes de mise à disposition des données à des autorités étrangères).

Protection des infrastructures critiques : cinq ans après la loi

Par **Yves VERHOEVEN**
Agence nationale de la Sécurité des Systèmes d'Information (ANSSI)

Génèse d'un dispositif réglementaire

Émergence d'une préoccupation globale

Les enjeux de cybersécurité sont désormais bien connus : aux vagues successives de virus subies par le grand public depuis le début des années 2000 viennent s'ajouter les révélations d'attaques ciblées hautement sophistiquées, conduites à l'initiative d'États. Outre des activités de cyberespionnage, ces révélations ont mis au jour des attaques de sabotage contre des infrastructures soutenant des activités économiques ou industrielles, à l'image de l'opération Olympic Games contre les centrifugeuses iraniennes en 2010, de la cyberattaque à des fins de sabotage contre la chaîne TV5Monde en 2015, ou encore des attaques en 2015 et 2016 contre la grille électrique ukrainienne, privant d'électricité plusieurs centaines de milliers de foyers ukrainiens.

Ces événements éclairent *a posteriori* les préoccupations des premiers pays qui, dès la fin du XX^{e} siècle, ont identifié le risque de déstabilisation majeure des cyberattaques et ont commencé à se mobiliser. Ainsi, la première résolution de l'Assemblée générale des Nations Unies sur le sujet (résolution 53/70 issue du premier comité sur le désarmement et la sécurité internationale à l'initiative de la Russie, « Les progrès de la téléinformatique dans le contexte de la sécurité internationale ») date du 4 janvier 1999.

La cybersécurité des infrastructures critiques est rapidement apparue prioritaire, puisque la poursuite des travaux sur le sujet au sein des Nations Unies a abouti en 2004 à la résolution 58/199 portant sur la « Création d'une culture mondiale de la cybersécurité et protection des infrastructures essentielles de l'information ». Dans cette résolution, l'Assemblée générale « note que désormais, par suite des progrès de l'interconnectivité, les infrastructures essentielles de l'information se trouvent exposées à des menaces et à des faiblesses toujours plus nombreuses et diverses qui donnent lieu à de nouvelles préoccupations en matière de sécurité » et « invite les États membres et toutes les organisations internationales compétentes à tenir compte, notamment, de ces éléments et de la nécessité de la protection des infrastructures essentielles de l'information ».

Quelques années plus tard, en 2008, c'est l'Organisation de coopération et de développement économique (OCDE) qui produit, *via* son groupe de travail sur la sécurité de l'information et la vie privée, et adopte lors de sa 1 172^{e} session, le 30 avril 2008, la « Recommandation de l'OCDE du Conseil sur la protection des infrastructures d'information critiques [C(2008)35] ». Dans celle-ci, le Conseil de l'OCDE « [reconnaît] que le fonctionnement de nos économies et de nos sociétés est de plus en plus tributaire de systèmes et réseaux d'information qui sont interconnectés et interdépendants, au plan tant intérieur qu'international ; qu'un certain nombre de ces systèmes et réseaux sont d'une importance nationale critique ; et que leur protection est un domaine prioritaire pour la politique publique nationale et la coopération internationale ».

L'action de la France

Ces recommandations trouvent une traduction concrète en France à partir de 2008, *via* le Livre blanc sur la défense et la sécurité nationale. La menace contre la nation liée aux cyberattaques

y figure pour la première fois parmi les menaces stratégiques, en troisième position en raison de sa probabilité élevée de survenue et de l'impact majeur qu'elle est susceptible d'avoir. Cette orientation amène la France à créer l'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI) dès 2009. Celle-ci commence rapidement à travailler avec des opérateurs publics et privés d'infrastructures critiques, en développant un modèle de coopération public-privé aujourd'hui encore envié à l'étranger. Mais il faut attendre 2011 et l'article L33-10 du Code des postes et communications électroniques pour que les opérateurs de communication électronique soient les premières infrastructures critiques en France à voir leur cybersécurité régulée. Et ce n'est pas avant 2013 qu'apparaît une orientation explicite sur la cybersécurité de l'ensemble des infrastructures critiques pour la défense et la sécurité nationale.

Le Livre blanc sur la défense et la sécurité nationale de 2013 comporte un chapitre sur « la lutte contre la cybermenace », qui prévoit : « S'agissant des activités d'importance vitale pour le fonctionnement normal de la Nation, l'État fixera, par un dispositif législatif et réglementaire approprié, les standards de sécurité à respecter à l'égard de la menace informatique et veillera à ce que les opérateurs prennent les mesures nécessaires pour détecter et traiter tout incident informatique touchant leurs systèmes sensibles. Ce dispositif précisera les droits et les devoirs des acteurs publics et privés, notamment en matière d'audits, de cartographie de leurs systèmes d'information, de notification des incidents et de capacité pour l'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI), et, le cas échéant, d'autres services de l'État, d'intervenir en cas de crise grave. » Ce sont ainsi plus de 250 Opérateurs d'Importance vitale (OIV), publics et privés, dont la liste est classifiée, qui devront désormais respecter des exigences de cybersécurité en plus des exigences de sécurité physique déjà applicables.

Cette orientation du Livre blanc sur la défense et la sécurité nationale se concrétise par l'article 22 de la loi de programmation militaire (LPM) du 18 décembre 2013, qui crée les articles L1332-6-1 à L1332-6-6 du Code la défense. L'ANSSI se voit attribuer la capacité de fixer les exigences de sécurité pesant sur les systèmes d'informations dits « d'importance vitale » (SIIV) ainsi que de réaliser ou faire réaliser des contrôles sur ces systèmes. Les OIV doivent aussi déclarer à l'ANSSI les incidents affectant leurs SIIV. Ce cadre prévoit par ailleurs la capacité pour l'ANSSI de qualifier des prestataires pour réaliser certains types de prestations requises par la réglementation (notamment audits et détection d'incidents de sécurité). Enfin, chaque manquement aux exigences de ce cadre réglementaire peut être sanctionné pénalement par une amende de 150 000 euros.

Même si l'ANSSI est positionnée comme régulateur trans-sectoriel en matière de cybersécurité, il est évident que cette autorité ne saurait être exclusive de l'autorité que les ministères et les régulateurs sectoriels peuvent avoir sur leurs OIV. Il est donc attendu que l'ANSSI, les ministères de tutelle des OIV et les régulateurs sectoriels se coordonnent afin d'assurer une articulation efficace entre les politiques publiques dont ils sont responsables.

Alors que la France avait accumulé un retard de près d'une décennie par rapport aux pays les plus avancés dans la prise en compte du besoin de cybersécurité pour ses infrastructures critiques, ce cadre réglementaire en a fait un pays précurseur en la matière.

La mise en œuvre des dispositions légales

La finalisation du cadre réglementaire

Vu l'impact potentiel de cette réglementation nouvelle et le besoin d'acceptabilité de la part des OIV, l'ANSSI a opté pour une co-construction des textes d'application avec les opérateurs concernés. L'année 2014 a ainsi été utilisée pour conduire des expérimentations avec quelques OIV. Les années suivantes ont été consacrées à la conduite de groupes de travail sectoriels afin de définir les règles applicables aux OIV, en tenant compte des spécificités sectorielles. À l'issue de

plus de 200 réunions de travail, les arrêtés sectoriels ont ainsi été produits pour chacun des secteurs d'activité d'importance vitale. Tous comportent vingt règles de sécurité informatique autour des thématiques suivantes : gouvernance, gestion des risques, protection, détection, réaction et gestion de crise. Ces règles correspondent à des bonnes pratiques et ont chacune des délais propres pour la mise en conformité des OIV.

Les arrêtés sectoriels résultant de ce processus sont entrés en vigueur par vagues :

- 1er juillet 2016 : alimentation, gestion de l'eau, produits de santé ;
- 1er octobre 2016 : transports et énergie (hors nucléaire) ;
- 1er janvier 2017 : finances, audiovisuel, communications électroniques et Internet, industrie ;
- 1er avril 2017 : nucléaire civil ;
- 1er octobre 2017 : activités industrielles de l'armement, espace ;
- 1er octobre 2019 : activités civiles de l'État.

La définition d'un plan de réponse aux crises majeures cyber

L'article 22 de la LPM prévoit des dispositions relatives à la gestion de crise : « Pour répondre aux crises majeures menaçant ou affectant la sécurité des systèmes d'information, le Premier ministre peut décider des mesures que les opérateurs mentionnés aux articles L.1332-1 et L.1332-2 doivent mettre en œuvre. »

L'État s'est doté d'un plan de gestion des crises d'origine cyber, PIRANET, pour se préparer à un scénario où des OIV seraient atteints afin de produire un effet incapacitant sur la Nation. En complément, des exercices sont régulièrement organisés afin de tester le niveau de préparation des différentes parties prenantes, notamment les services de l'État et les OIV : CyberEurope au niveau européen, PIRANET au niveau national, ou encore des exercices sectoriels à l'initiative de régulateurs sectoriels ou des opérateurs eux-mêmes. L'ANSSI apporte plusieurs fois par an, outre sa participation, son expertise en matière de planification et d'organisation d'exercices en soutien à l'organisation de tels exercices.

La mise en conformité des OIV

Le travail de sensibilisation et d'assistance de l'ANSSI auprès de certains OIV avait déjà bien démarré au moment de l'adoption de la LPM de 2013, notamment auprès des OIV victimes de cyberattaques. Un certain nombre de systèmes d'information voués à être déclarés SIIV étaient donc déjà sécurisés de manière appropriée avant la publication des arrêtés sectoriels les concernant.

Formellement, la publication de chaque arrêté sectoriel appelle la déclaration sous trois mois à l'ANSSI de la liste des SIIV de chaque OIV du secteur. Fin 2018, plus de 1500 SIIV avaient été déclarés à l'ANSSI, preuve d'une approche volontaire de la vaste majorité des OIV. Aujourd'hui, aucun manquement n'a encore justifié d'amende.

Autre signe de dynamisme dans la mise en conformité des SIIV aux exigences réglementaires : la saturation des carnets de commande des prestataires qualifiés en matière d'assistance à la sécurisation des SIIV.

La principale mesure restant en suspens jusqu'à récemment était la règle exigeant le recours à des systèmes de détection qualifiés par l'ANSSI, en raison de l'absence d'une offre suffisante. Ce point a été levé en avril 2019 avec la qualification des sondes de Thales et Gatewatcher.

La qualification des prestataires

Vu l'ampleur du chantier de la sécurisation de l'ensemble des SIIV, la loi a d'emblée prévu la possibilité pour l'ANSSI de déléguer des activités à des prestataires privés. Dans le cadre des Visas de sécurité de l'ANSSI, on retrouve deux catégories :

- Les prestataires d'audit en sécurité des systèmes d'information (PASSI), qui réalisent des audits obligatoires préalablement à l'homologation des SIIV, peuvent offrir des services de conseil en sécurisation des SIIV, et peuvent assurer des contrôles par délégation de l'ANSSI ;
- Les prestataires de détection d'incidents de sécurité (PDIS), qui opèrent les systèmes de détection qualifiés exigés par la réglementation.

Ces prestataires jouent un rôle-clé dans la mise en œuvre de la réglementation française sur la cybersécurité des OIV. De plus, la création de ces catégories a permis de structurer le marché. En septembre 2019, on peut compter 13 PASSI qualifiés et 4 PDIS qualifiés.

Une approche ambitieuse de la cybersécurité des infrastructures critiques

La directive européenne pour la cybersécurité des opérateurs de services essentiels

S'inspirant de la démarche française, l'Union européenne a entamé en 2013 des travaux en vue d'adopter une directive de même nature. La négociation s'est conclue par l'adoption et l'entrée en vigueur le 6 juillet 2016 de la directive 2016/1148 (dite « directive NIS »). La directive appelle à se doter d'une stratégie de cybersécurité, d'une autorité nationale compétente en la matière, et de capacités techniques ayant vocation à fonctionner en réseau. Elle impose également la mise en place d'un cadre très similaire dans sa structure à celui existant en France pour la cybersécurité des OIV. La France a ainsi su préserver et promouvoir son approche durant les négociations. Pour autant, la directive s'appuie sur une base juridique relative au bon fonctionnement du marché intérieur. La défense et la sécurité nationale constituent une prérogative exclusive des États membres. Les opérateurs régulés au titre de la directive sont donc qualifiés d'opérateurs de services essentiels (OSE) à l'économie ou à la société, relativement à l'impact disruptif que pourrait avoir un dysfonctionnement d'un de leurs systèmes d'information dits « essentiels » (SIE).

La vaste majorité des États membres ont choisi d'utiliser la loi de transposition pour couvrir de manière indiscriminée les champs relatifs au bon fonctionnement de l'économie et de la société d'une part, et de la défense et la sécurité nationale d'autre part. La France a quant à elle choisi de dupliquer le dispositif existant dans le Code de la défense, pour produire un cadre sur une base juridique distincte, couvrant des activités complémentaires de celles couvertes par la LPM.

Par ailleurs, la France a fait le choix d'une transposition très ambitieuse. Elle ne s'est pas restreinte à la liste minimale de services essentiels figurant en annexe de la directive NIS, mais a ajouté de nouveaux secteurs.

À ce jour, la désignation des OSE est en cours d'instruction en France.

Approche française du droit international autour des infrastructures critiques

En s'appuyant sur son expérience, la France a entrepris deux actions visant à soutenir la sécurité internationale et à éviter des déstabilisations du cyberespace liées à des actes inappropriés.

La première action a consisté en la promotion en 2015, au sein du groupe d'experts gouvernementaux des Nations Unies, du principe de diligence requise cyber *(cyber due diligence)*. Ce principe, acté dans la résolution 70/174, prévoit que : « Les États devraient répondre aux demandes d'aide appropriées formulées par un autre État dont une infrastructure essentielle est exposée à des actes de malveillance informatique ; ils devraient aussi répondre aux demandes appropriées visant à atténuer les conséquences d'activités informatiques malveillantes dirigées contre une infrastructure essentielle d'un autre État et exercées depuis leur territoire, en tenant

dûment compte de la souveraineté. » Cette approche conforte le principe de souveraineté des États dans le cyberespace, appelant prioritairement à la coopération. Elle délégitime de fait une intervention de l'État victime chez des États involontairement impliqués, pourvu que ceux-ci répondent de manière efficace aux demandes de coopération de l'État victime.

La seconde action de la France a consisté à se doter, en 2018, à l'occasion de la publication de la « Revue stratégique de cyberdéfense », d'une échelle de classement de la gravité des incidents cyber en fonction de leurs conséquences « dans le monde réel ». L'objectif est de donner les clés aux autorités politiques pour appréhender le niveau de gravité des attaques, et d'ajuster la nature de la réponse à la crise. Cette approche, inspirée de travaux anglo-saxons, constitue désormais la clé de voûte de la politique française de réponse aux cyberattaques. Elle est promue au sein de l'Organisation pour la sécurité et la coopération en Europe (OSCE) et est discutée dans les travaux des Nations Unies.

Conclusion

Les dispositifs réglementaires français en matière de cybersécurité permettent d'appréhender largement la cybersécurité des infrastructures critiques, et ont fait de la France une pionnière en la matière.

Malgré une approche ambitieuse, certains systèmes critiques ne sont pas encore couverts par ces réglementations, tels que les dispositifs médicaux, les véhicules autonomes, les machines à voter et le vote électronique. La prise en compte de la cybersécurité dans ces systèmes nécessite aujourd'hui une forte coopération avec les autorités sectorielles. L'objectif sera qu'elles intègrent des exigences de cybersécurité, conformément à l'approche promue par la « Revue stratégique de cyberdéfense » de 2018.

Retour sur la genèse de la cyberdéfense militaire française

Par le Général de division aérienne **Didier TISSEYRE**
Officier général commandant de la cyberdéfense

Introduction

Il y a cinquante ans, en 1969, la DARPA [1] déployait aux États-Unis le réseau ARPAnet [2], dédié aux forces armées américaines. Vingt ans plus tard, ARPAnet laissait la place à Internet et au *World Wide Web*. Ainsi, la numérisation (ou *digitisation*) du monde débute autour du plus vaste « objet » artificiel créé par l'homme au XX^{e} siècle : le cyberespace. L'espace numérique, ou cyberespace, est un domaine d'innovation et de confrontation à la fois nouveau et en constante évolution. Nouveau, il nécessite d'être enraciné de façon solide pour continuer à se développer, tout en assurant la sécurité et la protection de ceux qui y opèrent ; en évolution constante, il requiert une approche agile et la remise à plat de nos organisations et de nos rapports de pouvoir.

Depuis 2011, le ministère de la Défense, puis des Armées, et en particulier le Commandement de la cyberdéfense, son bras armé, construisent de façon solide et pérenne un modèle agile et efficace de cyberdéfense.

Le cyberespace a sa propre dynamique, liée à une expansion technique qui semble ne pas connaître de limite : hier l'interconnexion des réseaux, aujourd'hui le développement des puissances de calcul dans l'exploitation des données, demain l'explosion du nombre d'objets connectés, après-demain les processeurs quantiques. Internet constitue probablement la révolution technique humaine la plus innovante : il est source de richesses et vecteur de connaissances, ainsi que de nouveaux modèles économiques et culturels. Il raccourcit les distances et rapproche les individus. Le centre de gravité de nos sociétés, jusqu'alors essentiellement lié à des populations et à des territoires, se déplace progressivement dans ce nouvel espace. La dépendance au numérique s'accroît au rythme des progrès techniques et renforce par là même l'exposition à des vulnérabilités nouvelles.

La plupart des luttes de pouvoir, des crises et des conflits contemporains connaissent désormais, et ce, systématiquement, un développement dans le cyberespace. Les armées doivent appréhender le combat cybernétique comme une fonction stratégique à part entière dont les effets se combinent aux autres dans une manœuvre globale.

Un nouvel espace de confrontation

Véritable rupture en termes de technologie et d'emploi de la force, l'arme cyber est amenée à bouleverser les modalités de la guerre sans en renouveler profondément les principes. Multiplicité d'acteurs étatiques, masqués ou non, organisations terroristes ou criminelles, frontières gommées, perceptions troublées, repères faussés, propagation rapide, droit international non respecté, code de conduite bafoué : tels sont les risques du cyberespace. Une zone grise, un brouillard, dont les effets sont, eux, bien réels, parfois dévastateurs. Le combat dans le cyberespace est de nature asymétrique, hybride, parfois invisible et en apparence indolore. Pourtant, l'emploi de l'arme

(1) *Defense Advanced Research Projects Agency.*
(2) *Advanced Research Projects Agency Network.*

cyber est susceptible de porter gravement atteinte aux capacités et aux intérêts souverains des États.

Nous pouvons aujourd'hui définir quatre grandes catégories de cybermenaces : l'atteinte à l'image (défigurations de sites officiels, campagnes de dénigrement, usurpation d'identité, propagande, amplification de rumeurs, déstabilisation…), l'action « mafieuse » (arnaques à la carte bancaire, rançons, trafics en tous genres…), l'espionnage (détournements discrets d'informations circulant sur les réseaux numériques d'une cible) et le sabotage (altération du fonctionnement d'un système par le biais d'une attaque informatique).

Ces menaces, qui naissent dans le cyberespace, ont les mêmes caractéristiques que celles de l'espace physique : des individus malfaisants préparent des actes terroristes, désinforment, leurrent, volent ou encore détruisent. Les frontières qui séparent ces acteurs (cybercriminels, hacktivistes, États, groupes terroristes, etc.) sont poreuses et la diversité des menaces qu'ils génèrent est extrêmement grande, allant de l'attaque sur un système de vote électronique à la paralysie de médias, en passant par l'extinction d'un système électrique. Ces scénarios s'appuient sur des réalités profondément asymétriques : de faibles moyens permettent d'obtenir des effets stratégiques, analogues à ceux d'actions plus conventionnelles, en particulier lorsqu'ils visent des infrastructures civiles critiques, ou des capacités militaires cruciales dont dépend notre souveraineté.

La fréquence et l'ampleur des attaques augmentent sans cesse dans le cyberespace, témoignant d'une prolifération préoccupante des moyens d'agression. Si peu d'États disposent pour l'heure des moyens de mener des actions cyberoffensives de grande ampleur, causant des dommages importants, leur nombre et leurs capacités devraient s'accroître rapidement, favorisés par le faible coût et par la diffusion rapide des technologies numériques. Ensuite, l'arme cyber d'État, dont la conception nécessite parfois des moyens colossaux, est susceptible d'être copiée et répliquée très facilement. Utilisant déjà Internet à des fins de planification, de propagande et de recrutement, les groupes terroristes pourraient devenir des acteurs à part entière du domaine cyber. Il existe, enfin, une réelle difficulté dans la détermination de l'origine des attaques.

Une montée en puissance rapide

Pour protéger, défendre et agir face à ces cybermenaces, la cyberdéfense française s'est construite grâce à la volonté gouvernementale et à sa prise en compte dans les lois de programmation militaire successives. Confrontée à des adversaires, des ennemis ou des concurrents dotés de capacités informatiques offensives, la France a bénéficié d'un ambitieux plan d'actions ministériel, fondé sur une doctrine et une organisation renouvelées, permettant à nos forces de se déployer et de conduire, face à cette menace, le combat numérique.

Le Livre blanc de la Défense et de la Sécurité nationale de 2008 avait fait état pour la première fois de la menace posée par le développement du cyberespace. La création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a suivi en 2009, puis celle du poste d'officier général de cyberdéfense au sein de l'état-major des armées en 2011. La structure de cyberdéfense n'a ensuite cessé, tout au long de ces huit années, de se développer pour s'adapter aux nombreux enjeux opérationnels. Le Livre blanc de 2013 est venu préciser qu'au sein de la doctrine nationale, la capacité informatique offensive, associée à une capacité de renseignement, concourt de façon significative à la posture de cybersécurité.

Le Pacte Défense Cyber 2014-2016 a ensuite mobilisé le ministère des Armées dans l'objectif de faire de la France une grande puissance militaire de la cyberdéfense et de faire émerger une communauté nationale de cyberdéfense. Le « changement d'échelle » annoncé souligne la nécessité d'industrialiser la cyberdéfense militaire de la France. En octobre 2015 est créé le centre

des opérations de cyberdéfense (CO CYBER), qui a pour mission de planifier et de conduire les opérations militaires dans le cyberespace.

Le chemin accompli en une décennie est à la mesure de l'enjeu et des ambitions de la France de devenir une grande puissance cyber.

Le COMCYBER, Commandement de la cyberdéfense

Cette montée en puissance franchit un seuil symbolique très important en 2017 avec la création, par décret, du Commandement de la cyberdéfense (COMCYBER), qui est désormais – à l'intérieur de l'état-major des armées – l'organisme de référence et de tutelle des opérations militaires dans le cyberespace. Plus récemment, la « Revue stratégique de défense et de sécurité nationale », publiée en octobre 2017, la « Revue stratégique de cyberdéfense », publiée en février 2018, et la Loi de Programmation militaire 2019-2025, publiée en juillet 2018, consacrent un rôle majeur à la cyberdéfense militaire en lui conférant une plus grande visibilité et en augmentant ses moyens financiers et humains. Le 18 janvier 2019, la France, par la voix de la ministre des Armées, reconnaissait publiquement que la lutte informatique offensive figurait à son arsenal des moyens utilisables contre un adversaire, en réponse, ou non, à une agression préliminaire.

Pour garantir la souveraineté nationale dans le cyberespace, le ministère des Armées dispose de capacités lui permettant de se protéger contre les attaques informatiques, de les détecter et d'en identifier les auteurs. Il dispose également de la capacité à exploiter les failles informatiques d'un ennemi, en contexte de confrontation, et à maîtriser toutes les facettes du combat numérique. Le COMCYBER est directement placé sous l'autorité directe du chef d'état-major des armées, à l'image du Commandement des opérations spéciales.

Son décret de création précise qu'il est chargé de la protection et de la défense des systèmes d'information du ministère et de la conduite d'actions numériques à l'encontre des systèmes d'information adverses.

La cyberprotection consiste à bâtir d'épaisses murailles autour des systèmes d'information ainsi qu'à mesurer en permanence leur efficacité face à une menace toujours évolutive. La défense de ces systèmes vient en complément : plus dynamique, elle consiste à patrouiller, guetter, surveiller et intervenir sur les systèmes d'information en cas d'attaque, pour éradiquer la menace et reconstruire la muraille. L'action offensive, quant à elle, enrichit, avec l'arme numérique, la palette des options mises à la disposition de l'État. Le cyberespace est devenu un espace de confrontation à part entière au même titre que l'espace maritime, terrestre ou aérien, ou plus récemment l'espace exo-atmosphérique. Aujourd'hui, aucune opération militaire ne se conçoit sans cette dimension.

Le modèle actuel de ce commandement a été construit dans une logique d'économie des forces, de mutualisation des compétences et de concentration des efforts, mais aussi dans une logique de réseau, à l'instar de l'espace matériel et immatériel sur lequel il agit. Il permet une interaction fructueuse entre les acteurs du numérique étatiques et privés et assure une maîtrise des actions par l'intermédiaire d'une chaîne fonctionnelle dédiée. Le modèle français de cyberdéfense suit l'évolution sociétale actuelle : pour les citoyens utilisateurs du cyberespace, le ministère des Armées inspire sécurité et confiance ; il est le lieu privilégié de la création et de l'émulation d'une cyber-résilience. Le COMCYBER se veut fédérateur du ministère des Armées, et porteur d'une logique de renforcement des capacités interministérielles.

La défense de la France et de l'Europe doit s'adapter aux enjeux actuels et futurs du champ de bataille numérique. La supériorité opérationnelle de nos forces, c'est-à-dire la capacité à maîtriser des crises, comme celle d'entrer en premier sur un théâtre de conflit et à y contraindre un adversaire, passent désormais par la recherche et l'obtention de la supériorité dans le cyberespace.

C'est pourquoi la cyberdéfense au ministère des Armées est pensée dans l'action et construite dans la réalité d'un monde moderne qui a déjà réalisé sa transformation numérique.

Près de 3400 cybercombattants, répartis dans les armées et les différents services du ministère des Armées, sont placés sous l'autorité de l'officier général COMCYBER. Il appuie son action sur un état-major opérationnel d'environ soixante-dix personnes, organisé en quatre pôles.

Le ministère des Armées et le COMCYBER occupent une place singulière dans l'organisation nationale de la cyberdéfense. Cette dernière repose sur le principe de séparation des aspects défensifs et offensifs, et son organisation s'articule en trois grands partenaires, en plus du COMCYBER : l'ANSSI, la DGSE et la DGSI. Les aspects défensifs sont dirigés, au niveau gouvernemental, par l'ANSSI. Le ministère des Armées assure donc, par le biais du COMCYBER et en pleine coordination avec l'ANSSI, la défense de ses propres réseaux. Il peut, en outre, renforcer l'ANSSI si cette dernière le demande, au cas où notre pays serait victime d'une attaque cyber majeure.

Les moyens offensifs de la cyberdéfense sont détenus et mis en œuvre par le COMCYBER, en lien avec d'autres organismes. Sous l'autorité du chef des armées, il dirige l'emploi des moyens cyberoffensifs utilisés dans le cadre des opérations militaires.

Le COMCYBER s'appuie également sur un écosystème de partenariats internationaux. Comme pour tous les domaines sensibles dont la nature impose une culture forte du secret national – à l'instar du renseignement et des opérations spéciales – la cyberdéfense n'en est pas moins un domaine dans lequel des échanges internationaux, souvent sur un mode bilatéral, sont possibles, sinon indispensables. Ces coopérations prennent des formes diverses, de l'échange des bonnes pratiques à de véritables mécanismes de partage d'informations – permettant au COMCYBER d'affiner sa connaissance de la situation et de la menace cyber – jusqu'à la conduite d'opérations coordonnées. Balisées par des lignes rouges nationales, ces coopérations constituent aujourd'hui un levier de connaissance, d'efficacité opérationnelle et de rayonnement du COMCYBER au sein de la communauté militaire internationale de cyberdéfense.

Perspectives pour le futur

La montée en puissance de la cyberdéfense militaire se poursuit. Le passage à l'échelle évoqué plus haut est toujours d'actualité et de nombreux défis restent à relever.

En premier lieu se pose le défi de la ressource humaine. Cet aspect constitue d'ailleurs une des facettes du défi plus global de la numérisation du ministère des Armées. Il s'agit de recruter et de former les cybercombattants dont le ministère a besoin pour opérer dans le cyberespace, à un niveau qui soit à la hauteur des enjeux qui se posent à nous. Le recrutement et la fidélisation des cybercombattants est un redoutable défi à relever pour toutes les grandes organisations. Conjoncturelle ou structurelle, la pénurie des talents est une réalité qui crée de fait une tension concurrentielle très forte, sur un marché du travail très demandeur. Face à ce problème, le service public en général et la cyberdéfense militaire en particulier doivent d'ores et déjà faire preuve d'inventivité afin de capter l'attention des jeunes diplômés, en vue de susciter et de nourrir en eux un intérêt qui pourra se concrétiser par une collaboration plus ou moins longue. Il faut être clair, le secteur privé a l'avantage d'offrir les perspectives de rémunération les plus intéressantes. Le secteur public, lui, a l'avantage d'offrir un cadre de travail porté par la recherche d'efficacité et non contrainte par le chiffre d'affaires, donc favorable à l'excellence technique. Il offre de plus l'occasion de servir le pays de façon concrète et d'acquérir une expérience très solide et reconnue.

La formation des cybercombattants est également un défi de taille. Le modèle de formation actuel doit être renouvelé. Ce constat s'est d'ailleurs imposé dans toute la communauté du numérique des armées. Il s'agit de concevoir un nouveau modèle, mieux adapté aux réalités d'aujourd'hui et

à ce que l'on peut entrevoir de celles de demain. Il faut garantir au ministère la mise à disposition d'une ressource humaine cyber entretenue en permanence au plus haut niveau technique. Cet objectif nécessitera de faire converger les efforts de tous les acteurs du ministère. Une coordination interne renforcée sera indispensable. La création d'un centre d'expertise des formations et des parcours professionnels cyber du ministère des Armées, en somme une « académie cyber », pourrait constituer l'élément structurant de la réponse globale à cette problématique. Le ministère des Armées possède de vrais atouts à faire valoir en termes de formation.

Enfin, la cyberdéfense est confrontée à un défi technique dont l'ampleur ne se rencontre que dans le domaine du numérique. Aucun autre domaine ne connaît des cycles de renouvellement technique aussi rapides. Il s'agit, en permanence, de connaître toutes les évolutions réalisées (et si possible celles qui le seront à brève échéance), de maîtriser ces techniques et de former tout le personnel nécessaire pour les maîtriser sur une large échelle.

Plusieurs enjeux se dessinent à court terme, comme l'acquisition d'une capacité d'hypervision. À moyen terme, l'intelligence artificielle devra être mise au service de la détection et de la réaction aux agressions sans cesse plus perfectionnées que nous pourrions rencontrer. À plus long terme, l'informatique quantique devrait créer une rupture très importante avec, notamment, le basculement massif, complet et définitif de tout le chiffrement classique dans le domaine du vulnérable.

Conclusion

La cyberdéfense demeure une priorité très forte du ministère des Armées avec l'ambition de donner à la France les moyens de construire un outil à la hauteur de ses ambitions opérationnelles et d'assurer pleinement sa cybersécurité.

L'inauguration par la ministre des Armées le 3 octobre dernier à Rennes du premier bâtiment entièrement dédié à la conduite des opérations cyber, au sein du pôle d'excellence cyber bâti avec la région Bretagne et à proximité immédiate d'une Cyberdéfense Factory destinée à faire éclore des entreprises du domaine par l'aide de l'État, témoigne de cette dynamique qui permet à la France de rayonner et lui confère un statut de cyberpuissance.

Nouveaux rôle et enjeux pour l'État dans la lutte contre la cybercriminalité

Par **Thierry DELVILLE**
PricewaterhouseCoopers (PwC)

La cybersécurité est devenue une préoccupation centrale des dirigeants, qu'il s'agisse des responsables publics ou des dirigeants d'entreprises. Sur les trois dernières années, les chiffres observés à travers des sondages réguliers classent entre la troisième et la cinquième position la cybersécurité au rang des sources d'inquiétude majeures à côté du terrorisme, de l'incertitude géopolitique, de l'augmentation des régulations ou encore des changements climatiques [(1)].

Voilà bientôt quarante-cinq ans qu'un premier virus informatique [(2)] a été identifié sur ce qui n'était pas encore le réseau Internet. Aujourd'hui, l'hyperconnexion, la transformation digitale de l'économie et de la société en général, font du cyberespace le cinquième champ de conflictualité sur lequel sont engagées désormais la plupart des grandes armées.

Les activités criminelles bénéficient également, dans cette nouvelle dimension, d'un contexte très favorable en raison d'une sociologie propre à la cybercriminalité : absence de frontière, population criminelle qui évolue et se diversifie, passant de la recherche du profit facile à des activités mieux préparées et ciblées en y consacrant des moyens plus élaborés. L'espionnage et l'ingérence au profit d'organisations privées voire d'États complices ou donneurs d'ordres perdurent et cristallisent une véritable « cyber guerre froide ». Tout cela est de nature à motiver le passage à l'acte dont le retour sur investissement est bien plus rémunérateur que dans le champ de la délinquance « non cyber ».

Pour lutter contre la cybercriminalité, pour investiguer, pour juger les auteurs interpellés, l'État demeure un acteur central, dans son rôle de protecteur des droits fondamentaux et des libertés individuelles, mais il apparaît de plus en plus évident que mener à bien cette mission appelle d'autres modalités de travail et d'interventions.

Mieux connaître la menace et sa progression

Dans un rapport de 2014 [(3)], une mission interministérielle dirigée par le procureur général Marc Robert avait considéré que la cybercriminalité apparaissait comme une « nébuleuse d'autant plus difficile à cerner qu'elle renvoie à des procédés techniques essentiellement évolutifs maîtrisés par les seuls initiés et que peinent à cerner les dispositifs statistiques traditionnels ». S'inspirant des multiples définitions d'origines nationales et internationales, dont aucune ne répondait à la dimension pédagogique de compréhension partagée du phénomène, il avait suggéré cette définition générique : « La cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet. »

Connaître la réalité du phénomène constitue en effet un besoin préalable pour évaluer la réalité d'une menace et son évolution. « Si tu ne connais ni ton adversaire ni toi-même, à chaque bataille tu seras vaincu », écrit Sun Tzu dans *L'Art de la guerre*. Connaître la réalité de la cybercriminalité malgré l'absence de définition juridique précise représente à ce titre un défi essentiel. Dans son

(1) https://www.pwc.com/gx/en/ceo-survey/2019/report/pwc-22nd-annual-global-ceo-survey.pdf
(2) Lancé en 1971 sur le réseau Arpanet sous le nom de *Creeper*.
(3) https://www.ladocumentationfrancaise.fr/rapports-publics/144000372/

rapport de 2019, le ministère de l'Intérieur rappelle une nouvelle fois la difficulté d'établir une vision consolidée reposant sur les statistiques dans son rapport sur « l'état de la menace liée au numérique en 2019 [4] ».

La construction d'une vision partagée est à encourager. La connaissance de cette « topographie cybercriminelle » à l'échelle nationale nécessite l'agrégation de données multiples que seule une vision élargie, au-delà de celle des services institutionnels, permettra d'obtenir. S'il est d'usage de qualifier de « chiffre noir » de la délinquance les faits de crimes ou délits non signalés aux autorités, nombre d'experts qualifient de « trou noir » la part de ces mêmes faits commis dans l'espace cyber.

Un cadre réglementaire impose à certaines catégories de victimes d'informer l'ANSSI (Agence nationale de la Sécurité des Systèmes d'Information) dont le rôle de régulateur interministériel s'est renforcé ces dernières années. Ainsi, après la Loi de programmation militaire 2013-2019 et la directive NIS, les OIV et OSE [5] constituent autant d'entreprises stratégiques sur lesquelles reposent des obligations d'équipement et d'information des autorités en cas d'incidents. Les autres entreprises, moins sensibles, ne sont pas soumises à ces obligations.

Ces règles ne créent pas *de facto* d'obligation de déposer plainte ni d'ouvrir une enquête pénale. La poursuite des infractions repose également sur la bonne synergie entre les services de l'État (à vocation technique et à vocation judiciaire) et sur la volonté des victimes qui craignent encore trop souvent pour leur réputation voire d'éventuelles sanctions [6].

Encourager le dépôt de plainte à travers de nouveaux outils [7] et une forte sensibilisation de l'ensemble des acteurs, systématiser les échanges croisés au sein des services de l'État, bâtir les conditions d'un recueil plus large notamment avec le secteur privé permettront d'établir une mesure de suivi pérenne et exhaustive de la cybercriminalité.

Mieux connaître pour mieux prévenir

Si la connaissance des faits et le partage d'informations constituent un point-clé dans la mise en place d'un dispositif de lutte efficace, pour l'État, agir efficacement, c'est avant tout mieux prévenir, sensibiliser, informer.

L'identification des menaces et des réponses techniques est partagée sous l'impulsion de l'ANSSI par le réseau des CERT [8] qui constitue un appui technique essentiel pour les professionnels experts, mais le dispositif n'est pas diffusé au-delà de cette communauté. Combien, sur les trois millions d'entreprises en France, s'appuient sur cette base de connaissance ?

D'autres initiatives majeures ont vu le jour ces dernières années telles que la plateforme cybermalveillance.gouv.fr qui recense les incidents dont ont été victimes les entreprises ou les particuliers avant de mettre ces derniers en contact avec des techniciens référencés sur le site. Ce groupement d'intérêt public (GIP) diffuse aussi *via* les réseaux sociaux de nombreuses informations et messages d'alertes. Également d'autres actions sont à signaler : e-enfance (sur le cyberharcèlement), stop-jihadisme (pour la propagande en ligne), Perceval (pour signaler les escroqueries à la carte bancaire) sans oublier la plateforme Pharos qui recense les signalements de contenus illicites depuis bientôt dix ans.

(4) https://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019
(5) Opérateur d'importance vitale et Opérateur de service essentiel.
(6) Le fait de ne pas s'être signalé comme victime d'un vol de données peut valoir très cher au sens de la réglementation RGPD avec des sanctions possibles jusqu'à 2 % du chiffre d'affaires (article 83.4 RGPD).
(7) https://www.interieur.gouv.fr/Archives/Archives-ministres-de-l-Interieur/Archives-Gerard-Collomb-mai-2017-octobre-2018/Communiques-du-ministre/Ouverture-de-la-plateforme-Percev-l-Signalement-des-fraudes-a-la-carte-bancaire
(8) https://www.cert.ssi.gouv.fr/

Les moyens de la prévention s'organisent mais il est essentiel de voir plus loin et d'organiser l'effort collectif de diffusion de la connaissance :

- développer le retour d'expérience des entreprises touchées en le faisant au plan sectoriel pour aller plus loin dans l'actualisation de l'évolution des menaces ;
- encourager le retour d'expérience avec les prestataires certifiés sous l'autorité de l'ANSSI et des autres services de l'État pour informer sur l'apparition de nouvelles menaces et de nouveaux *modus operandi* ;
- développer de nouvelles pratiques et méthodes pour se préparer aux attaques de plus en plus massives et systémiques.

Beaucoup a déjà été fait et il en reste bien davantage à faire !

Quels moyens pour mieux lutter contre la cybercriminalité ?

Faut-il considérer avec Myriam Quemener [(9)] que « le droit s'épuise à poursuivre la preuve numérique dont les frontières s'échappent toujours plus loin » ? Incontestablement le législateur ne cesse de courir après les nouveaux risques numériques. Sur ces trois dernières années, sont ainsi intervenus des textes réprimant (liste non exhaustive) le cyberharcèlement, le *revenge porn,* la provocation au suicide. Tout récemment la loi PACTE [(10)] introduit des règles visant à lutter contre les nouvelles fraudes apparues avec les levées de fonds à partir de monnaies virtuelles (ICO). Cette adaptation permanente aux nouvelles pratiques numériques et la nécessité de créer de nouvelles incriminations ne devrait pas cesser dans les années à venir.

Les moyens et techniques d'enquête se développent également : l'offre *digital forensic* s'est transformée et des avancées importantes ont pu être réalisées en matière d'interception, de géolocalisation et d'exploitation des données de masse que ne manquent pas de récupérer les enquêteurs lors des perquisitions faites sur les lieux d'affaires retentissantes (par exemple dans le cadre des attentats de 2015). Cette évolution profite, pour partie, également aux prestataires privés qui interviennent en cas de crise ou remédiation de crise.

Parmi les attentes en termes d'évolution du droit, il faut souligner les nouveaux enjeux que constituent la conservation des données (après l'arrêt Télé2 de décembre 2016 de la CJUE), les moyens pour les enquêteurs de contourner les techniques d'anonymisation ou encore l'accélération de l'accès transfrontalier aux données. L'essentiel de ces points se situe dans une dimension que le droit national seul ne peut résoudre.

L'essentiel des enjeux de lutte contre la cybercriminalité est adressé à l'échelle internationale. La capacité grandissante d'Europol avec la création en 2013 de l'European Cybercrime Centre (EC3 [(11)]), illustré par exemple par son action dans la gestion des contenus illicites sur Internet avec la création de la plateforme européenne IRU, les nombreux textes de la commission (la directive NIS, RGPD), le Cyberact [(12)], le renforcement du rôle de l'ENISA dans la certification des solutions de confiance à l'échelle européenne, toutes ces avancées traduisent bien l'idée que l'avenir de la lutte contre la cybercriminalité passe par l'Europe et, au-delà, par le développement d'initiatives d'envergure internationale.

La politique pénale doit également gagner en visibilité, par le nombre de magistrats formés et spécialisés en premier lieu, mais aussi se traduire par des sanctions qui reflètent la gravité du

(9) *Le Droit face à la disruption numérique*, Éditions Gualino, avril 2018.
(10) https://www.amf-france.org/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France
(11) https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
(12) https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_fr

phénomène et sortent la cybercriminalité d'une perception quelque peu anecdotique. Sans répliquer les sanctions très fortes voire définitives infligées aux États-Unis [13], il importe que l'exemplarité de la sanction infligée par la justice pour les actes de cybercriminalité les plus graves soit posée.

Les acteurs de plus en plus nombreux de la lutte contre le cybercrime

La France a pris assez tôt conscience de l'importance du sujet que ce soit pour légiférer ou pour organiser la première forme de sa riposte. Dès 1994, la Préfecture de Police créait un service d'enquête en charge des fraudes aux technologies de l'information (la BEFTI), peu après, la police et la gendarmerie créaient les structures qui aujourd'hui encore (OCLCTIC, C3N) représentent des pôles d'expertise reconnus à l'échelle internationale, capables d'investiguer sous le contrôle de quelques magistrats spécialisés. D'autres services d'enquête des douanes ou encore Tracfin se sont au fil des années dotés d'équipes dédiées.

Du côté de la justice, la désignation de magistrats référents, la création d'une section spécialisée chargée des faits de cybercriminalité à Paris (Section F1 du parquet de Paris) et la mise en place des JIRS en province sont autant de réponses à cette évolution. La création d'un parquet spécialisé de type PNF ou PNAT représenterait un palier supplémentaire pour une réponse judiciaire mieux adaptée.

D'autres acteurs étatiques interviennent dans le champ de la cybercriminalité. L'ANSSI décrit sur son site Internet la cybercriminalité en ces termes : « La cybercriminalité est un vaste sujet qui concerne en premier lieu les ministères de l'Intérieur et de la Justice, en étroite collaboration avec l'ANSSI. » Le rôle central de cette agence est un fait incontesté et son expertise technique en fait aussi un atout essentiel pour tout ce qui relève de la détection des menaces et de l'analyse des incidents. Les services de renseignement jouent également un rôle essentiel dans cette lutte. La DGSI dispose du pouvoir d'enquête judiciaire pour les attaques mettant en jeu des entreprises ou des cibles relevant de la défense des intérêts vitaux ou stratégiques de la nation.

La « Revue stratégique de cyberdéfense [14] » de 2018 recommande que soit permise la mise en place d'un échange croisé de données techniques entre les experts techniques de la cyberdéfense (l'ANSSI, mais aussi le COMCYBER du ministère de la Défense, et la DGSE) et les enquêteurs en cybercriminalité.

La dimension hybride des attaques cyber où le monde criminel peut côtoyer le renseignement et celui de la défense, donne une perspective particulière au traitement diplomatique de certains faits. Les événements marquants qu'ont été des attaques comme *WannaCry* ou *NotPetya*, d'autres affaires outre-Atlantique ou plus près de nous aux Pays-Bas [15], ont montré une évolution dans les postures diplomatiques et judiciaires avec la désignation d'individus ou d'États criminels supposés [16] (notamment la pratique du *name and shame)* mais également de compagnies insuffisamment protégées et potentielles victimes.

Autres acteurs, et non des moindres, dans cette lutte, les prestataires privés sont particulièrement impliqués dans les phases de prévention mais également celles de remédiation. Ils sont au cœur des crises traversées par la plupart des victimes de cyberattaques et leur identification comme des

(13) https://en.wikipedia.org/wiki/Ross_Ulbricht
(14) http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/
(15) https://www.huffingtonpost.fr/2018/10/04/derriere-laffaire-de-la-cyberattaque-aux-pays-bas-le-puissant-grule-service-de-renseignement-militaire-russe_a_23551536/
(16) https://www.theguardian.com/politics/2018/may/23/uk-threatens-to-name-and-shame-state-backers-of-cyber-attacks

acteurs de confiance repose de plus en plus fréquemment sur des labels ou des certifications. L'État se doit d'avoir vis-à-vis de cette expertise une action en profondeur allant de l'information la plus précise possible (dans les deux sens) pour déjouer les menaces en cours, à l'exercice de son pouvoir de contrôle en cas de dérives ou d'insuffisances avérées. L'animation de cet écosystème d'experts est inévitable, c'est un enjeu de filière mais aussi de souveraineté.

Se préparer aux nouveaux défis du cyber dans une dimension élargie

L'histoire de la cybercriminalité s'écrira encore longtemps et de nombreux textes nationaux interviendront pour répondre aux limites du travail des enquêteurs, accentuer le rôle de vigilance et la responsabilité des opérateurs, incriminer de nouvelles pratiques…

La lutte contre le crime dans les environnements digitaux futurs reposera sur des moyens consacrés à la recherche, à la prospective et à l'innovation. Peu avant le dernier sommet du G7 à Biarritz, la nouvelle responsable d'EUROPOL, Catherine de Bolle, soulignait que l'arrivée de la communication 5G et les nouveaux enjeux liés aux IoT ou à l'IA constituaient autant d'avancées qui remettent en cause les capacités des services d'enquête, qu'il s'agisse d'interception ou de techniques d'investigation.

Au-delà des nouveaux outils et des nouveaux enjeux, c'est bien dans le champ des nouvelles régulations internationales qu'il conviendra d'être présent. Le traité de Budapest, acte fondateur de l'entraide internationale dans cette lutte, date de 2001 et n'est toujours ratifié que par une cinquantaine d'États. L'appel de Paris du président de la République, en novembre 2018, pour la confiance et la sécurité dans le cyberespace ne rencontre pas d'écho de la Chine, des États-Unis ou de la Russie… L'enjeu demeure, comme cela a été rappelé au sommet du G7 de Biarritz en août 2019, de travailler mieux ensemble… Mais de l'intention aux actes, il y a encore du chemin.

Le rôle de l'État sera central dans les années à venir pour lutter contre la cybercriminalité mais il ne se jouera plus, comme par le passé, avec une séparation nette entre le régalien d'un côté et l'expertise de l'autre. La lutte contre le crime dans le numérique se jouera dans un réseau où le partage de l'information deviendra une vertu cardinale. Sensibiliser, prévenir, partager : telles sont et seront plus encore demain les clés à réunir pour lutter à armes, si ce n'est égales à tout le moins comparables, avec des criminels pour qui ces valeurs sont déjà bien intégrées.

À la poursuite des cybercriminels

Par **Jacques MARTINON**
Mission de Lutte contre la Cybercriminalité (MLC)

Introduction

Le cybercriminel est dans la majorité des cas un délinquant ayant le souhait d'optimiser sa rentabilité économique et qui s'adapte en conséquence aux nombreuses opportunités du monde numérique. L'aspect communautaire est également important, des spécialistes émergeant afin d'offrir une galaxie de services (*Cybercrime as a Service*) dans le cadre d'un écosystème désormais bien établi. Toutefois, certains acteurs de la cybercriminalité ont des motivations différentes, soutenus voire armés par des ressources étatiques plus ou moins clandestines, dans le cadre de guerres économiques larvées (cyberespionnage) ou de démonstrations de puissance (cybersabotage), multipliant les pré-positionnements à l'intérieur de systèmes critiques. Comme le relève la « Revue stratégique de Cyberdéfense » (février 2018 [(1)]), la menace est hybride et le cloisonnement entre cyberdéfense et cybercriminalité s'estompe.

Les acteurs judiciaires de lutte contre la cybercriminalité doivent donc adapter rapidement leurs stratégies, méthodes et organisations afin d'améliorer leur efficacité. La France n'a initié véritablement ce mouvement qu'en 2015, dans les suites du rapport de référence sur la cybercriminalité « Protéger les internautes », élaboré sous l'égide du procureur général Marc Robert [(2)]. Des progrès indéniables ont été réalisés, mais la poursuite de ces efforts est essentielle afin de consacrer un véritable levier judiciaire redouté par les cybercriminels et activable dans le champ de la cyberdéfense.

Si toutes les juridictions peuvent connaître des faits de cyberdélinquance [(3)], il convient de relever que le tribunal de grande instance de Paris bénéficie d'une compétence concurrente nationale en matière de cyberattaques [(4)]. Les contours d'une politique pénale de lutte contre la cyberdélinquance sont en voie de consolidation en priorisant les tendances les plus préoccupantes touchant la population française ainsi que son tissu économique.

Seront présentées dans un premier temps les caractéristiques principales de la cybercriminalité (1), avant d'aborder les adaptations stratégiques et organisationnelles des acteurs judiciaires, ainsi que les nouvelles relations de ces acteurs avec ceux de la cybersécurité (2).

Une cybercriminalité polymorphe et occulte

La typologie de la cybercriminalité demeure un défi intellectuel puisque l'angle traditionnel des qualifications pénales est imparfait. Les « cyberattaques » recouvrent en réalité de

(1) http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf
(2) Rapport « Protéger les internautes » du groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014, consultable à l'adresse suivante http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf
(3) Nous utiliserons indifféremment les expressions « cybercriminalité » et « cyberdélinquance », étant entendu que le terme « cybercriminalité » est le plus usité du fait de son pendant anglo-saxon « cybercrime », alors même que la quasi-intégralité des infractions « cyber » sont bien des délits, et non des crimes au sens du droit pénal français.
(4) Article 706-72-1 du Code de procédure pénale (créé par la loi n°2016-731 du 3 juin 2016) : « Pour la poursuite, l'instruction et le jugement des infractions entrant dans le champ d'application de l'article 706-72, le procureur de la République, le pôle de l'instruction, le tribunal correctionnel et la cour d'assises de Paris exercent une compétence concurrente à celle qui résulte de l'application des articles 43, 52 et 382. »

nombreux « phénomènes cyber » distincts dans leur mode opératoire et leur motivation, tels le cyberespionnage, le cybersabotage, le rançongiciel…

Aujourd'hui, la cybercriminalité reste largement occulte, notamment car les outils statistiques traditionnels sont *de facto* inopérants pour apprécier finement les évolutions des phénomènes. À cela s'ajoutent les problématiques classiques du chiffre noir et d'une preuve numérique parfois chimérique.

Une cybercriminalité polymorphe et évolutive

La cybercriminalité a pour caractéristiques principales d'être polymorphe et naturellement très évolutive, bénéficiant du dynamisme de l'écosystème numérique.

Une classification délicate

La cyberdélinquance au sens strict couvre les phénomènes pénaux dont l'objet est l'atteinte à un Système de Traitement automatisé de Données (STAD) réprimée par les articles 323-1 à 323-4 du Code pénal. Dans la pratique, cette catégorie est divisée entre les phénomènes de haute intensité (atteinte aux intérêts fondamentaux de la Nation, dimension internationale, haute technicité, nombre important de victimes avérées ou supposées) et de basse intensité.

La seconde catégorie regroupe les phénomènes qui ont pour vecteur principal un STAD ou ont été facilités par son utilisation, il s'agit de la cyberdélinquance au sens large, incluant de nombreuses escroqueries. Ces infractions mixtes couvrent également la lutte contre les activités illicites sur l'Internet sombre (*darknets* [5]).

Les nouveaux métiers de la cybercriminalité

La cybercriminalité prospère et de nouveaux « métiers » fleurissent régulièrement, faisant naître le concept de « *Cybercrime as a Service* » (analogie avec les services informatiques traditionnels), telles les locations/ventes d'infrastructures de type *botnets* (réseau d'ordinateurs ou d'objets connectés [6] « zombies », sous le contrôle d'un serveur dit *Command & Control*), de maliciels divers (comme certains rançongiciels qui connaissent un regain dévastateur auprès des entreprises et des collectivités territoriales), des services de *Crypter/Packer* (augmentant la furtivité des maliciels), de *Money mules* (personne qui transfère de l'argent acquis illégalement pour le compte de tiers) ou encore de *Mixer/Blender* [7] (facilitant le blanchiment des cryptomonnaies).

Les cryptomonnaies sont sources de nombreuses opportunités, qu'elles soient dérobées aux plateformes d'échanges ou aux particuliers, ou bien que la puissance de calcul de terminaux soit détournée afin de « miner » des cryptomonnaies au bénéfice de l'attaquant (*Cryptojacking*).

Plus original, il existe des campagnes de recrutement *via* des annonces d'emploi pour des administrateurs de *Darknets,* comme ci-dessous pour Liberty Market (figure 1) :

> « **Nous cherchons à recruter un membre**, homme ou femme, qui possède une bonne orthographe. Vous devrez être familier avec la gestion ergonomique des pages web. Il faudra que vous puissiez vous connecter au moins une heure et demie, quatre fois par semaine. Vous serez en charge de la correction des posts du forum et responsable de leur bonne lisibilité. Vous devrez aussi corriger des douzaines de posts à chaque connexion. Vous aurez votre propre tableau de bord afin que vous puissiez travailler en toute autonomie. »

Figure 1. Source : www.ladn.eu

(5) Le plus célèbre étant le protocole TOR (*The Onion Router*).
(6) Un cas célèbre étant le Botnet issu du maliciel Mirai en 2016, ayant servi à des attaques DDos (*Distributed Denial of Service*) touchant notamment OVH et Dyn, cette dernière affectant une partie critique d'Internet au niveau de la gestion des services DNS (*Domaine Name System*). En août 2019, le C3N (Gendarmerie nationale) a démantelé avec succès le Botnet Retadup, composé de plus de 500 000 machines infectées.
(7) Le site Bestmixer.io a toutefois été mis sur la touche par une action conjointe d'EUROPOL et des enquêteurs financiers néerlandais, avec un chiffre d'affaires estimé à 200 millions d'euros.

Dans la même veine, on relèvera un service de type « Tag Telegram », où des personnes sont simplement rémunérées pour réaliser des tags dans des zones urbaines prédéterminées, de façon à fournir des indications techniques pour rejoindre une discussion Telegram d'un dealer. Ce nouveau *job* permet de matérialiser « l'ubérisation » rampante des trafics de stupéfiants, où le consommateur commande directement sa drogue *via* son *smartphone* et une application de messagerie cryptée, et se fait livrer à domicile H24 7j/7.

Figure 2 : cas ukrainien (15$/jour – SMIC mensuel local 140$). Source : Trustwave

Une des conséquences probables pourrait être l'éclatement des logiques des territoires de points de *deals*, avec un déplacement sur la visibilité, furtivité et popularité de leur vecteur numérique de communication. D'autres tendances inquiétantes semblent se dessiner avec des applications d'échange décentralisées, anonymes et basées sur les cryptomonnaies (par exemple : Openbazaar, Haven).

Une cybercriminalité occulte

La lutte contre la cybercriminalité est handicapée par plusieurs facteurs, notamment un nombre important d'infractions qui ne sont pas portées à la connaissance de la justice et une preuve numérique aléatoire.

Le chiffre noir de la cybercriminalité

Certains phénomènes cybercriminels de haute intensité, comme le cyber-espionnage ou le cyber-sabotage, sont peu judiciarisés, du fait de leur nature sensible [(8)]. La publicité d'une cyber-attaque à l'encontre d'une entreprise peut nuire à son image. Le règlement européen pour la protection des données personnelles (RGPD) est un espoir, dès lors que les violations de données personnelles conduisent à une obligation de notification dans les 72 heures à la CNIL [(9)].

Concernant les particuliers, les raisons du chiffre noir sont diverses, du fait d'un caractère parfois imperceptible de l'infraction ou d'un sentiment erroné de l'inutilité de la plainte, souvent couplé à de faibles préjudices matériels.

Une meilleure sensibilisation semble nécessaire, d'où l'importance du dispositif national d'assistance aux victimes d'actes de cybermalveillance [(10)], et des mesures facilitant le dépôt de plainte. La future plateforme THESEE (projet porté par le ministère de l'Intérieur) est susceptible d'améliorer la connaissance statistique pour certains phénomènes de cybercriminalité. La récente

(8) La doctrine américaine est différente à cet égard, au vu de l'activisme récent du *Department of Justice (DoJ)* à l'encontre de ressortissants chinois ou russes.
(9) Voir le cas d'Airbus en janvier 2019.
(10) https://www.cybermalveillance.gouv.fr/

Loi de Programmation pour la Justice (LPJ) insère d'ailleurs de nouvelles dispositions afin d'encadrer la plainte en ligne [11].

Preuve numérique, "going dark [12]" et extraterritorialité

La libéralisation du chiffrement a amélioré sensiblement le niveau de cybersécurité, mais a provoqué de manière collatérale des difficultés propres aux investigations judicaires. La banalisation des applications de messageries instantanées chiffrées avec des protocoles particulièrement robustes, comme ceux dits *End to end,* est un défi actuel. De même, la généralisation du chiffrement de type *full disk* sur les terminaux informatiques, dont les *smartphones*, a rendu délicate l'exploitation forensique. Enfin, comme déjà évoqué, les architectures réseaux de type TOR (*The Onion Router*) participent à l'obfuscation des comportements criminels sur les *Darknets*. Demain, la fusion annoncée entre les applications de messageries et les cryptoactifs ne manque pas d'inquiéter les professionnels [13]. L'annonce du LIBRA par la société Facebook, avec son caractère systémique au vu du nombre de ses utilisateurs potentiels, a suscité une forte réaction politique qui devra se concrétiser en régulation efficiente en termes de mécanismes AML (mesures anti-blanchiment) et KYC (connaissance de clientèle).

Complétant un tableau déjà bien sombre, s'ajoute la difficulté d'une preuve numérique désormais largement stockée en dehors de nos frontières, du fait de l'essor de l'informatique à distance (*Cloud*), mais une éclaircie semble percer les nuages.

En effet, une révolution est en cours avec le futur règlement européen "E-Evidence", doublé d'une directive dite « représentant », cette dernière posant le prérequis juridique de l'applicabilité du droit européen aux entreprises mondiales dirigeant leur activité économique sur le territoire européen [14]. Le sujet est au centre de tensions diplomatiques avec les États-Unis, un indispensable dialogue devant être mené par la Commission européenne avec ces derniers afin de résoudre certains conflits de lois. Des négociations entourant un second protocole additionnel à la Convention de Budapest contre la cybercriminalité (Conseil de l'Europe) sont par ailleurs bien avancées.

Dans l'intervalle, et anticipant ces révolutions dans l'accès transfrontalier à la preuve, la politique interne de certains GAFAM (Google par exemple) s'est modifiée récemment en transférant la gestion de certaines réquisitions judiciaires françaises de leur maison mère basée aux États-Unis à leur filiale de droit irlandais [15].

Une adaptation stratégique et organisationnelle des acteurs judiciaires

Une enquête cyber possède plusieurs spécificités, souvent liées à la preuve numérique. La dissémination des victimes cyber sur le territoire conduit à une certaine rationalisation du traitement judiciaire, tandis que la culture du silo administratif doit laisser la place à des échanges inter-institutionnels du fait de la nature transversale des enjeux numériques.

(11) Nouvel article 15-3-1 du Code de procédure pénale.
(12) Cette expression d'origine militaire fait référence à la perte soudaine des communications de l'adversaire pouvant être analysées au profit de moyens de communications indétectables.
(13) Voir le lancement du réseau TON et la cryptomonnaie GRAM par l'entreprise TELEGRAM, annoncé pour le dernier trimestre 2019, suite à une levée de fonds de 1,7 milliard de dollars.
(14) Le Règlement général de Protection des Données (RGPD) européen avait posé une première pierre à l'édifice, quoique sur des critères de rattachement distincts.
(15) Force est de constater que la quasi-totalité des sociétés californiennes du numérique sont installées en Irlande, potentiellement pour des questions d'optimisation fiscale.

Aperçu de stratégies judiciaires

Seuls quelques exemples seront évoqués dans le présent article, par manque d'espace mais aussi par volonté de ne pas trop en dévoiler (le lecteur nous pardonnera mais les cybercriminels sont à l'affût de toute information en la matière [16]). Comme le disait le Doyen Carbonnier, à propos du procès civil : « Si les coups bas sont interdits, les simples ruses de guerre ne le sont pas. »

La récupération de la preuve numérique nécessitera souvent d'identifier et de localiser les serveurs "Back End", où se situe l'essentiel des éléments pouvant être dissimulés derrière une multitude de serveurs "Proxy", afin de lancer *in fine* des opérations de perquisition chez le prestataire. Il n'est pas rare que les serveurs en question soient à l'étranger, et une fine coopération judiciaire internationale sera primordiale.

Concernant les techniques spéciales d'enquête, le régime de l'enquête sous pseudonyme est particulièrement adapté. La traçabilité de certains cryptoactifs comme le Bitcoin peut également être facilitée par des logiciels commerciaux.

Lors de l'interpellation des suspects, priorité sera donnée au "Live Forensics", c'est-à-dire aux investigations numériques d'urgence sur les supports informatiques découverts, afin de minimiser des difficultés techniques ultérieures comme le chiffrement des données.

Enfin, la recevabilité des preuves obtenues par des services d'enquête étrangers n'est pas un sujet simple, et la jurisprudence nous paraît relativement instable. Ainsi la Cour de cassation a considéré que la création d'un faux site pédophile par les autorités américaines constituait une provocation à l'infraction, et donc annulera la procédure française (Cass. Crim., 7 février 2007, n°06-87.753). Toutefois, en 2014, elle validera un recueil de preuve *via* un forum créé par le FBI sur la fraude à la carte bancaire (Cass. Crim., 30 avril 2014, n°13-88.162). Assurément les débats juridiques se poursuivront avec la multiplication des techniques de pot de miel (*Honey Pot*) par certaines autorités étrangères.

Adaptations organisationnelles et relations des acteurs judiciaires avec ceux de la cybersécurité

Constats sur l'organisation judiciaire en 2019

Sans pouvoir détailler ici les multiples compétences territoriales de l'autorité judiciaire en matière de cybercriminalité, il sera rappelé le rôle primordial du tribunal de grande instance de Paris bénéficiant depuis la loi du 3 juin 2016 d'une compétence concurrente nationale en matière d'atteintes aux STAD et de crimes de sabotage informatique [17].

Cette réforme a permis de consolider la création en 2015 d'une section dite « F1 » du parquet de Paris dédiée au traitement de certaines affaires de cybercriminalité, notamment les plus complexes. Les effectifs de cette section sont en progression [18]. Le constat est plus inquiétant au siège, avec l'absence notamment de juge d'instruction véritablement spécialisé. Des dépêches de centralisation du traitement de certains phénomènes de cybercriminalité sont à relever, produites par la Mission de Lutte contre la Cybercriminalité de la Direction des Affaires criminelles et des Grâces (DACG) du ministère de la Justice [19].

(16) Preuve en sont les échanges en procédure pénale détectés sur certains forums de *Darknets*.
(17) Nouvel article 706-72-1 du Code de procédure pénale.
(18) Trois magistrats, ainsi qu'un assistant spécialisé et un greffier (septembre 2019).
(19) Exemple : dépêches DACG des 10 mai 2017 et 22 juin 2018 concernant d'une part la mise en œuvre opérationnelle de la compétence nationale concurrente du parquet de Paris en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) et le traitement judiciaire des « rançongiciels », et d'autre part la centralisation du traitement des « fraudes aux réparations informatiques ».

Au-delà, les juridictions interrégionales spécialisées (JIRS) connaissent de plus en plus de contentieux de la cybercriminalité, notamment liée à la criminalité organisée [20]. Enfin, un réseau de magistrats « cyber-référents » dans les tribunaux, cours d'appel et JIRS est en voie de généralisation, dans les suites de la première réunion nationale des magistrats cyber-référents, co-organisée le 14 juin dernier par le parquet de Paris et la DACG.

Densification des liens entre les acteurs judiciaires et ceux de la cybersécurité

L'administration centrale (DACG), *via* la mission précitée, contribue aux travaux stratégiques du centre de coordination des crises cyber (C4), instauré suite à la « Revue stratégique de Cyberdéfense » précitée, ainsi qu'aux réunions du Groupe de Contact permanent (GCP). Ce GCP, piloté par la délégation ministérielle en charge des industries de sécurité et à la lutte contre les cybermenaces (DMISC), a pour objectif d'améliorer le dialogue avec les acteurs privés comme Apple, Google, Twitter, Microsoft, Facebook, et récemment Dropbox, dans un esprit constructif partagé.

Enfin, la DACG fait partie du conseil d'administration du GIP ACYMA (cybermalveillance.gouv.fr) et participe à la formation commune « Souveraineté numérique et cybersécurité » de l'IHEDN (Institut des hautes Études de la Défense nationale) et de l'INHESJ (Institut national des hautes Études de Sécurité et de Justice) dont le public est constitué de hauts cadres publics et privés, ainsi que de membres de la société civile.

Conclusion

Le levier judiciaire doit encore gagner en maturité mais des progrès sont indéniablement en cours. La coopération internationale est un facteur-clé de ce succès, avec l'aide conjointe d'EUROPOL, d'EUROJUST et d'INTERPOL. Les menaces issues du monde numérique ne doivent pas rester sans réponse, d'autant que la surface d'attaque ne cesse de s'étendre, avec des conséquences potentiellement systémiques pour l'économie et des mises en danger de l'intégrité physique de nos citoyens. Le constat peut sembler alarmiste mais quelle réaction adopter demain en cas de rançongiciel paralysant un hôpital ou entraînant un dysfonctionnement d'une voiture connectée à pleine vitesse sur autoroute ? Jusqu'ici, tout va (presque) bien.

Figure 3 : Gunshow, KC GREEN

(20) Exemple : le démantèlement de la Main noire, une plateforme du *Darknet*, sous la supervision de la JIRS de Lille.

Innovation et startups cybersécurité en France : le début de l'embellie ?

Par **Gérôme BILLOIS**
et **Jules HADDAD**
Wavestone

Nul n'est sans savoir que la menace cybersécurité évolue rapidement. Les cybercriminels font preuve d'une imagination sans limite et améliorent sans cesse leurs méthodes d'attaque pour contourner les barrières de protection mises en place. Il est donc nécessaire que ces technologies de protection s'adaptent afin de se mettre à niveau, exacerbant l'importance de l'innovation dans la cybersécurité. Ceci est particulièrement vrai dans le secteur de la finance, cible récurrente d'attaques cybercriminelles avec des niveaux de sophistication élevés. Les systèmes anti-fraude, les systèmes transactionnels, les applications mobiles sont régulièrement la cible d'attaques réussies et lucratives pour les cybercriminels.

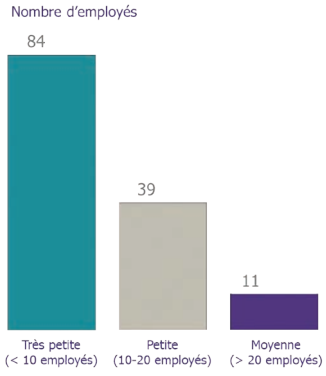
De plus, avec la tension que connaît actuellement le marché des compétences en cybersécurité, les actions manuelles doivent petit à petit laisser place à l'automatisation. Les solutions permettant d'industrialiser ces actions ont la part belle, comme par exemple dans le domaine de la surveillance ou de la détection, et ont pour enjeu de réduire le nombre de faux positifs souvent très chronophages. On peut également citer l'utilisation nouvelle de l'intelligence artificielle (ou plutôt du *machine learning*) dans ces domaines, et en particulier pour la lutte contre la fraude, permettant en effet de réduire ce nombre de faux positifs et donc gagner en efficacité.

Cette nécessité d'innover favorise la création de startups dans le domaine de la cybersécurité à l'échelle internationale. Cette année a montré l'amorce d'une transformation de l'écosystème des cyber-startups françaises : le dynamisme des startups n'est plus à prouver et les entrepreneurs français brillent par leur capacité à innover sur différents sujets de cybersécurité. Quelles actions concrètes permettraient d'intensifier le développement de ces startups, d'acquérir une nouvelle envergure et, ainsi, de confirmer le changement d'échelle amorcé ?

Un écosystème de plus en plus dynamique

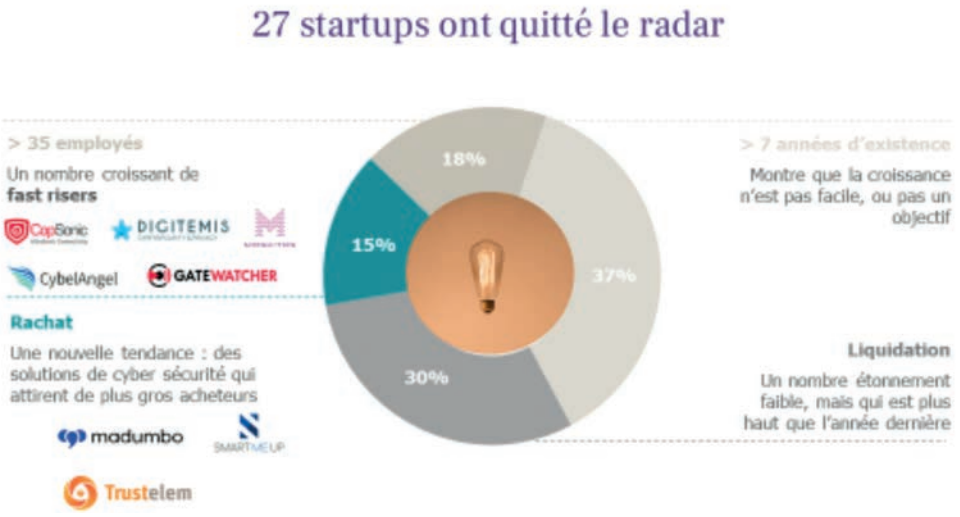
+ 18% de croissance en nombre de startups depuis janvier 2018

Nous recensons désormais 134 startups cybersécurité dans notre « radar des startups françaises en cybersécurité », ce qui représente 25 startups de plus qu'en janvier 2018. Il est intéressant de remarquer que leur taille évolue également de manière positive : si les « très petites entreprises » restent majoritaires, le nombre de « petites entreprises » a augmenté de près de 56 %. Au total, les startups représentent plus de 1 200 emplois, soit 9 % de plus que l'année précédente, et ce, pour la troisième année consécutive !



Concernant les sorties, 27 startups ont quitté notre radar, soit seulement 4 de plus que l'année dernière. Parmi ces dernières, 37 % sortent du radar à cause de leur ancienneté

(> 7 ans d'existence) et sans pour autant dépasser le critère de la taille limite (< 35 employés), ce qui est un signe de difficultés de croissance ou bien simplement d'un manque de volonté de croissance et de prise de risque par les fondateurs. Ce manque de prise de risque est appuyé par un faible taux de liquidation (30 %). Cependant, nous constatons cette année que les cas de croissance rapide (dépassant les 35 employés avant d'atteindre les 7 ans d'existence) sont plus nombreux (18 %) et observons même les premiers rachats (15 %), ce qui témoigne d'une attractivité plus forte de ces acteurs.



Au niveau géographique, peu de surprises par rapport aux années précédentes, avec un centre névralgique positionné sur le bassin parisien. L'écosystème reste néanmoins bien réparti avec des présences régionales issues des différents incubateurs. En particulier, le pôle rennais gagne en importance avec les nombreux investissements réalisés par le ministère des Armées qui souhaite y créer un véritable deuxième pôle d'expertise en France sur les sujets cybersécurité, comme le montre la présence de l'activité cybersécurité de la DGA sur son campus de Bruz.

Des signes particulièrement positifs pour la transformation de l'écosystème qui s'observent chez les clients…

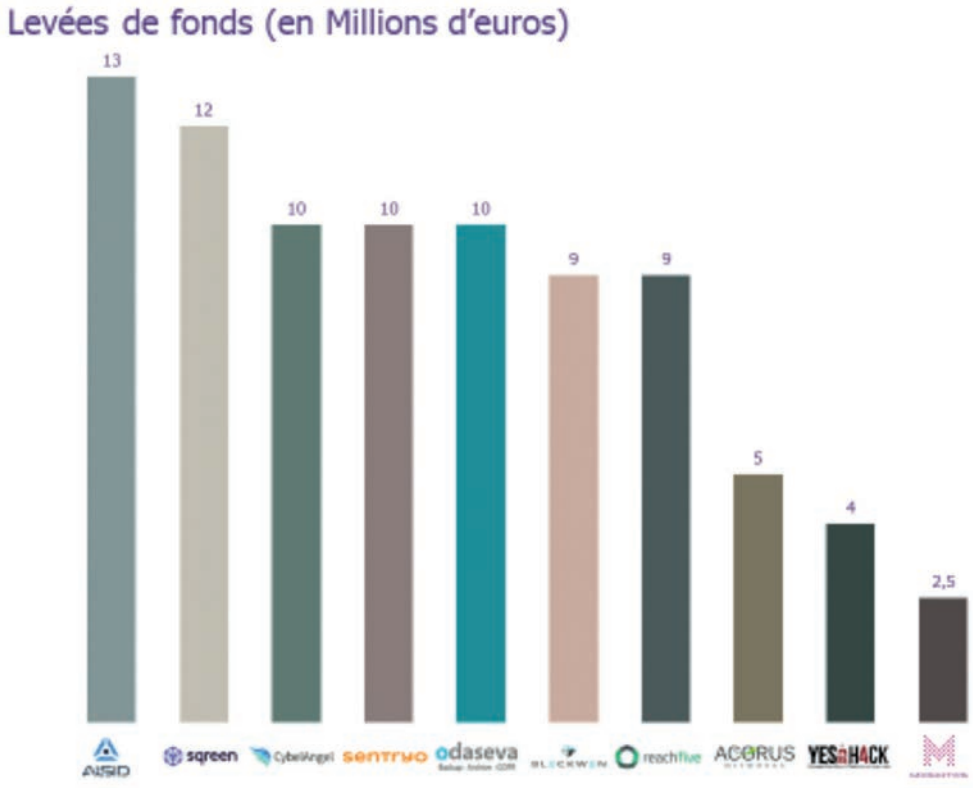
Identifié l'année dernière comme un axe essentiel au développement de l'écosystème, le financement des POCs [1] par les entreprises devient une pratique de plus en plus répandue puisqu'elle concerne 67 % des startups que nous avons interrogées. Cette démocratisation est un signe particulièrement positif pour l'écosystème, car en plus de supprimer cet investissement initial pour les startups, cela montre que les grands groupes évoluent et font confiance à nos pépites françaises.

… du marché…

On ne peut que saluer l'ampleur prise par les levées de fonds cette année. Au niveau de notre radar, le total est quatre fois supérieur à celui de 2017 et pas moins de sept startups ont levé des montants avoisinant les 10 millions d'euros. Il est également intéressant de mentionner la structure française Vade Secure qui a levé 70 millions d'euros *via* le fond américain General Catalyst, et la startup franco-américaine Dashlane qui a levé 110 millions de dollars. Il faut également noter que Vade

(1) *Proofs of Concept*.

Secure fera partie de Next40, ce programme d'accélération réservé aux 40 pépites de la French Tech et dévoilé récemment par le gouvernement. Cette ampleur est le résultat d'un début de démystification de l'écosystème qui permet aux investisseurs d'être moins frileux sur le sujet. Une autre preuve de cette confiance est la création d'un fonds d'investissement dédié, Brienne III. Cette structure qui a déjà réalisé un premier *closing* de 80 millions va permettre de continuer à rassurer les investisseurs et contribuer à l'« évangélisation » de l'écosystème.



Nous observons aussi les premiers *exits* des startups françaises. Ils concernent quatre startups de notre radar cette année, dont notamment Trustelem acquise en juillet par Wallix [(2)], Sentryo qui est en négociation avancée avec Cisco pour une intégration d'ici le premier trimestre 2020 [(3)], et Madumbo qui a été rachetée par l'éditeur franco-américain Datadog [(4)]. Ils sont une preuve que ces startups françaises sont de plus en plus différenciantes, ce qui les rend plus attractives. En revanche, ces *exits* sont très souvent portés par des structures étrangères et, dans la majorité des cas, ils entraînent la délocalisation des centres de décisions et de R&D de ces startups, ce qui reste dommageable pour l'entretien du dynamisme de l'écosystème et la souveraineté technologique en France.

Autre signe positif de l'évolution du marché, on observe également l'ouverture de la Défense, notamment avec la fondation de l'"Innovation Défense Lab" qui sera accueilli au sein du "Starbust

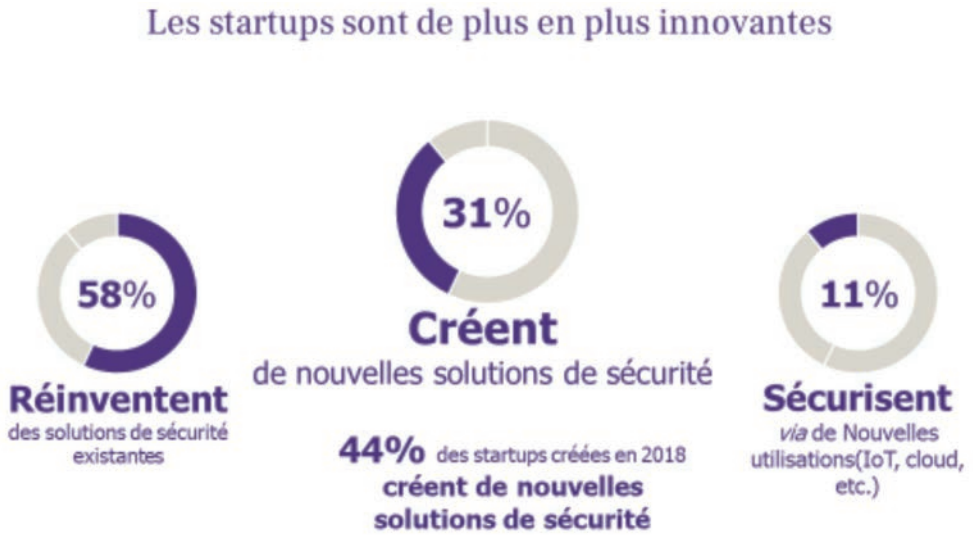
(2) WALLIX (2019), « Wallix signe la première acquisition de son plan ambition 21 », communiqué de presse.
(3) CERTES N. (2019), « Cisco prêt à mettre la main sur Sentryo », Le *Monde informatique*.
(4) CROCHET-DAMAIS A. (2019), « Datadog rachète la start-up parisienne MAdumbo et se renforce dans l'IA », *Journal du Net*.

Accelerator" et qui favorisera la collaboration des startups avec la DGA [5]. En parallèle, l'État a lancé un projet de campus de la cybersécurité. Cette entité aura pour vocation de créer des synergies entre les différents acteurs de l'écosystème en réunissant notamment des acteurs industriels, des startups, des universitaires, ainsi que certains ministères et agences [6].

…et des startups

L'internationalisation des startups reste un gros levier de croissance, et les startups cybersécurité françaises l'ont compris. La moitié de celles que nous avons interrogées ont déjà des clients à l'étranger, et 15 % sont en recherche d'opportunités à l'international : elles se donnent ainsi les moyens d'accéder à des marchés plus importants, plus stratégiques et potentiellement plus matures… et donc, de trouver les leviers de croissance nécessaires à leur développement.

De plus, le positionnement de l'innovation change pour l'année 2019 grâce à une augmentation de la proportion de startups innovantes parmi les nouvelles créations. En effet, 44 % des startups créées cette année proposent des solutions disruptives n'existant pas auparavant sur le marché. Cela porte à 31 % le nombre total de startups de notre radar appartenant à cette catégorie alors qu'il n'était que de 19 % l'année dernière.



Les entrepreneurs cybersécurité innovent dans les domaines matures de la cybersécurité, et ce malgré la concurrence. Ils n'hésitent pas à les aborder sous un angle nouveau afin de gagner des parts de marché, comme pour la gestion des identités et des accès (IAM), où certaines startups utilisent l'intelligence artificielle pour améliorer la rapidité de prise de décision, ou encore la sécurité de la donnée, où elles proposent par exemple des solutions de stockage décentralisé afin de rendre aux entreprises le contrôle de leurs données.

D'un autre côté, les startups comprennent les enjeux du marché et se positionnent sur les sujets « porteurs ». C'est le cas de la protection de la vie privée avec notamment la mise en application du RGPD, ou bien les solutions d'échange collaboratif qui promettent à la fois un niveau de sécurité élevé

(5) Ministère des Armées (2018), « Le ministère des Armées lance l'Innovation Défense Lab », Actualité de la DGA sur le site internet du ministère des Armées.
(6) Services du Premier ministre (2019), « Un campus cybersécurité pour renforcer l'écosystème français », communiqué de presse du service de communication des services du Premier ministre.

et une expérience utilisateur acceptable. Dans le même temps, la thématique de la gestion de crise a fait son apparition avec des solutions permettant d'assister les entreprises dans la gestion des crises de grande ampleur. En revanche, la sécurité par déception, qui consiste à tromper l'attaquant pour l'empêcher de mener à bien une attaque, est encore trop peu appréhendée par les startups françaises.

Des challenges qui freinent la progression des startups

Les échanges réalisés avec les équipes de startups présentes dans le radar permettent d'identifier des challenges concrets qui, pour certains, sont ambitieux à relever.

Les startups ont du mal à recruter des profils adéquats

À l'instar de l'ensemble du marché, les startups cyber sont confrontées à une pénurie de main-d'œuvre spécialisée. Les jeunes diplômés ne sont pas suffisamment formés à la cybersécurité dans les écoles françaises pour alimenter les effectifs ou être à l'initiative de création de startups. Cet état de fait, partagé par l'intégralité du marché en cybersécurité, est encore plus prégnant pour les startups qui ne peuvent pas souvent suivre la course salariale qui s'ensuit.

Des fondateurs de startups peu enclins à la prise de risque

66 % des fondateurs ont déjà expérimenté *une* création d'entreprise, mais rarement *plusieurs,* alors que la moyenne d'âge de ces entrepreneurs dépasse les quarante ans. Le profil des fondateurs révèle plutôt des experts que des *serial* entrepreneurs audacieux. Si on peut saluer la ténacité de certaines startups, il faut souligner la peur de l'échec qui est un problème récurrent en France, mais pas à l'échelle internationale. Par exemple, un entrepreneur de la Silicon Valley ou israélien ne sera vraiment considéré qu'après plusieurs échecs de création d'entreprise.

Une stratégie marketing carencée…

Les équipes des startups sont davantage composées de profils techniques et spécialisés sécurité, que commerciaux. Il en résulte une difficulté des startuppers à rendre leur offre commerciale attirante auprès des prospects. Des efforts sont à faire sur le volet marketing, aussi bien au niveau du produit que du discours. À titre d'exemple, les incubateurs anglo-saxons déploient des programmes d'accélération business élaborés, comme l'incubateur londonien Cylon dédié à la cybersécurité qui forme à « pitcher » efficacement sa startup auprès de potentiels investisseurs, clients et partenaires. Les startups d'outre-Manche et d'outre-Atlantique en récoltent les fruits et sont réputées pour leur force commerciale.

…qui se répercute sur les ventes

Les startups françaises ne rencontrent pas de problèmes liés à leur phase de création, mais ont en revanche du mal à faire connaître leurs solutions et à vendre à court et moyen terme. Seules 15 % des startups contactées nous ont confirmé faire plus de 500 000 euros de chiffre d'affaires. Parmi ces startups, deux tiers ont déjà entre 4 et 7 années d'existence sur le marché de la cybersécurité.

Comment concrétiser cette transformation ?

Pour les startups, apprendre à se vendre

Les startups doivent proposer des solutions sur étagère et ainsi atteindre un plus grand nombre de clients avec des coûts optimums. Pour ce faire, il est nécessaire que les fondateurs identifient et valorisent une proposition unique de vente plutôt qu'un segment de marché.

Un axe-clé pour eux serait de se positionner sur des problématiques non résolues par les solutions traditionnelles. En effet, les grands groupes sont plus enclins à collaborer avec les startups lorsqu'elles résolvent des problèmes pour lesquels aucune solution n'existe sur le marché. La startup Alsid, qui se distingue par son premier rang dans notre classement des levées de fonds, est un bel exemple puisqu'elle traite une problématique pour laquelle aucune solution n'existait auparavant : le monitoring de la sécurité d'Active Directory.

Savoir présenter un pitch clair et attirant en se concentrant sur les éléments différenciants est un axe d'amélioration-clé du développement des startups. En effet, c'est une étape cruciale dans la relation avec les investisseurs, les partenaires et les clients afin de les convaincre de la valeur ajoutée de la solution.

Un autre élément à envisager est de penser au design et à l'expérience utilisateur dès la création de la solution. Dans un marché où ces critères ne sont pas forcément pris en compte par les concurrents, cela peut représenter un vrai atout. Exemple singulier sur le marché, la startup israélienne Cybereason l'a bien compris et a engagé un *VP Créative & Head of Design* pour imaginer le design de ses produits parallèlement à la construction des fonctionnalités.

Pour finir, les startups ne doivent pas hésiter à réfléchir « international » dès leur lancement (langue de travail, documentation des codes sources, rédaction des documents produits…) afin de ne pas alourdir inutilement l'effort à fournir, déjà conséquent sur le plan commercial, pour accéder à des marchés plus matures et pouvoir ainsi accélérer le passage à l'échelle.

Pour le marché

Les avantages liés à l'incubation sont nombreux pour les startups (regard extérieur, service à prix réduit, proximité avec d'autres…), mais en même temps la cybersécurité est un domaine avec des besoins spécifiques (confidentialité, expertise scientifique, protection physique…). Ces raisons font que peu de startups en cyber trouvent leur place efficacement dans un incubateur standard. Cela exacerbe le besoin d'un incubateur spécialisé dans la cybersécurité. De plus, cet incubateur pourrait devenir un totem de l'innovation cyber « à la française » et un lieu d'accueil des investisseurs et des grands clients. La France réfléchit à se doter d'un hub dédié à la cybersécurité et les premières propositions ont été remises à Matignon à la fin du mois de novembre 2019. Il faut espérer que ce lieu proposera réellement un environnement propice au développement des startups, ainsi que des services d'accompagnement qui ne soient pas seulement liés à de l'aide à la recherche.

Enfin, il serait pertinent de favoriser la création de startups par d'anciens membres de la cyberdéfense des Armées ou de l'ANSSI. En effet, leur réseau et leur expertise professionnelle, acquis en début de carrière, sont des facteurs de succès dans l'écosystème cyber, comme l'ont prouvé les ex-collaborateurs de l'ANSSI et désormais fondateurs des startups Alsid et Citalid.

Pour les clients

Afin de permettre le développement de l'écosystème, les clients doivent accepter la prise de risque. Ils ont pour l'instant des difficultés à faire confiance et à contractualiser rapidement avec de jeunes structures innovantes. Pour un quart des startups interrogées, le temps de signature du contrat après la réalisation du POC est supérieur à six mois, et cette observation est particulièrement prégnante chez les grands groupes. Ces derniers devraient s'inspirer des grandes entreprises israéliennes qui se tournent très vite vers les startups lorsqu'elles identifient des problèmes pour lesquels le marché traditionnel n'offre pas de solutions en acceptant les risques mais en négociant également des tarifs très attractifs pour le futur.

On pourrait également envisager la création d'un accompagnement à la prise de risque de la part de l'État afin d'encourager la collaboration des grands groupes avec les startups. En restant sur l'exemple israélien, l'État a créé une agence indépendante qui sélectionne des projets innovants pour lesquels à chaque shekel investi par le secteur privé, l'État investit un shekel sans contrepartie [(7)].

Mobilisons-nous pour concrétiser la transformation

L'année 2019 a montré une vraie embellie dans l'innovation cybersécurité en France. Pour que l'écosystème continue sur sa lancée et concrétise son passage à l'échelle, les axes d'améliorations évoqués se doivent d'être accompagnés par un changement d'état d'esprit de l'écosystème, qui

(7) The Israeli Innovation Authority (2019), "About us", page internet du site officiel de The Israeli Innovation Authority.

demeure pour l'instant trop fermé. Avec la collaboration des différents acteurs, nul doute que la dynamique amorcée se confirmera. Les grands projets entamés à l'échelle de l'État, en particulier le Campus cyber, sont une opportunité unique pour transformer notre écosystème. Nous pouvons aussi nous réjouir des annonces récentes faites par le gouvernement, sur la création de fond de financement "late stage", qui pourront régler une partie des problèmes rencontrés sur le sujet, en particulier pour garder nos pépites en France ou *a minima* en Europe. Nous espérons observer l'an prochain les effets de ces annonces sur la croissance des startups et les levées de fonds.

Le RGPD au service de la cybersécurité

Par **Jean LESSI**
Commission nationale de l'Informatique et des Libertés (CNIL)

La cybersécurité, première des libertés informatiques ? Il n'est sans doute pas opportun de souhaiter à cette formule, dans le monde numérique, le succès que celle dont elle s'inspire a connu dans le monde physique. Les premières des libertés, à l'ère informationnelle, ce sont, plus que jamais, le droit au respect de la vie privée et le droit de chacun à maîtriser les usages faits de ses données personnelles. Mais l'on sait que, sans mesures appropriées de sécurité, et, plus encore, sans une culture profondément partagée de la cybersécurité, ces libertés individuelles sont des plus fragiles.

Cybersécurité et protection des individus, même combat

Ce n'est pas par le prisme des droits et libertés individuels que la cybersécurité vient d'abord à l'esprit, et donc à l'agenda, mais par celui de l'intérêt des organismes, et plus précisément de leurs intérêts vitaux. La crainte de l'interruption d'activité, bien sûr, vient en premier. Suivent les risques d'atteinte au patrimoine informationnel, qu'il s'agisse de secrets d'État ou de secrets industriels et commerciaux, à protéger contre toute menace de chantage ou contre des menées d'intelligence économique. Rien de nouveau, jusqu'ici, à l'ère numérique. Et pourtant, depuis les années 2000, les bases de données personnelles ont pris une place accrue dans ce patrimoine informationnel. Terreau de l'économie numérique, particules élémentaires d'un grand nombre d'activités commerciales, elles sont devenues un actif stratégique de grande valeur.

C'est là que se rejoignent les droits des individus et les intérêts des organismes traitant la donnée. On pourrait n'y voir qu'une superposition accidentelle. Or, les deux sont intrinsèquement liés. Une violation de données affecte simultanément deux catégories de victimes : les personnes physiques et les organismes (privés ou publics). Du côté des personnes physiques, s'il s'agit d'une atteinte à la confidentialité de leurs données, elles risquent purement et simplement de voir leur vie privée divulguée ou menacée de l'être avec les risques qui s'ensuivent : chantage, tentatives d'hameçonnage, voire usurpation d'identité. L'impact psychologique associé est réel. S'il s'agit d'une atteinte à la disponibilité ou à l'intégrité de leurs données personnelles (quand les données sont confiées à des tiers comme lors de la disparition de photos téléchargées sur un service en ligne, la disparition d'un dossier médical également chargé en ligne), les personnes perdent là aussi, selon des degrés divers, une forme de maîtrise de leur vie privée, voire intime.

Du côté des organismes, une violation de données représente une atteinte à leur réputation mais aussi parfois une perte économique sèche. On pourra citer à titre d'exemple l'attaque de la banque du Bangladesh qui permit de dérober 101 millions de dollars. Aucun organisme ne peut rester absolument indemne face au préjudice d'image et de réputation causé par un incident de sécurité affectant la protection de ses données dès lors que cet incident reçoit une publicité. Et les faits rappellent régulièrement que conserver le secret sur un incident n'est ni souhaitable, ni parfois possible en pratique, ni d'ailleurs légal, dans certains cas de figure.

On l'a vu, l'organisme et les personnes physiques ne sont que les deux faces d'une même médaille. De même, il est assez vain de vouloir distinguer, dans une politique de sécurisation de son patrimoine, les données personnelles et celles qui sont des données « non personnelles ». L'imbrication est fréquente et justifie une dynamique commune.

Ce qui caractérise surtout l'évolution récente de notre économie numérique, c'est que cette imbrication est de plus en plus systémique. Un incident reste rarement cantonné au face-à-face entre un organisme et un individu : ce sont le plus souvent des fichiers, des bases entières, qui sont concernés. Une attaque peut toucher une masse d'individus se comptant en centaines, en milliers voire en millions. De manière plus générale, la combinaison de la quantité, de la précision, de la variété, de la richesse des données traitées (qu'il s'agisse des données collectées initialement, de celles générées par l'activité des individus en ligne ou des données inférées par les opérateurs) fait de la sécurisation de ce patrimoine une condition absolue de la confiance que les citoyens peuvent nourrir dans les fondements mêmes de l'économie numérique.

La cybersécurité est donc la clé de voûte de ces modèles économiques. Il en va de même pour les nouveaux modèles d'administrations publiques que l'on a vus se développer depuis les années 1990 sur l'exploitation d'un seul et même terreau : la donnée personnelle. Côté pile, on trouve le patrimoine informationnel constitué de ces données, combinées, enrichies, massifiées. Côté face, on doit trouver la confiance des personnes physiques dans la capacité des organismes à traiter leurs données conformément à leurs engagements, et, en tant qu'ils en sont les dépositaires, à ne pas les perdre. L'équation ne se simplifie guère lorsqu'on y ajoute les nombreuses forces centrifuges de notre économie numérique : transferts internationaux (d'un point A à un point B, mais aussi les transferts ultérieurs), multiples intermédiaires au sein de chaînes de sous-traitance ou de coresponsabilité parfois complexes et opaques, stockage dans le *cloud*, etc.

Le RGPD, un puissant outil de cybersécurité

La loi Informatique et Libertés du 6 janvier 1978 n'avait pas la réputation d'être un instrument de cybersécurité. Et pourtant, elle l'était au plus haut point. Dès 1978, son article 29 précisait que : « Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés. » Tout y était : l'obligation, sa définition, et sa raison d'être, à savoir la confiance mise par les déposants dans le dépositaire. Et de fait, la sécurité était déjà omniprésente dans les contrôles opérés par la CNIL et leurs suites répressives. Bon an, mal an, au moins 80 % des contrôles mettaient en lumière des manquements à l'obligation de sécurité, et une majorité des sanctions prises chaque année par la formation restreinte de la CNIL épinglaient des manquements de cette nature.

Cependant, force est de constater que la loi de 1978, avant-gardiste d'une certaine manière, n'a pas pu ou su créer l'électrochoc nécessaire pour rehausser le niveau de sécurité des organismes français, publics ou privés. S'inscrivant dans la continuité du texte français et en application depuis le 25 mai 2018, le Règlement général sur la Protection des Données (RGPD) doit désormais venir en concrétiser pleinement les promesses.

Le RGPD reprend, tout d'abord, l'obligation de sécurité. Sans en modifier en rien la substance, il en enrichit – et en allonge – la formulation. Sans entrer dans les détails, on peut mentionner le soin mis par l'article 32 à souligner la nécessaire adéquation et proportionnalité des mesures de sécurité à la nature et à l'intensité concrètes des risques dans chaque contexte ; la mention expresse du chiffrement dans la panoplie des mesures ; l'approche très large retenue de la notion de sécurité, incluant « la confidentialité, l'intégrité, la disponibilité et la résilience constantes » des systèmes d'information, etc. Rien dans cette approche n'est étranger à la doctrine d'emploi, par la CNIL, de la loi du 6 janvier 1978. Mais tout est désormais écrit, expressément.

Innovation apportée par le RGPD : le niveau des sanctions désormais applicables est considérablement rehaussé. À la hauteur des enjeux, les sanctions peuvent aller jusqu'à 2 % du

chiffre d'affaires mondial ou 10 millions d'euros pour un manquement à la sécurité – le plus élevé des deux plafonds étant retenu.

Le RGPD rend donc plus crédible l'obligation de sécurité préexistante. Par ailleurs, tenant compte des écosystèmes complexes de traitement des données, il met à la charge des sous-traitants des obligations propres – assorties de sanctions propres aux prestataires – en matière notamment de sécurité, alors que le droit antérieur ne connaissait qu'une seule tête : le responsable de traitement. Cela ne signifiait pas que le sous-traitant était déresponsabilisé avant le 25 mai 2018, mais sa responsabilité était avant tout contractuelle ou commerciale, par ricochet. Désormais, le contenu du contrat est spécifié à l'article 28 et le sous-traitant doit en outre répondre, devant le régulateur voire devant le juge, de ses obligations en matière de sécurité.

Mais la principale innovation du RGPD, propre au domaine de la cybersécurité, réside dans la mise en place de multiples procédures autour de l'obligation de sécurité, la mettant ainsi au cœur de la gouvernance et des process des organismes et créant d'utiles cordes de rappel pour les organismes qui la perdraient de vue.

On peut notamment citer le dispositif mis en place en cas de violation de données. À trois étages, ce dispositif va *crescendo* en fonction du degré de risque pour les droits des personnes. Si la violation n'entraîne pas de risque, le responsable du traitement doit seulement documenter, en interne sous forme d'un registre, la violation qui vient de se produire. Si elle entraîne un risque, il doit en outre notifier cette violation à la CNIL, au plus tôt et dans un délai en principe maximal de soixante-douze heures. Si la violation entraîne un risque élevé, il doit, enfin, informer les personnes concernées de la violation dont leurs données ont fait l'objet, au plus tôt. L'organisme peut différer cette information (à la différence de la notification à la CNIL) en cas de nécessité, liée par exemple à la mise en place d'une opération de cyberdéfense ou à l'ouverture d'une enquête sur l'origine et les canaux de l'attaque.

Cette nouvelle « discipline de la sécurité » monte progressivement en puissance. Au cours de la première année d'application du RGPD, la CNIL a reçu plus de 2 000 notifications de violation – pour environ 89 000 au niveau de l'Union européenne, avec de fortes variations d'un État à l'autre. Ce dispositif à trois étages a, en réalité, une triple vertu : faire monter en compétence les organismes sur les questions de cybersécurité en les incitant à mieux maîtriser leurs risques et à apprendre à réagir en cas d'incident ; protéger les personnes physiques concernées par une violation contre les risques subséquents (hameçonnage par exemple) ; intérioriser le caractère systémique des enjeux de sécurité qui lient l'entité et l'ensemble des personnes physiques embarquées dans ses traitements de données, et proportionner les obligations de l'une aux risques causés pour les autres.

Le RGPD prévoit une autre obligation procédurale en matière de sécurité : la réalisation, avant la mise en œuvre d'un traitement susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques, d'une analyse d'impact relative à la protection des données. L'analyse d'impact est, fondamentalement, une analyse de risque évaluant de façon formalisée les impacts sur les personnes et sur les entreprises. Elle inclut un plan d'action en matière de sécurité et également un principe d'amélioration continue. De nouveau, l'obligation de procédure, de méthode, doit conduire à se poser les bonnes questions, à acquérir des réflexes, à trouver des solutions pour, au final, mieux protéger (et donc mieux traiter) les données personnelles des uns et des autres.

La cybersécurité et le RGPD, du texte à la politique publique

Un texte ne fait pas une politique publique. C'est en impulsant dans son domaine et en animant, aux côtés d'autres institutions, une véritable politique publique de cybersécurité que la CNIL entend traduire en actes les potentialités du RGPD – et contribuer à rehausser collectivement d'un

ou, si possible, de plusieurs crans le niveau de « cybersécurité collective » dans notre pays, tant le niveau de départ est, pour le dire pudiquement, perfectible.

Cela suppose, tout d'abord, de tenir un discours de cybersécurité accessible à tous les organismes, des plus petits aux plus gros. En matière de protection des données personnelles, l'expérience montre que c'est en embarquant tout l'écosystème économique et administratif que l'on peut efficacement limiter les points de fuite, tant ils sont nombreux. La cybersécurité doit donc se démocratiser, et toucher les petites et moyennes entreprises, les collectivités publiques de petite taille, ou encore le secteur associatif. La CNIL leur consacre des outils dédiés (guide PME-TPE élaboré avec la Banque publique d'Investissement, guide dédié à la sensibilisation des collectivités territoriales), en cohérence avec les contenus éditoriaux de l'ANSSI (qui a publié en partenariat avec la CPME un guide des bonnes pratiques de l'informatique). Elle cherche également de plus en plus à développer des contenus pédagogiques à leur attention (registre simplifié des opérations de traitements, etc.) Cette orientation doit se poursuivre dans les années à venir, possiblement sous de nouvelles formes (recommandations, règlements-types, etc.). La pédagogie ne passe pas seulement par le discours, mais aussi par des outils maniables, numériques, pour passer aux travaux pratiques. La CNIL a ainsi outillé ses guides « sécurité » et « AIPD » dans un logiciel gratuit et *open source*, disponible en dix-huit langues.

Mais cela suppose aussi de sensibiliser et de faire monter en compétence les citoyens eux-mêmes sur les sujets de cybersécurité. En effet, tout ne peut pas reposer sur les seuls organismes : les individus ont leur propre part de responsabilité. Sans verser dans un quelconque pessimisme, le caractère systémique des risques, à l'ère informationnelle, nécessite, très sérieusement et avec détermination, une mobilisation de tout le tissu social autour de cet enjeu commun. L'éducation au numérique sous toutes les facettes, c'est-à-dire l'éducation aux « dessous des cartes » de l'économie numérique, aux bonnes et mauvaises pratiques en ligne, et en particulier aux bons réflexes à adopter dans la sécurisation de sa vie privée (et de celle des autres) sur le web, fait partie intégrante de cette entreprise. Les « 10 conseils pour rester net sur le net », la réalisation d'une vidéo du Youtubeur *Le rire jaune* en partenariat avec la CNIL et la MGEN, et d'autres actions de la CNIL ou des membres du collectif Educnum, tendent à diffuser cette culture.

L'entrée en application du RGPD marque donc une étape essentielle dans le rehaussement du niveau de cybersécurité du pays et du continent européen. Il ne fera pas tout, loin de là. Mais au-delà des obligations connexes et des procédures qu'il a créées, le RGPD aura apporté sa pierre. Il jette les bases, en matière de cybersécurité, d'une politique publique. Il est temps de mesurer l'imbrication des enjeux pour les citoyens comme pour les organismes et d'être à la hauteur.

Une agence au cœur de la cybersécurité européenne

Par **Jean-Baptiste DEMAISON**
ENISA

Une prise en compte précoce des enjeux de cybersécurité au niveau européen

Une agence européenne, avant l'heure

Base Héraklion

Alors que la plupart des États membres de l'Union européenne (UE) ne disposaient pas encore d'agence dédiée aux enjeux de cybersécurité, le Conseil de l'UE et le Parlement européen ont décidé en 2004 (1), la création de l' « agence européenne pour la sécurité des réseaux et de l'information », l'ENISA. Son mandat a été prolongé à deux reprises en 2008 puis en 2011 avant d'établir l'agence à titre permanent en 2019 (voir *infra* « Le *Cybersecurity Act* : révolution certification »).

Basée en Grèce et initialement établie à Héraklion selon le souhait des autorités grecques – avant son déplacement progressif à Athènes – l'ENISA a vu son positionnement progressivement renforcé au sein de l'écosystème institutionnel européen ainsi qu'auprès des États membres, à mesure que l'enjeu de la cybersécurité s'est imposé au cœur des préoccupations des décideurs publics. Chargée en priorité de conseiller les États sur le développement des capacités de cybersécurité (*capacity building*), l'ENISA s'est notamment illustrée dans le développement de corpus méthodologiques et d'offres d'accompagnement ayant permis la mise en place de plusieurs CSIRTs (2) gouvernementaux (équipes de réponse à incidents) et de stratégies nationales de cybersécurité.

Très tôt, l'ENISA a également choisi de jouer un rôle actif en faveur du développement de la coopération entre États, en particulier au travers du cycle d'exercices « Cyber Europe ». Organisé tous les deux ans depuis 2010, celui-ci a permis de simuler des crises d'origine cyber de dimension européenne affectant des secteurs critiques (énergies, télécommunications, etc.) et de tester la capacité des États à y faire face ensemble. Ces exercices ont, en outre, permis de préfigurer le développement de mécanismes de coopération technique et opérationnelle, tels que des procédures standards opérationnelles (3).

L'agence européenne a été sollicitée pour accompagner l'élaboration et la mise en œuvre des politiques publiques européennes en matière de cybersécurité. L'ENISA a notamment joué un rôle actif auprès des États dans le cadre de la mise en œuvre de l'article 13a du « paquet télécom », première législation européenne à avoir inclus des obligations en matière de cybersécurité pesant aujourd'hui sur les opérateurs de télécommunications.

Sécurité économique vs. sécurité nationale

Imaginée par la Commission européenne au début des années 2000, l'ENISA devait, à l'origine, répondre à la nécessaire sécurisation de l'Internet européen, afin de garantir la sécurité du marché

(1) Règlement (CE) n°460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (texte présentant de l'intérêt pour l'EEE).
(2) *Computer Security Incident Response Team*.
(3) *Standard Operating Procedures ou SOPs*.

unique à l'heure de sa transformation numérique. Celle-ci a ainsi été établie sur la base juridique du marché intérieur, domaine de compétences partagées entre l'UE et les États membres. L'arrivée de l'agence n'a, de ce fait, pas été sans susciter une certaine prudence de la part d'États habitués à traiter seuls des enjeux de sécurité informatique *via* le prisme régalien de la sécurité et de la défense nationale.

À plusieurs reprises par la suite, la question de la compétence de l'UE et du rôle de l'ENISA sur les aspects les plus sensibles de la cybersécurité s'est posée. L'ENISA a notamment vu son rôle encadré en matière de soutien opérationnel aux États victimes de cyberattaques, dont le caractère volontaire a été très tôt consacré, à l'initiative d'États – dont la France – ayant considéré qu'il incombait à chacun de se doter d'une capacité de réponse autonome. *A contrario*, un modèle centralisé au niveau européen aurait-il été privilégié à l'époque, plutôt qu'un modèle de capacités décentralisées et de coopération, il y a fort à parier que ces capacités européennes seraient insuffisantes pour protéger l'UE face à la menace cyber actuelle.

Un cadre de régulation en développement

La protection des infrastructures critiques

À mesure que l'enjeu de la cybersécurité a pris de l'ampleur au niveau politique européen, l'utilité d'une action coordonnée des États et de l'UE pour relever le défi commun de la souveraineté numérique de l'Europe face aux menaces pour la sécurité et la confiance numériques, s'est progressivement imposée comme une évidence.

Après deux communications de la Commission européenne dédiées à la protection des infrastructures d'information critiques (*Critical Information Infrastructure Protection* ou CIIP), une étape importante a été franchie en 2013 avec la proposition de directive sur la sécurité des réseaux et des systèmes d'information (« directive NIS »). Adoptée en 2016 [4], la directive NIS a étoffé et étendu les règles de sécurité contraignantes applicables aux opérateurs de télécommunications, à des « opérateurs essentiels au maintien d'activités sociétales et/ou économiques critiques » dans des sept secteurs incluant l'énergie, la banque ou encore les transports : obligation de mise en œuvre de règles de sécurité, clarifiées dans un document de référence non contraignant adopté par l'ensemble des États membres de l'UE en 2018 [5] ; obligation de notifier les incidents informatiques ayant un impact significatif sur leurs services essentiels, à leur autorité nationale compétente ou à leur CSIRT national/gouvernemental.

La directive NIS a également établi un cadre de coopération formel entre États en matière de cybersécurité, au travers de deux enceintes respectivement de niveaux politique et technique. Premièrement, le « groupe de coopération », réunissant des représentants des agences nationales de cybersécurité, la Commission européenne et l'ENISA, chargé de soutenir et de faciliter la coopération stratégique entre les États membres ; faciliter l'échange d'informations, renforcer la confiance mutuelle et élever le niveau global de maturité et les capacités nationales de cybersécurité. Deuxièmement, le « réseau des CSIRTs », premier réseau de coopération technique et opérationnelle réunissant l'ensemble des États membres de l'UE et du CERT-EU, activement soutenu dans son fonctionnement par l'ENISA. Lancé en 2017, ce réseau a rapidement confirmé son utilité en ayant facilité les échanges entre CERTS nationaux de plusieurs États membres, dont la France et l'Estonie, en réponse aux crises *Wanna Cry* et *NotPetya*.

(4) 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.
(5) http://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf

Peu de temps après, le Conseil de l'UE s'est également doté d'un premier groupe informel consacré à la cybersécurité (le groupe des amis de la présidence cyber) devenu en 2017, groupe de travail formel, chargé de traiter des enjeux stratégiques et diplomatiques de la cybersécurité (le groupe de travail horizontal sur les questions cyber).

Une stratégie pour l'Europe

Proposée en 2013, la directive NIS l'a été à l'occasion de la publication de première la stratégie européenne de cybersécurité [6], offrant pour la première fois des orientations stratégiques en matière de cybersécurité sur l'ensemble du spectre des domaines de compétences de l'UE.

Au-delà de la cybersécurité du marché unique du numérique, pris en compte par l'ENISA et dans la directive NIS, la stratégie a souligné l'importance d'un positionnement de l'UE sur les enjeux cyber diplomatiques et de défense. Ce volet émergent du portefeuille cyber européen a vu le jour dans la continuité des travaux conduits depuis plusieurs années à l'ONU, avec l'implication de plusieurs États européens dont la France, sur les règles de droit international et les normes de comportement responsables des États dans le cyberspace. En 2017 [7], cette orientation s'est concrétisée par l'adoption, par les États membres, d'une boîte à outils cyber diplomatique établissant une doctrine de prévention, de coopération et d'escalade contrôlée de l'UE, pouvant aller jusqu'à des mesures coercitives, face aux cyberattaques malveillantes dont pourraient être victimes ses États membres.

La stratégie européenne de cybersécurité a également mis au centre du débat public l'enjeu de l'autonomie stratégique de l'UE en matière de produits et de solutions numériques et de sécurité. Actant pour la première fois à ce niveau les risques de « dépendance » de l'Europe à l'égard de solutions développées en dehors de son territoire, cet axe de travail a notamment conduit à la signature d'un partenariat public-privé entre la Commission européenne et l'organisation européenne de cybersécurité (ECSO), avec pour objectif de rassembler des représentants publics, privés et académiques en vue de stimuler le développement de l'écosystème industriel cyber européen.

La création en 2012, peu de temps avant la publication de la stratégie européenne, d'un CERT dédié aux institutions, agences et entités de l'UE avait également été signalé comme une décision majeure de l'UE en faveur du renforcement de sa propre cybersécurité. Confirmé dans son rôle et ses missions, le CERT-EU constitue aujourd'hui l'un des garde-fous pour la sécurité des données sensibles de l'UE et celles confiées à l'UE par les États membres.

Une nouvelle agence, à l'aube d'une nouvelle ère

Le *Cybersecurity Act* : révolution certification

Un mandat renforcé

L'adoption en 2019 du règlement européen « *Cybersecurity Act* » constitue un virage pour la cybersécurité européenne. Il dote, tout d'abord, l'ENISA d'un nouveau mandat, désormais permanent, confirmant le caractère incontournable de l'agence dans la prise en compte des enjeux de cybersécurité au niveau européen. Actant, par ailleurs, son implantation à Athènes avec le soutien des autorités grecques, le règlement tourne également une page de l'histoire de l'ENISA qui ne s'écrira désormais plus depuis la Crète.

(6) Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé ».
(7) "Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities" ("Cyber Diplomacy Toolbox"), Brussels, 7 June 2017, 9916/17.

Au-delà de l'établissement durable de l'ENISA dans le paysage institutionnel européen, le *Cybersecurity Act* étoffe les missions principales de l'agence et lui en attribue de nouvelles. En changeant de nom et en devenant l'« agence européenne pour la cybersécurité », l'ENISA entre dans une nouvelle ère [8]. Le rôle de l'ENISA en matière de soutien à la coopération opérationnelle des États en réponse aux incidents informatiques est ainsi renforcé, en permettant notamment à l'agence de faciliter désormais, à la demande d'États, la gestion technique d'incidents ou de crises dont ils seraient victimes. Active depuis plusieurs années en faveur de la sensibilisation du grand public au risque numérique, au travers du « mois européen de la cybersécurité » [9], son action en la matière est érigée au rang de mission principale, au même titre que le soutien au développement capacitaire des États et le développement d'une expertise européenne en matière de cybersécurité.

Un cadre pour la certification en Europe

Nouvelle mission majeure pour l'ENISA et véritable rupture pour l'Europe, le *Cybersecurity Act* établit également un « cadre européen de certification de sécurité numérique », inspiré d'un accord de coopération (SOG-IS) ayant réuni jusqu'à plus d'une dizaine d'États membres, qui avaient accepté la reconnaissance mutuelle des certificats de sécurité émis dans leur pays respectifs.

Derrière l'appellation technique experte se cache une révolution en germe pour la sécurité et la confiance numérique en Europe. Ce cadre établit des principes et mécanismes communs à l'ensemble des États membres de l'UE, permettant d'évaluer et de certifier le niveau de sécurité de potentiellement tout type de solution ou de service numérique bénéficiant d'un schéma de certification, à différents niveaux d'exigences de sécurité (élémentaire, substantiel, élevé). *Cloud*, systèmes embarqués, systèmes de contrôle industriels… le champ des possibles est gigantesque et permet d'entrevoir un espace numérique européen où les citoyen(ne)s, entreprises, industriels et administrations seront un jour en mesure de s'appuyer sur une évaluation fiable, et reconnue partout en Europe, du niveau de sécurité des solutions numériques qu'ils souhaitent déployer.

Volontaire par conception, ce cadre de certification n'en est pas moins disponible, dans le cas où les législateurs européens décideraient de rendre contraignante la certification de certaines solutions ou services, dans le cadre de futures directives ou de futurs règlements sectoriels ou spécifiques à un domaine technologique. Le potentiel de ce cadre dépasse, en outre, le renforcement du niveau de sécurité numérique des européen(ne)s. Dans un contexte de prise en compte croissante de l'enjeu de la sécurité des sytèmes d'information et de la protection des données, avec le règlement général sur la protection des données à caractère personnel, l'introduction de la certification de sécurité européenne est un nouveau signal envoyé à l'international, sur le refuge que constitue de manière croissante l'UE pour les données.

Une plateforme européenne pour faire passer à l'échelle le modèle de cybersécurité européen

Un défi de gouvernance

Le *Cybersecurity Act* constitue une étape importante pour la cybersécurité européenne et un changement d'échelle pour l'ENISA. Il ne constitue toutefois qu'une étape dans le cheminement

(8) À titre d'anecdote, le nom « agence européenne pour la cybersécurité » est le résultat d'un compromis, proposé par la France, visant à réconcilier les tenants du renoncement au concept de « sécurité des réseaux et de l'information », devenu obsolète et ceux qui « ne souhaitaient pas que l'ENISA fût une "agence *de* cybersécurité" comme les autres », apparentant son champ de compétence à celui d'une agence nationale, alors que l'ENISA n'avait toujours pas vocation à assurer pour des bénéficiaires directs leur cybersécurité.
(9) *European Cybersecurity Month*.

vers une gouvernance et des mécanismes européens aptes à répondre à l'ensemble des défis posés à la cybersécurité européenne.

Dans le contexte de la transformation numérique accélérée de l'ensemble des acteurs économiques et de la société, la capacité de l'Europe et des États membres à se protéger des menaces et à y répondre, passera par un modèle de coopération efficace et respectueux des compétences nationales, qui conditionne le développement de la confiance. Au cœur de cette dynamique, l'ENISA devra basculer d'un modèle de facilitation à un modèle de « plateforme » ouverte apte à agréger et à diffuser le meilleur des connaissances, de l'expertise à l'état de l'art. Elle devra également parvenir à faire converger, lorsque cela est nécessaire, les acteurs pertinents de l'écosystème, comme dans le cadre de l'élaboration des schémas de certification.

L'ENISA devenue « plateforme européenne pour la cybersécurité » devra également signifier qu'elle est une agence apte à agir avec agilité et en tant que point de référence incontournable pour l'ensemble des institutions, agences et entités de l'UE, de plus en plus conscientes des enjeux de cybersécurité. Alors que les initiatives sectorielles prenant en compte le risque numérique, telles que dans le domaine de l'aviation ou l'énergie, vont se multiplier à l'avenir, l'ENISA devra être garante d'une prise en compte d'exigences de cybersécurité adaptées et demeurer une conseillère privilégiée auprès des instances européennes.

De nouveaux défis de régulation

Suite à la nomination d'une nouvelle Commission, de nouvelles initiatives devraient voir le jour dans les mois à venir : la question de la prochaine législation consacrée à la cybersécurité se pose d'ores et déjà. Alors que la perspective d'une version 2 de la directive NIS se fait jour, une approche alternative ou, au moins, parallèle pourrait être de choisir de faire peser les prochaines obligations réglementaires européennes en matière de cybersécurité, sur les fournisseurs de produits et services numériques eux-mêmes plutôt que sur leurs utilisateurs : disponibilité des mises à jour de sécurité, certification, sécurité par défaut, fin de vie des produits, séquestre des codes sources en cas de cessation d'activité… sont autant de pistes à explorer pour renforcer la sécurité des solutions déployées.

Les acteurs de *supply chain* numérique, tels que les intégrateurs, chargés de répercuter les mises à jour, devraient également être concernés. Une telle perspective confirmerait l'orientation stratégique du cadre européen de certification, conçu pour amener des solutions sécurisées *by design* et par défaut aux utilisateurs, et ce faisant, accroître leur confiance dans les usages numériques. De surcroît, ce choix s'inscrirait en cohérence avec les principes de l'Appel de Paris lancé en 2018 par le Président de la République en faveur de l'élaboration de principes communs de sécurisation du cyberespace.

Le cyber en assurance, un risque presque comme les autres ?

Par **Benjamin DUCOS**
et **Luc de LIGNIÈRES**
AXA

Depuis plusieurs semestres, la forte croissance du nombre d'attaques cyber et la violence des conséquences extrêmes – opérationnelles, financières ou réputationnelles – qu'elles font peser sur les organisations qui en sont victimes renforcent la nécessité pour ces entreprises ou institutions de se protéger efficacement. Dans un marché de la cyber assurance estimé à moins de cinq milliards d'euros, mais en forte croissance – on parle de 30 % par an –, les regards se tournent vers les assureurs avec une double question : en quoi l'assureur peut-il contribuer, *via* des mécanismes d'assurance cyber, à la protection de ses clients, particuliers ou entreprises ? Et comment l'assureur se prémunit-il du risque opérationnel, c'est-à-dire du risque de ne pas être en mesure de servir ses assurés, face à la menace cyber ?

Le cyber en assurance, un risque presque comme les autres ?

Le risque cyber en assurance présente des caractéristiques d'un risque traditionnel en assurances dommages : il est incertain et imprévisible ; il se couvre en assurances tant pour les particuliers que pour les entreprises ; sa couverture d'assurance se définit à travers différentes garanties ; il peut toucher un ou plusieurs assurés simultanément comme cela arrive dans tout autre événement ; enfin, à l'instar de tout risque traditionnel, la prévention joue un rôle déterminant.

Pourtant le risque cyber présente des caractéristiques qui lui sont propres. Tout d'abord, il est systémique : comme un tremblement de terre, sa propagation peut être fulgurante, et toucher simultanément toutes les catégories d'assurés, qu'ils soient particuliers ou entreprises. Mais à la différence du tremblement de terre, il est potentiellement géographiquement sans limites. Il est également mal connu. La distribution du risque cyber s'apparente à une courbe qui tend vers un « Dirac [1] » : au regard d'événements moyens d'impact modéré, l'événement majeur est supposé très rare et ses conséquences extrêmes. Or, aucun événement majeur n'est survenu jusqu'à présent qui permettrait d'en déduire des impacts ! Le coût de l'événement majeur est donc soumis aux interprétations et estimations des parties prenantes dans la modélisation du risque (assureurs, fournisseurs de modèles, intervenants informatiques…). Dès lors, les primes d'assurance ne reflètent qu'imparfaitement le risque. Tant que l'événement majeur ne survient pas, la modélisation de la profitabilité du segment cyber reste incertaine. Enfin, il est en permanente évolution, sujet aux progrès techniques apportés dans l'industrie informatique, que ces progrès viennent des opérateurs, des dispositifs de sécurité mis en place par les clients ou de l'ingéniosité des hackers.

L'assureur dispose d'une double perspective sur le risque cyber : la compagnie d'assurance est à la fois dans le fauteuil du conducteur, en tant qu'assureur expert de ce type de risque, mais également sur le siège du passager, en tant que société majeure dans le paysage économique, et

(1) La distribution de Dirac est une fonction qui prend une valeur infinie en 0 et 0 sur le reste de la distribution. Appliquée au cyber, cela reviendrait à dire que l'événement de probabilité (quasi) nulle prend une valeur extrême alors que les autres événements de la distribution ont un coût (quasi) nul.

donc potentiellement cible d'attaques cyber. La stratégie cyber d'un assureur s'articule autour de deux volets : être capable d'offrir des protections d'assurance à ses clients contre le risque cyber (l'assureur cyber) tout en se protégeant lui-même contre le risque opérationnel émanant du cyber. C'est ainsi que la gestion du risque de l'information, au sens du risque opérationnel porté par l'assureur, et les fonctions commerciales ou expertes (tarification ou mesure de l'exposition par exemple) travaillent très étroitement ensemble pour faire progresser la connaissance qualitative et quantitative de ce risque.

La connaissance qualitative résulte en effet à la fois de l'observation jour après jour des risques et menaces qui pèsent sur l'assureur, d'un dialogue resserré entre chaque échelon de l'environnement de contrôle ainsi que d'un enrichissement mutuel avec les typologies d'incidents qui affectent les assurés. Des passerelles sont régulièrement à tirer entre les événements, afin d'accroître la compréhension de ces phénomènes : il ne se passe pas une semaine sans qu'un incident ne déclenche une investigation technique sous l'angle cyber, soit chez l'assureur en propre, soit chez un de ses assurés. La mesure quantitative est également une dimension-clé car elle permet de connaître, et donc d'agir, sur le niveau d'acceptation du risque cyber. Pour cela, les assureurs doivent identifier leur exposition au risque cyber au travers de leur activité mondiale d'assurance, d'une part, et de leur risque opérationnel lié à l'information, d'autre part. Des travaux qui sont menés sur ces quantifications doit découler une compréhension fine et chiffrée de l'exposition globale de l'assureur au risque cyber.

En tant qu'institution financière de premier ordre qui subit des attaques et qui gère ses propres risques opérationnels, l'assureur est donc bien placé sur ce sujet : le fait d'être à la fois une cible et un grand acteur de la prévention et de la protection permet d'allouer à la compréhension des ressorts du risque cyber des moyens plus importants que ne peuvent le faire d'autres acteurs. Et cette connaissance intime peut être partagée avec l'expertise mise à la disposition des assurés en matière de risque cyber.

De la couverture implicite à la couverture explicite… deux cas de figure

Pour l'assureur comme pour l'assuré, deux cas de figure se présentent :

- soit le risque cyber est implicitement protégé dans les couvertures traditionnelles au travers des garanties dommages aux biens ou responsabilité civile. On parle alors de « couverture silencieuse » (*silent coverage* ou *non-affirmative coverage)*.
- soit des garanties sont délivrées explicitement et spécifiquement pour couvrir le risque cyber. Ces garanties sont regroupées sous le vocable de « couverture affirmative » (en anglais, *affirmative coverage)*. Les garanties se subdivisent en trois segments : pour les entreprises, les garanties dommages propres (qualifiées de *first party* en anglais) couvrent les pertes subies sur les biens de l'assuré : pertes de données, perte d'exploitation, rançon et extorsion… Toujours pour les entreprises, les garanties de responsabilité civile (*third party* en anglais) qui protègent l'assuré contre les dommages aux tiers qu'il pourrait générer, de façon similaire à l'offre des garanties responsabilité civile : fuite de données personnelles, erreurs et omissions liées à la réalisation du risque cyber. Pour les particuliers enfin, les garanties offertes sont relatives au vol d'identité, au vol des moyens de paiement, à un conflit avec un commerçant en ligne ou encore à des actions de e-réputation visant à restaurer l'image sur Internet.

Nous pourrions penser que les couvertures silencieuses suffisent à protéger l'assuré contre le risque cyber et que les couvertures affirmatives sont donc inutiles. Ce n'est pas le cas car la couverture affirmative apporte un vrai plus en termes de garanties. Pour illustrer la différence entre couverture silencieuse et couverture affirmative, prenons l'exemple d'une usine affectée par une attaque cyber,

par exemple provoquant le dérèglement d'un programme informatique. Imaginons que cette attaque conduise à l'incendie de l'usine : la couverture silencieuse agit car le feu est couvert en dommages aux biens ; la couverture affirmative couvrira quant à elle la perte de données consécutive à l'événement cyber. Supposons maintenant que l'usine ne brûle pas mais ne puisse plus fonctionner : la couverture silencieuse ne peut jouer car il n'y a pas de dommages matériels (incendie ou dommage matériel aux machines par exemple) et la perte d'exploitation consécutive à un dommage matériel ne peut donc s'appliquer. La garantie cyber de la couverture affirmative, outre l'indemnisation de la perte de données, agit également au titre de la garantie perte d'exploitation *first party*.

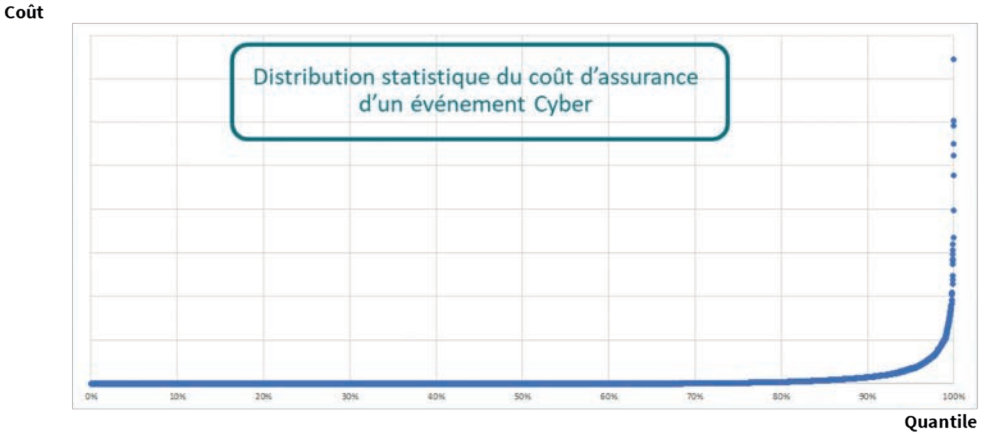
L'assurance cyber, poussée par les nouveaux usages

L'assurance cyber est le fruit de son époque, et son développement est le résultat combiné de plusieurs facteurs technologiques, réglementaires ou événementiels. Tout d'abord, l'utilisation massive de données et la digitalisation rapide des échanges avec les usagers ou les clients exposent les organisations aux risques de l'information (fuite, piratage, etc.) ; or, les nouveaux usages d'informatique dématérialisée et partagée (*cloud*) augmentent la surface d'attaque tout en l'étendant en dehors des frontières traditionnelles des organisations, par le truchement de l'externalisation. Concomitamment, ce sont les contraintes réglementaires et la judiciarisation croissante qui ont amené le marché américain de l'assurance cyber à prendre son essor avant le reste du monde. En effet, dès octobre 2011, la *Securities and Exchange Commission* (SEC) a imposé aux sociétés faisant appel à l'épargne publique de signaler sans délai les incidents de cybersécurité. Et de plus en plus, les législateurs, notamment européens, ainsi que les régulateurs du marché de l'assurance, incitent les opérateurs à se doter de mécanismes de cybersécurité robustes, ce qui les conduit à considérer l'assurance comme un levier essentiel parmi un ensemble de moyens de gérer ce risque : ainsi la directive européenne *Network and Information Security* de juillet 2016 (NIS, 2016/1148) engage les États membres à identifier les secteurs les plus critiques au fonctionnement de la Nation et à promouvoir la mise en œuvre de pratiques renforcées de cybersécurité chez les industriels désignés. D'autres règles ne sont peut-être pas étrangères à l'accélération de la demande de contrats d'assurance cyber : les nouvelles règles de protection des données personnelles (Personal Identifiable Information, PII) comme la norme PCI-DSS [(2)] et le RGPD [(3)], ont non seulement poussé les sociétés à investir pour se protéger et pour être en mesure de mener à bien leurs obligations déclaratives auprès des autorités, mais elles contribueront sans doute à les inciter à se couvrir avec des garanties assurancielles de plus en plus solides. Mais la nature internationale du risque cyber s'oppose à la logique réglementaire calquée sur des zones d'intervention géographiquement contenues. La nature des garanties elles-mêmes peut varier d'un pays à l'autre au gré de l'évolution de la maturité des marchés domestiques [(4)] ou en fonction des événements qui surviennent : la garantie « rançon », jusqu'alors peu mentionnée, s'est développée à la suite des deux grandes attaques par virus de 2017, *WannaCry* et *NotPetya*. Si la manifestation du risque cyber peut sembler évidente lorsqu'un assuré est sujet à une cyber-attaque soudaine et mondialement référencée (de type *Wannacry*), elle est plus délicate à circonscrire lorsque l'attaque est sournoise (logiciel malveillant), progressive dans le temps et que les connexions avec les dommages subis par l'entreprise sont difficiles à mettre en évidence. Cette difficulté est accentuée par la nature des garanties d'assurance mises en jeu, alors que la sinistralité passée, qui permettrait de s'appuyer sur un référentiel, est aujourd'hui rare voire absente, d'autant plus que le client lui-même n'est peut-être pas prêt à communiquer, par exemple, ses failles dans ses systèmes informatiques ou l'éventuelle demande de rançon dont il a été victime.

(2) *Payment Card Industry Data Security Standard*.
(3) Règlement Général sur la Protection des Données, entré en vigueur en mai 2018.
(4) N'oublions pas qu'entre les États-Unis, la France ou l'Espagne, le marché d'assurance évolue de 1 à 10.

Force est de constater que si les attaques cyber sont de plus en plus fréquentes et qu'il ne se passe pas une semaine sans qu'une entreprise ne fasse les frais de cette sophistication croissante de la menace, il n'y a pas encore eu à ce jour de « cyber ouragan » à grande échelle [5], au sens où plusieurs institutions ou organisations de plusieurs pays seraient massivement touchées, simultanément, par une ou plusieurs attaques, répondant à une même volonté. Dans un rapport de novembre 2018, l'Institut Montaigne a développé deux scénarios de cyber ouragan où, s'appuyant sur une quantification réalisée par les Lloyd's of London, les pertes mondiales coûteraient entre 4,6 milliards et 53,1 milliards de dollars (données 2017). On voit que ces scénarios sont très volatils et passent d'un extrême à un autre : l'incertitude domine encore. Dans ce contexte, c'est tout un marché qui se cherche, dans lequel l'assureur, par sa capacité à analyser les données existantes, à modéliser le risque à venir et à supporter le sinistre le cas échéant, est indéniablement un acteur-clé sur lequel s'appuyer.

Pour un assureur, l'évaluation du risque cyber passe en priorité par la connaissance de son exposition à ce risque ; sa capacité à associer pour chacune des garanties qu'il délivre l'engagement contractuel en montant est essentielle à l'appréhension du risque d'assurance cyber. En outre, comme pour tout produit d'assurance, c'est sur cet engagement que la prime d'assurance pourra être évaluée. L'assureur se doit donc d'être en mesure de connaître ce montant par garantie, par police d'assurance, par portefeuille d'assurance, par pays et monde entier. Cette mesure de l'exposition se fait spécifiquement par garantie dans le cadre des couvertures affirmatives. Elle se fait *via* le suivi des expositions aux garanties dommages aux biens et responsabilité civile traditionnelles dans les couvertures silencieuses. Enfin, comme le risque cyber est en évolution constante, la collecte de l'exposition doit être régulièrement mise à jour tant dans les montants alloués que dans la nature des garanties offertes. La sinistralité passée est l'autre élément à suivre en priorité. À partir d'un historique de sinistres qui s'enrichit au fil des ans à mesure que les garanties cyber s'étoffent et que le marché se développe, la vision du risque cyber est progressivement affinée. Toutefois, comme précédemment évoqué, la distribution des événements cyber tend vers une distribution « Dirac » :



Or, la prime d'assurance résulte avant tout de la moyenne théorique attendue de tous les sinistres qui peuvent potentiellement survenir. S'il y a peu d'expérience de sinistres connus, ce qui est le cas pour l'assurance cyber, la moyenne historique des sinistres apporte une contribution partielle à la

(5) Lire à ce sujet le rapport de novembre 2018 de l'Institut Montaigne « Cybermenace : avis de tempête, treize propositions pour augmenter la cyber-résilience de l'ensemble du tissu économique et de notre société » (2018) (https://www.institutmontaigne.org/publications/cybermenace-avis-de-tempete).

tarification. Et dans une courbe telle que ci-dessus, on comprend bien que l'événement extrême contribuera fortement à la moyenne théorique, et ce, beaucoup plus que pour des produits d'assurance traditionnels.

Par ailleurs, l'assureur doit être en mesure de mobiliser le capital suffisant pour absorber le coût de cet événement extrême, capital dont la rémunération est également à répercuter dans la prime d'assurance. On estime théoriquement que la rémunération du capital pour couvrir le risque cyber représente plus du tiers de la prime d'assurance alors qu'elle en représente en général moins de 10 % pour une branche d'assurances dommages. L'événement extrême, par son double impact dans la prime d'assurance, *via* sa contribution dans la moyenne théorique et *via* son impact direct dans la rémunération du capital, devient l'élément majeur de la fixation de la prime d'assurance. Négliger l'évaluation de l'événement extrême revient à sous-estimer de façon certaine la prime d'assurance associée au risque d'assurance cyber. Cela rappelle aussi l'importance du marché de la réassurance (l'assurance des assureurs) qui permet aux compagnies d'assurance de réduire le coût de cet événement extrême, soit en plafonnant son montant *via* des couvertures de sinistres appelées « en excédent de sinistres », soit en le partageant *via* des couvertures de réassurance en quote-part. D'autres couvertures, de type *Catbond*, peuvent également contribuer à réduire le risque d'assurance cyber. Dans ces montages, c'est le marché financier qui supporte le risque extrême s'il se déclare selon des conditions prédéterminées (un indice marché, un montant…) en échange d'une rémunération de type obligataire.

Une demande d'assurance en fort développement

Les entreprises qui souscrivent aujourd'hui des polices d'assurance cyber sont principalement les services financiers, les éditeurs de logiciels ou de solutions techniques, mais aussi l'hôtellerie et le commerce de détail, ainsi que les opérateurs de santé : tous cherchent à se prémunir contre les pertes d'exploitation qui résulteraient d'attaques cyber, et à se protéger contre les surcoûts engendrés par les conséquences de ces attaques, tant en conseil en communication de crise qu'en gestion du retour à la normale. Aux États-Unis ou au Royaume-Uni, une entreprise sur deux déclare ainsi avoir souscrit une assurance cyber. Si elles contribuent utilement à couvrir les risques des entreprises qui souscrivent leurs contrats, les compagnies d'assurance sont aussi prudentes, rappelle AM Best [6] dans une étude de juin 2019 : elles veillent à ce que leur exposition à ce risque ne dépasse ni leur appétit au risque, ni leur capacité financière. Même si le marché mondial de cyberassurance est estimé [7] à environ 5,3 milliards de dollars en 2018, il n'existe pas encore de chiffre agrégé de l'activité d'assurance cyber monde entier, soit du fait de la variété des régulateurs (EIOPA en Europe, NAIC aux États-Unis, OSFI au Canada, etc.), soit parce que tous les opérateurs et notamment les captives d'assurance ne sont pas tenus à des obligations similaires de reporting. Mais on observe un fort développement de la souscription de polices d'assurance et dans un marché qui croît d'environ 30 % par an, les analystes [8] estiment que le marché de cyberassurance pourrait encore doubler d'ici à 2020, et passer progressivement à environ 20 milliards de dollars d'ici à 2025. Le marché américain est le plus mature et le plus ancien : il a commencé à se développer dès le début des années 2000, et en 2017 il représentait 3,1 milliards de dollars de primes d'assurances [9] ; tandis qu'en France, le marché de la cyberassurance est relativement nouveau : il représente environ 80 millions d'euros à la fin 2018.

(6) https://www.insurancejournal.com/news/national/2019/06/18/529747.htm
(7) Etude PwC, *Insurance 2020 & beyond Reaping the dividends of cyber resilience* (2015).
(8) Etudes réalisées par PwC en 2015 (*Insurance 2020 & beyond Reaping the dividends of cyber resilience*) ou Munich Re en 2018 (*Cyber insurance market outlook*).
(9) Rapport, *National Association of Insurance Commissioners* (août 2018).

Le risque cyber pour l'assureur AXA : servir ses clients tout en se protégeant

Le risque cyber majeur auquel AXA peut être exposé n'est pas de même nature entre risque d'assurance et risque opérationnel. En effet, le hacker, source du risque majeur, a deux façons d'intervenir : soit il cherche à occasionner massivement des dégâts et à affecter le plus grand nombre (premier cas) ; soit il vise spécifiquement une entreprise, dont il aura étudié au préalable les failles technologiques, qu'il cherchera ensuite à affecter le plus sévèrement possible (second cas). À titre d'exemple, le rançongiciel *WannaCry* a utilisé en mai 2017 une faille de sécurité Windows, qui avait fait l'objet d'un correctif livré deux mois avant par l'éditeur [(10)] mais que de nombreuses compagnies n'avaient pas encore installé. Le virus a donc infecté un grand nombre d'ordinateurs parmi cette population vulnérable, générant de nombreuses pertes, mais sans cible particulière. À l'inverse, lorsque, en décembre 2013, un hacker attaque Target, la troisième enseigne américaine de supermarchés, c'est précisément cette société qui est visée avec peu d'impacts collatéraux sur d'autres assurés. Dans un scénario extrême, le risque d'assurance est maximal dans le premier cas car le montant assuré dépend du nombre de victimes, inconnu *a priori,* alors que dans le second cas, le sinistre ne peut pas dépasser la garantie contractuelle donnée à l'assuré visé. À l'inverse, le risque opérationnel sera maximal si AXA est ciblé par l'attaque d'un hacker (second cas), alors que les répercussions du premier cas resteront limitées car les protections demandées demeurent « standard », et bien moindres que celles exigées dans le deuxième cas.

Afin de suivre le risque assurance, AXA a donc développé un modèle dédié au cyber qui s'appuie sur plusieurs étapes. La première étape consiste à identifier et collecter les expositions d'assurance au risque cyber par police d'assurance au sein du groupe (nature des garanties et montants de couverture). Dans la deuxième étape, des scénarios existants ou potentiels sont modélisés « physiquement » de façon à appréhender notamment les enjeux maximums auxquels AXA est exposé. Enfin, la troisième étape aboutit à transposer statistiquement la vision par scénario de la deuxième étape et à permettre ainsi d'attribuer à des périodes de retour d'événements les coûts d'assurance induits. Chaque année, cette approche est affinée au gré des événements cyber nouvellement survenus, de l'expérience sinistres afférente, des améliorations internes de collecte de données et de modélisation.

On comprend bien que la seconde étape, la modélisation de scénarios, est primordiale pour mesurer à quel risque extrême s'expose AXA. Elle repose sur trois actions principales :

- La constitution et la mise à jour de la bibliothèque de scénarios : quels scénarios considère-t-on comme critiques pour AXA étant donné sa typologie de risques (catégories de clients, nature des garanties, montants de garanties alloués, etc.) ? À quels scénarios de marché se réfère-t-on ?
- Le développement du modèle « physique » : à l'image d'un processus industriel, en fonction du scénario retenu, AXA établit ses hypothèses de modélisation théorique : comment se propage l'événement cyber ? Qui est touché ? Quelle est l'ampleur de la destruction, qui dépend entre autres de la nature des clients affectés ? La réponse à ces questions et leur modélisation permettent d'estimer le coût maximal théorique auquel AXA pourrait être exposé.
- La confrontation des résultats à des experts – qu'ils proviennent du groupe AXA ou qu'ils soient issus du monde académique – ou la comparaison avec d'autres modèles développés sur le marché.

Dans ce contexte, les compétences demandées pour appréhender le risque assurance sont à la fois la connaissance assurancielle (connaissance de la mécanique d'assurance cyber et de la nature

(10) Bulletin de sécurité MS-17-010.

des garanties), la compréhension de la nature du risque (un événement affectant l'informatique dématérialisée et partagée (*cloud*) ou de type rançongiciel (*ransomware*) n'impacte pas le marché de la même manière), et la compétence actuarielle (collecte de données et approche stochastique). AXA développe en interne cette connaissance qui est enrichie par des recherches académiques, notamment *via* une Initiative de Recherche conjointe avec l'École nationale de la Statistique et de l'Administration économique (ENSAE) et Sorbonne Université. Par ailleurs, le fonds AXA pour la Recherche, en finançant des chaires dans ces domaines, contribue également à cet enjeu associant recherche interne et recherche académique.

Considéré maintenant en tant que risque opérationnel pour l'assureur lui-même, le cyber requiert à la fois une compétence affûtée en gestion des risques ainsi qu'une vaste connaissance des systèmes informatiques. La société d'assurance va modéliser des scénarios reposant sur différentes histoires vraisemblables où tout ou partie des systèmes d'information sont l'objet d'attaque, d'indisponibilité ou encore de corruption de données. Ces « histoires » sont analysées, disséquées, et associées à des unités de valeur (coût de personnel, coût de remédiation, perte d'exploitation, etc.) : elles permettent d'évaluer le coût réaliste d'un tel scénario. Les données proviennent de l'entreprise elle-même (parc de machine, configuration, etc.) ainsi que de son expérience réelle des incidents récents et, dans certains cas, de données provenant de sachants extérieurs à l'entreprise : cabinets de conseil, entreprises du marché ou encore associations professionnelles. Chez AXA, de tels scénarios sont réalisés annuellement et collectés à travers toutes les entités qui constituent le groupe : la somme de ces scénarios, ou leur corrélation, permet de calculer une charge en capital requise dans le cadre de Solvabilité II. Au-delà de l'obligation réglementaire, ces travaux permettent une quantification des impacts possibles d'événements majeurs et facilitent donc les discussions et la hiérarchisation des priorités quant aux moyens d'en empêcher la survenance ou d'en ralentir les effets. Cette quantification des risques cyber ne se fait pas en silo mais participe d'une organisation globale en lignes de défense complémentaires : si les opérationnels sont les premiers acteurs de la gestion de leurs risques, eux-mêmes appuyés par des experts de première ligne qui répondent à une stratégie décidée et suivie globalement par la direction de la sécurité du groupe, notamment en matière de cyberdéfense, des fonctions de seconde ligne sont positionnées dans chaque entité au sein du *risk management*. Celles-ci aident à anticiper les risques de l'information, en procédant à la modélisation des risques, mais aussi en questionnant les décisions à prendre, lors de comités stratégiques, afin d'obtenir la mise en œuvre d'un environnement de contrôle fiable ; ces experts du risque aident aussi à orienter l'allocation de moyens sur les bonnes priorités, et enfin organisent la restitution de ces sujets au comité des risques. Une gouvernance décisionnaire de haut niveau, le *Group Information Risk Board*, permet d'ailleurs d'engager le groupe dans des mesures préventives ou curatives, elles-mêmes régulièrement auditées dans un évident souci d'amélioration continue.

En conclusion

De façon générale, l'assurance d'un risque naît de sinistres qui génèrent des pertes économiques importantes et qui soulignent le besoin d'une protection d'assurance afin de permettre le maintien de l'activité professionnelle en toute circonstance assurée (client entreprise) ou de préserver le patrimoine privé (client particulier). L'assureur appuie alors son estimation du risque sur la base des pertes antérieures. De son côté, le risque opérationnel, au sens de la directive Solvabilité II de 2009, a un périmètre restreint à une entreprise et, à ce titre, la gestion du risque opérationnel s'intéresse à anticiper les risques extrêmes auxquels l'entreprise pourrait faire face, en s'appuyant à la marge seulement sur les événements du passé. Ces deux approches ne s'appliquent pas aussi facilement au risque cyber. Le risque cyber est nouveau en assurance et personne ne sait quantifier les pertes antérieures, nul ne saisit pleinement le risque d'autant plus qu'il évolue sans cesse – l'une des problématiques actuelles est par exemple l'imputabilité d'un acte de guerre réalisé au travers

d'un piratage informatique – mais tout le monde sait que le risque cyber est potentiellement majeur et justifie une protection d'assurance. Incité par les assurés demandeurs de protection, l'assureur doit prendre un risque qu'il ne connaît pas et dont il n'a pas pu mesurer les conséquences passées.

Le risque cyber est dorénavant inhérent à toute activité, qu'elle soit entrepreneuriale ou individuelle. L'assureur se doit donc d'accompagner son client dans son activité en lui apportant conseils en prévention et solutions de protection appropriées à ses besoins. Mais l'enjeu est aussi de permettre que l'assureur soit toujours en capacité de servir ses clients : qu'en temps ordinaire, il protège les données qui lui ont confiées et qu'en cas de sinistre, il assiste ses assurés. En effet, en cas de catastrophe naturelle, chacun s'attend légitimement à ce que son assureur soit debout ; il en va de même pour les événements cyber, où l'assureur doit pouvoir résister à un cyber ouragan : il lui faut donc anticiper le risque cyber en étant toujours à la pointe de la protection et en restant en permanence en veille. La menace cyber est ainsi faite : pour être en mesure de proposer à ses clients les garanties qu'ils demandent, un assureur doit viser un très haut niveau de protection opérationnelle. C'est un défi nouveau mais stimulant !

Défis de la recherche scientifique en cybersécurité

Par **Claude KIRCHNER** et **Ludovic MÉ**
Inria

Sécuriser un système d'information, c'est assurer la confidentialité, l'intégrité et la disponibilité des ressources qui y sont stockées et des services qui y sont offerts. À cette fin, on doit à la fois protéger ces ressources et services, mais aussi détecter d'éventuelles attaques et y réagir efficacement. Si la sécurité des systèmes et la protection des données personnelles ont globalement progressé durant ces vingt dernières années, beaucoup reste à faire, tant dans la mise en œuvre opérationnelle que dans les phases amont de recherche et développement. Dans cet article, nous nous intéressons aux défis de recherche scientifique que lancent la protection de nos systèmes d'information, la détection des attaques contre ces systèmes et la réaction à ces attaques, sans oublier les défis liés à la connaissance de la menace, à la sécurité de certains domaines particulièrement sensibles, ou aux aspects humains, économiques et sociétaux de la sécurité.

Le numérique et la sécurité

La numérisation générale de nos sociétés nous porte vers une cyber-civilisation globale dont la cybersécurité est un enjeu majeur de viabilité. Cette transformation fondamentale est portée par les avancées scientifiques, technologiques et les innovations et usages qui en résultent, en particulier mais pas seulement dans le domaine du numérique. Paradoxalement, cette situation, inédite à cette échelle, pose à son tour de nouvelles questions scientifiques dans les domaines traditionnels du numérique que sont les sciences informatique, mathématique, électronique, robotique, etc. Compte tenu de ses conséquences profondes sur l'humain et ses environnements sociaux et environnementaux, cette situation interroge aussi les sciences du droit et de l'économie, les sciences humaines et sociales et les sciences de l'environnement qui sont également mises au défi de nous aider à comprendre, maîtriser et assumer les évolutions en cours.

Pour mieux analyser les défis de la recherche en cybersécurité, examinons premièrement les principales raisons de l'impact du numérique depuis le début du siècle dernier.

Le premier point, crucial, est l'émergence scientifique du concept d'information comme un concept fondamental au même titre que la matière, l'énergie et le vivant : *"Information is information, not matter or energy. No materialism which does not admit this can survive at the present day"*(1). Cette identification de l'information en tant que concept fondamental nous permet de comprendre pourquoi la révolution numérique a tant d'impact sur nous. En effet nous sommes des systèmes de traitement biologique de l'information (et nous ne sommes pas que cela bien sûr) et, en tant que tels, nous interagissons avec les systèmes de traitement numérique de l'information que nous avons créés. Ces interactions, d'élémentaires il y a quelques dizaines d'années, sont devenues telles que ces systèmes de traitement d'information biologiques et numériques se complémentent, collaborent et maintenant se combinent avec des conséquences profondes pour l'Humain et ses organisations. La cybersécurité ne peut pas être considérée seulement comme traitant de la

(1) WIENER N. (1948), *Cybernetics: or control and communication in the animal and the machine*, 2nd revised version in 1961. The MIT Press, Cambridge, MA.

sécurité des systèmes numériques, elle doit prendre en compte l'ensemble des éléments entrant en jeu. Nous devons en effet mieux comprendre l'impact des réseaux sociaux, les mécanismes de désinformation, mais aussi appréhender les défenses comme les attaques sur l'ensemble des systèmes d'information. Ces attaques peuvent cibler le système de traitement numérique lui-même (on parlera alors de cyber-attaques) ; elles peuvent aussi utiliser une cyber-attaque pour affecter le traitement d'information biologique humain (comme dans le cas de Cambridge Analytica).

Le deuxième point réside dans l'ampleur du déploiement des systèmes numériques. Il n'est plus de système ou d'organisation qui ne soit peu ou prou informatisé **:** processus industriels, financiers, économiques, de transport ; systèmes de santé ; systèmes de production-transport-consommation d'énergie ; villes et leurs immeubles et habitats ; véhicules automatisés ; système de développement scientifique et technologique lui-même, etc. La numérisation globale de tout notre environnement induit une complexité jamais atteinte à toutes les échelles **:** personnelle, locale, nationale, continentale, globale. La défense de cet ensemble de systèmes de traitement d'information est d'une complexité ainsi jamais atteinte **: i**l n'est pas étonnant que sa maîtrise soit particulièrement difficile.

Le troisième et dernier point que nous voulons souligner ici c'est la rapidité du déploiement et des évolutions des systèmes informatisés. Le rythme de l'avancement des connaissances et des innovations qui peuvent en être issues n'a jamais été aussi rapide de toute l'histoire de l'humanité. Cette rapidité nécessite de mettre en œuvre des stratégies agiles et bien informées pour permettre une défense adaptée et jamais définitive.

Dans ce contexte complexe, intime vis-à-vis de l'humain, totalement pervasif et en évolution rapide et profonde, la cybersécurité a un rôle fondamental permettant d'établir la confiance. Le respect de la vie privée, la confiance dans nos institutions et nos modes d'organisation personnels, familiaux, collectifs, professionnels en dépendent fondamentalement. Quels sont les défis majeurs à relever dans les cinq à dix ans pour qu'en 2030 (demain !) nous puissions encore, et si possible mieux, fonder nos souverainetés numériques personnelles et collectives ?

Des menaces aux défis de recherche

La démarche de sécurisation consiste à d'abord identifier les menaces puis à concevoir des mécanismes de protection et de détection pour les contrer. Un mécanisme essentiel est la cryptographie. Cependant, bien que les primitives et les protocoles cryptographiques soient des éléments fondamentaux de la sécurité, des services de sécurité supplémentaires sont nécessaires, tels que l'authentification et le contrôle d'accès. Ces services de sécurité, généralement fournis par le système d'exploitation ou les périphériques réseau, peuvent eux-mêmes être attaqués et parfois contournés. Par conséquent, les activités entreprises sur le système d'information doivent être supervisées afin de détecter toute violation de la politique de sécurité. Enfin, comme les attaques peuvent se propager extrêmement rapidement, les systèmes de protection doivent réagir automatiquement ou au moins se reconfigurer pour éviter de propager les attaques. Tous ces mécanismes de sécurité doivent être soigneusement intégrés dans les applications critiques pour la sécurité. Ces applications doivent prendre en compte tous les systèmes de traitement et de communication d'information, qu'ils soient humains ou numériques. Outre l'humain dans toutes ses capacités, ils comprennent les systèmes informatiques traditionnels, mais aussi les systèmes industriels et les nouvelles infrastructures distribuées dont en particulier l'informatique en nuage (*Cloud)* et l'Internet des Objets (IoT) dans des déploiements dont la taille va bientôt dépasser le millier de milliards d'objets (tera-objets).

Chaque étape de l'amélioration de la sécurité pose des défis spécifiques. Dans cet article, nous nous intéressons aux défis scientifiques auxquels fait face le monde de la recherche pour chacune de ces étapes, sans prétendre à l'exhaustivité. Les défis que nous présentons ici reprennent en partie des éléments du Livre blanc Inria sur la sécurité numérique [(2)].

Connaître la menace

Rechercher et analyser systématiquement les vulnérabilités

La compromission de la cybersécurité est avérée et malheureusement bien plus profonde que ne le laisse apparaître le sommet de l'iceberg que représentent les attaques détectées. Elle peut avoir des conséquences dramatiques pouvant aller jusqu'à des impacts létaux massifs (qui n'ont pas encore été observés, mais dont on sait qu'ils sont possibles) et des destructions irréversibles à court (cinq ans) ou moyen terme (vingt ans) sur les ouvrages humains et plus globalement l'environnement. Les attaques sont de plus en plus sophistiquées en conception, en moyens déployés pour leur exécution et en capacité destructive.

Connaître son ennemi est un défi toujours aussi important. Une implication plus massive du monde académique des sciences dures comme des sciences humaines et sociales, dans tous les éléments de compréhension et de conception d'attaques existantes ou nouvelles, est souhaitable. L'étude géostratégique des conditions de la cybersécurité présente et à venir (dans les vingt prochaines années) pourra éclairer les décisions politiques à prendre. Cette implication renforcée doit permettre le développement de sciences expérimentales dans le domaine de la cybersécurité, appliquant des méthodologies scientifiques appropriées (éthique, reproductibilité, partage). Quelques laboratoires académiques en haute sécurité informatique existent de manière similaire aux laboratoires P3 et P4 en biologie. Les renforcer sera déterminant pour notre capacité en cybersécurité à observer, mesurer, attribuer, auditer, certifier et contribuer le cas échéant à la standardisation ou la normalisation.

Attaquer le matériel à partir de logiciels

Une catégorie d'attaques relativement nouvelles et évoluées se développe. Elle consiste à exploiter ou produire des vulnérabilités dans les éléments matériels des systèmes de traitement d'information, en commençant par les processeurs. Ces attaques se basent typiquement sur les propriétés physiques de la matière et exploitent l'utilisation dans les processeurs modernes de mécanismes d'optimisation pour gérer les caches, prédire les branchements ou exécuter du code en avance de phase afin de gagner du temps (exécution spéculative). Rowhammer et Spectre en sont des exemples récents. Rowhammer exploite les interactions électriques entre des cellules voisines pour inverser des bits de la mémoire pendant la lecture ou l'écriture d'une autre cellule. Spectre exploite la prédiction de branchement et l'exécution spéculative pour exfiltrer des informations au travers d'un canal caché basé sur l'accès au cache. Ces attaques sont particulièrement dangereuses puisqu'elles permettent d'atteindre les matériels à distance.

Ces attaques reposent sur une cause commune : l'abstraction. Typiquement, quand on propose un mécanisme de sécurité à un niveau donné d'abstraction, on a tendance à considérer que les niveaux inférieurs sur lesquels on s'appuie sont corrects et sûrs, ce qui n'est évidemment pas toujours le cas. Les attaques portent ainsi de plus en plus sur des niveaux d'abstraction de plus en plus proches des aspects physiques, allant des applications vers l'OS, le noyau, le *firmware* et maintenant le matériel.

(2) Coordonné par S. Kremer, L. Mé, D. Rémy et S. Roca, ce Livre blanc, publié en janvier 2019, dresse un tableau global de la sécurité numérique, identifie des défis scientifiques et présente les contributions des équipes-projets Inria : https://files.inria.fr/dircom/extranet/LB_cybersecurity_WEB.pdf

La prévention de ce type d'attaque est particulièrement coûteuse puisqu'elle passe par exemple par la limitation de la réduction de la surface des composants ou le rafraîchissement périodique des cellules par des opérations de lecture ou d'écriture. La détection de ces attaques est elle-même difficile du fait de l'absence de trace disponible au niveau de l'OS ou des applications.

Les défis sont donc ici particulièrement difficiles et aujourd'hui largement ouverts. Ils consistent à élaborer une typologie claire de ces attaques, à obtenir une meilleure compréhension de leur *modus operandi*, et à concevoir des contremesures implantées au niveau logiciel ou au niveau des composants matériels. Ce travail se fera dans un contexte difficile qui peut demander de revisiter des optimisations cruciales et utilisées depuis longtemps telles que l'exécution spéculative.

Protéger

Renforcer continûment la confiance dans le chiffrement

La confiance dans le chiffrement est centrale. Elle repose bien entendu sur la maîtrise des primitives cryptographiques, mais aussi très largement sur la crypanalyse. Pendant de la cryptographie (science de la conception des primitives cryptographiques), la crypanalyse est la science de l'attaque de ces primitives. C'est par une recherche duale en conception et en attaque, s'enrichissant l'une l'autre, que la confiance peut se renforcer.

Le défi est ici d'une part d'organiser la recherche de nouvelles attaques sur les algorithmes de chiffrement, conduites avec des moyens de calcul classiques ou quantiques, en se basant en particulier sur des mesures physiques corrélées aux secrets manipulés algorithmiquement ; d'autre part d'établir formellement des propriétés de robustesse des algorithmes et de leur implantation.

Prouver les protocoles cryptographiques

Les protocoles cryptographiques permettent, par échanges d'informations chiffrées, d'établir des propriétés de sécurité, comme par exemple l'authenticité de l'identité déclarée d'une entité agissant sur le réseau. La sécurité de ces protocoles, qui sont utilisés par exemple pour valider les transactions bancaires effectuées depuis un téléphone portable, est particulièrement délicate. Ces preuves sont en effet longues et complexes, faisant intervenir des interactions multiples entre différents cas. Les preuves réalisées « à la main », même par des informaticiens ou des mathématiciens confirmés, peuvent ainsi contenir des erreurs. La formalisation des protocoles et des propriétés à prouver, associée à l'automatisation des preuves, est la seule manière de parvenir à des preuves sans erreur et donc à un haut degré de sécurité.

Le défi est ici à composantes multiples. La première consiste à spécifier formellement les protocoles au niveau d'abstraction approprié. Ceci nécessite de modéliser l'environnement dans lequel s'exécute le protocole et le niveau d'abstraction, par exemple au niveau langage machine ou au niveau symbolique. Par ailleurs, il faut aussi modéliser les capacités de l'attaquant, son influence sur l'environnement dans lequel le protocole s'exécute, ses connivences éventuelles avec d'autres entités malveillantes. Ce travail permet de détecter et de corriger des erreurs de conception dans les protocoles et éventuellement dans leurs implémentations. Il apparaît aujourd'hui particulièrement important de le conduire dans le contexte de la 5G.

Calculer sur les données chiffrées

L'utilisation pervasive de l'informatique en nuage amène en particulier à considérer l'utilisation du chiffrement homomorphe. Ce dernier permet, par exemple pour l'opération d'addition, de rendre compatible cette opération avec une fonction de chiffrement au sens où la somme des chiffrés est exactement le chiffré de la somme des opérantes. Le chiffrement homomorphe permet donc de travailler directement sur les données chiffrées et d'éviter d'avoir à transmettre ou à

mettre à disposition sur le *cloud* des données non chiffrées. Toute la confiance réside donc dans la qualité de l'algorithme de chiffrement.

La difficulté principale dans ce contexte est de mettre au point des primitives de chiffrement homomorphes qui soient aussi universelles que possible au sens où elles sont homomorphes pour toutes les opérations utiles ou imaginables : on parle alors de chiffrement homomorphe universel ou complet. On sait aujourd'hui construire de telles primitives, mais elles sont de performances (en temps et en espace) faibles si bien qu'il n'est pas réaliste de les utiliser sur les machines et réseaux actuels.

Le défi majeur ici, difficile mais crucial pour renforcer la confiance dans l'utilisation des *clouds*, est de découvrir des primitives cryptographiques homomorphes fiables et efficaces en temps et en espace pour de larges classes d'opérations, si ce n'est universelles.

Chiffrer à l'heure de l'ordinateur quantique

Le passage du modèle de calcul classique de von Neumann à celui du calcul quantique peut changer la complexité de l'exécution d'un programme implantant dans chacun de ces deux modèles une fonction donnée. Les algorithmes tels que RSA, dont la complexité est exponentielle lorsqu'il s'exécute sur un modèle de calcul classique, sont de complexité polynomiale sur une architecture quantique. Dès que des machines quantiques disposant de suffisamment de qubits seront disponibles, RSA ne sera définitivement plus utilisable et les secrets mémorisés aujourd'hui avec RSA deviendront facilement lisibles.

De nouvelles primitives cryptographiques, dites post-quantiques, d'une complexité suffisante pour les deux modèles de calcul, ont été découvertes. Elles reposent sur différentes difficultés mathématiques, comme trouver un vecteur de faible dimension dans un réseau euclidien, ou encore décoder un code linéaire arbitraire.

Le défi est ici aussi particulièrement clair et important. Il consiste à trouver, à analyser et à faire les preuves de complexité pour ces nouvelles primitives cryptographiques. Il faudra aussi gérer en amont le fait que dans les vingt prochaines années (2040 dans le meilleur des cas), la plupart des primitives cryptographiques actuelles devraient ne plus être utilisables, si bien que toutes les informations chiffrées par ces moyens et actuellement conservées deviendront alors vulnérables.

Notons aussi qu'indépendamment du modèle de calcul quantique, l'utilisation de canaux de communication quantiques permet la communication de secrets dont la sûreté repose sur les propriétés quantiques de la matière, ce qu'on considère actuellement comme inviolable. Le défi est ici différent, la capacité à mettre en œuvre de tels protocoles de communication « parfaitement sûrs » étant aujourd'hui opérationnelle sur des distances de moins de 100 km, par exemple entre certaines banques suisses. Le défi, en particulier pour les physiciens, consiste à passer sur des distances plus importantes, par exemple pour communiquer entre le sol et les satellites ou entre sites terrestres éloignés de plusieurs milliers de kilomètres.

Formaliser et prouver pour sécuriser sûrement les systèmes

Actuellement, la sécurité des systèmes d'information repose principalement sur des approches d'ingénierie classiques, non formelles. Cette approche a bien entendu fait ses preuves, mais elle montre aussi des limites, comme les nombreuses attaques rendues publiques le prouvent. Les méthodes formelles apparaissent donc clés pour la mise en œuvre du concept de « sécurité à la conception ». Il s'agit de s'assurer par construction et de prouver de manière formelle et automatisée que telle ou telle propriété de sécurité (par exemple le fait que l'information contenue dans tel ou tel fichier ne puisse être lue que par tel ou tel utilisateur) est garantie par le système et les mécanismes de sécurité qui y sont déployés. Le système contient bien entendu à la fois des

dispositifs de traitement et de transport de l'information. On note d'ailleurs que ces dispositifs tendent à se confondre de par la virtualisation de plus en plus poussée des mécanismes réseau (*Software defined Network,* SDN).

Peut-être encore plus dans ce contexte que dans un autre, les défis sont ici importants et difficiles. Les méthodes formelles ont montré leur efficacité pour prouver la correction des protocoles cryptographiques, comme nous l'avons indiqué ci-dessus. Pour prouver le fonctionnement correct de logiciels (système d'exploitation complet, superviseur et hyperviseur, mécanisme réseau, etc.), il reste cependant encore beaucoup à faire. Un point résidera dans le passage à l'échelle, puisque des codes très volumineux et particulièrement complexes devront être validés. En outre, il faudra être capable de prouver toute la « pile » informatique, depuis les applications jusqu'au *hardware* (on l'a vu, les attaques ciblent de plus en plus les couches basses), en tenant compte aussi, bien entendu, des interactions entre les différentes couches. Les mécanismes de sécurité préventifs et réactifs (voir paragraphe suivant) devront eux-mêmes être prouvés. Pour ne donner qu'un exemple, on peut imaginer prouver qu'un système de détection d'intrusions assure la détection de telle ou telle classe d'attaque. Ce travail complexe aura un coût, qui reste à évaluer précisément, et à mettre en regard du coût de l'insécurité. Ce n'est qu'ainsi que les méthodes formelles pourront s'imposer, à moins que la régulation ne rende leur usage obligatoire, au service de la sécurité et de la protection des données, en particulier personnelles, comme cela est le cas pour la disponibilité de service dans les environnements critiques.

Détecter, diagnostiquer et endiguer les attaques

Détecter intrusions et anomalies

Comme expliqué précédemment, les activités réalisées sur un système d'information doivent être supervisées afin de détecter les atteintes à la sécurité de ce système. Deux approches sont actuellement utilisées : la détection de symptômes connus d'attaques connues (on parle alors de détection d'intrusions) et la détection de déviations d'usage des services informatiques offerts par le système, déviations qui pourraient être un marqueur d'attaques connues ou inconnues (on parle alors de détection d'anomalies). De tels mécanismes sont aujourd'hui largement déployés et utilisés, dans les antivirus, les IDS (*Intrusion Detection Systems*) ou les EDR (*Endpoint Detection and Response*). Cependant, l'efficacité de ces mécanismes reste souvent médiocre. D'une part, rien ne garantit que toutes les attaques seront détectées (risque de faux négatifs), d'autre part (et surtout), les retours d'expérience terrain montrent que des fausses alertes (faux positifs) sont émises, parfois tellement nombreuses qu'elles noient les vraies alertes qui deviennent alors difficiles à identifier par l'administrateur du système.

Actuellement, la détection d'intrusions s'appuie principalement sur l'analyse, paquet par paquet, du trafic réseau. Cette approche est insuffisante. En effet, chaque paquet pris indépendamment est trop pauvre en informations, ce qui limite l'efficacité de la détection, même si divers mécanismes d'agrégation d'informations ont été proposés. En outre la proportion de trafic chiffré augmente (les évaluations existantes laissent à penser que, déjà, de 50 à 80 % du trafic serait chiffré), ce qui rendra à terme obsolète une approche basée sur la recherche de *patterns* dans du trafic en clair. Dans ce contexte, deux défis sont à explorer : d'une part en s'appuyant sur les possibilités que pourrait offrir le calcul sur les données chiffrées (voir ci-dessus), envisager un traitement directement sur le trafic réseau chiffré. D'autre part en considérant que l'information n'est plus disponible sur le réseau, envisager d'autres sources d'information, par ailleurs plus riches sémantiquement, au niveau des applications ou des systèmes d'exploitation par exemple.

La détection d'anomalies est moins utilisée que la détection d'intrusions, même si divers mécanismes ont été proposés pour construire des modèles de référence du comportement du

système d'information. Les activités réalisées sur le système sont confrontées à la référence et une alerte est émise en cas de non-concordance. Il apparaît ici que les approches à succès de l'apprentissage statistique (*machine learning*) sont susceptibles de révolutionner ce domaine, comme elles ont pu révolutionner par exemple celui du traitement d'image. Cependant, l'application de ces techniques aux données à traiter en sécurité n'est pas triviale. Définir précisément ce qui peut être fait et ce qui est hors de portée est un défi en tant que tel. En outre, deux difficultés apparaissent : d'une part, les données qui permettraient de réaliser l'apprentissage sont rarement publiques ; d'autre part, nombre d'approches (*deep learning*, par exemple) souffrent d'un défaut considéré comme majeur en sécurité : on ne sait pas expliquer aujourd'hui les résultats qu'elles livrent. Ces deux difficultés devront être contournées. Une piste de recherche orthogonale serait d'éviter au contraire tout apprentissage : le modèle de référence serait alors fixé, par exemple *via* les spécifications des services offerts, ou *via* la spécification de la politique de sécurité. On analyserait alors la conformité des activités observées par rapport à ces spécifications.

Le test des mécanismes de détection, voire éventuellement leur certification, pose aussi des défis importants. Sur un plan très pratique, il n'existe pas aujourd'hui de plateforme de test librement accessible par les acteurs académiques pour tester leurs idées et les confronter à celles des autres. Une telle plateforme reste donc à construire, ce qui n'est pas simple. Sa disponibilité rendra les expérimentations reproductibles, alors qu'elles ne le sont généralement pas aujourd'hui (on dispose très rarement du code de détection et des données de test utilisées). Nous avons évoqué précédemment la possibilité de prouver les mécanismes réactifs, par usage des méthodes formelles. Les propriétés à certifier pourront par exemple être que telle classe d'attaque est détectable ou, plus généralement, que tel mécanisme est apte à détecter toute violation de telle politique de sécurité.

Par définition, analyser toutes les activités des utilisateurs est potentiellement attentatoire à leur vie privée. Un dernier défi de recherche en lien avec la détection est relatif à la conception de mécanismes de détection respectueux de la vie privée.

Diagnostiquer les violations de sécurité

Aujourd'hui, des *Security Operation Centers* (SOC) reçoivent des alertes (dont beaucoup de fausses, comme mentionné ci-dessus) que des opérateurs humains tentent de caractériser et d'enrichir. Ils utilisent pour ce faire la corrélation d'alertes, fonction importante des SIEM (*Security Information and Event Management*), qui permet par exemple de regrouper dans une même méta-alerte les informations disponibles sur une même attaque qui aurait été détectée par plusieurs outils de détection. Cette forme de corrélation (en fait de fusion d'informations) est utile mais n'offre pas une analyse fine de l'attaque avec reconstruction des étapes du scénario d'attaque et identification des objectifs réels de l'attaquant.

Pour parvenir à ce niveau d'analyse, il est important de prendre en compte, d'une part la nature même du système surveillé (les machines, leurs liens, les services offerts, les outils de sécurité en place et leur configuration, les vulnérabilités connues mais qui n'ont pas pu ou pas encore pu être corrigées, etc.), d'autre part des informations plus globales telles qu'un activisme observé dans telle ou telle partie du monde ou la recrudescence de telle ou telle forme d'attaque. Par ailleurs, le corrélateur doit aussi disposer de la description de scénarios d'attaques possibles, tels que donnés par exemple par une analyse de risque sous la forme d'un arbre d'attaque. Disposant de l'ensemble de ces informations, un défi de recherche important consiste à concevoir un mécanisme automatique de raisonnement sur le flux d'alerte, en mettant par exemple en œuvre des approches relevant de l'IA symbolique.

De manière complémentaire, il est important de conduire des travaux de recherche sur la visualisation de l'ensemble des informations relatives à la sécurité, dont les alertes, bien entendu. Ces informations sont de nature très diverses et sont fortement structurées, certaines étant beaucoup plus importantes

que d'autres. Il faut donc proposer à l'opérateur humain une image la plus pertinente possible de ce qui est en train de se passer sur le système. Il faut en outre lui permettre de naviguer efficacement dans ces données, qui sont extrêmement volumineuses. Au-delà du travail de visualisation, une recherche des bonnes formes d'interaction est donc aussi nécessaire.

Automatiser le déploiement des contre-mesures

Comme les attaques peuvent se propager extrêmement rapidement, les systèmes de protection doivent réagir automatiquement ou au moins se reconfigurer pour éviter la propagation des attaques. Les mécanismes existants aujourd'hui permettent par exemple la fermeture automatique d'un port sur un *firewall* (afin de bloquer une source d'attaque) ou encore la terminaison d'un processus système (là encore, pour stopper une attaque en cours *via* ce processus). Il n'y a pas d'évaluation de l'impact de la contre-mesure et, surtout, pas de raisonnement global sur la politique de sécurité et la manière dont il conviendrait de la modifier.

Si une attaque a réussi, c'est que la configuration des outils préventifs était incorrecte, auquel cas cette configuration doit être revue. Typiquement, la politique de sécurité elle-même était incorrecte ou incomplète, auquel cas cette politique doit être amendée et de nouvelles configurations des mécanismes de sécurité préventifs déployés. On a donc deux types de réactions possibles, l'un portant sur les configurations des mécanismes de sécurité, l'autre sur la politique et ces mêmes configurations. Le défi de recherche est ici d'être capable de diagnostiquer très rapidement l'incident en cours (voir paragraphe précédent), pour déclencher la réaction au plus vite. Un autre défi est de prouver, d'une part que les propriétés de sécurité que la police est censée garantir sont effectivement atteintes, tant au niveau de la politique qu'à celui de son implémentation, d'autre part que les modifications proposées ne perturbent pas les services offerts par le système. En outre, il serait bien entendu intéressant de pouvoir générer automatiquement l'implémentation de la politique (la configuration des outils de sécurité préventifs) à partir de son expression. Pour l'ensemble de ces travaux, les méthodes formelles apparaissent comme l'outil indispensable à la construction de systèmes capables de se défendre eux-mêmes et de s'adapter automatiquement à l'évolution des menaces, dans une forme d'*autonomic computing* que l'on préférera nommer ici « sécurité autonome ».

Notons pour conclure ce paragraphe que nous n'abordons pas ici une autre forme de réaction : la contre-attaque. Les enjeux éthiques, techniques et géopolitiques soulevés sont ici extrêmement délicats. En l'état actuel des connaissances et des capacités techniques, la contre-attaque automatique n'est absolument pas souhaitable et la présence d'humains « dans la boucle » indispensable.

Protéger les données personnelles et la vie privée

Mettre en œuvre le RGPD

Le Règlement général pour la Protection des Données (RGPD) est une avancée fondamentale européenne qui promeut des concepts et objectifs fondamentaux, en particulier pour le respect de la vie privée et la protection des données personnelles, incluant notamment les données de santé. Mais leur implémentation doit encore être développée très largement pour passer de l'énoncé de la régulation à sa mise en œuvre : trop de services et de dispositifs se comportent actuellement comme des boîtes noires, manquant ainsi l'objectif de transparence voulu par le Règlement. Par ailleurs les utilisateurs manquent d'informations et d'interfaces appropriées pour exprimer leur consentement ou leur opposition.

Les défis de recherche qui en résultent consistent premièrement à élaborer des outils d'analyse des risques de mise en cause du respect de la vie privée, et à élaborer des cadres formels permettant

de garantir la correction et l'auditabilité des solutions mises en œuvre. Ils consistent ensuite à concevoir les moyens permettant aux individus de maîtriser leurs données personnelles tout en permettant de gérer l'équilibre délicat entre utilisabilité, partage et respect de la vie privée. Cela implique en particulier de créer de nouveaux moyens, en particulier automatisés, pour exprimer les consentements ou refus et ce, de manière robuste et ergonomique.

Anonymiser les données personnelles

Le respect des données privées repose sur la gestion sécurisée de leur politique d'accès. Leur accès direct doit être préservé ; on retombe là sur les techniques de sécurisation par chiffrement ou par l'utilisation de politiques de sécurité appropriées. Cependant, ces données peuvent aussi être dévoilées indirectement, soit du fait de leur communication à des fins d'exploitation (on aura alors recours à des techniques d'anonymisation reposant typiquement sur la k-anonymisation ou sur la *differential privacy*), soit encore du fait de leur utilisation pour entraîner des algorithmes de reconnaissance basés sur l'apprentissage machine (les données d'entraînement peuvent être dévoilées, au moins partiellement, en ayant accès à l'algorithme de classification issu de l'entraînement initial ou continu).

On aboutit alors à des défis de recherche concernant la conception de techniques d'anonymisation robustes. Le sujet est difficile compte tenu de la diversité des données disponibles permettant des recoupements multiples. Par ailleurs, la distribution des données, évitant *a priori* le bénéfice pour les attaquants d'un accès centralisé, impose de trouver des stratégies de distribution minimisant le coût de l'accès aux données pour les algorithmes d'apprentissage ou d'exploitation.

Assurer la sécurité des contextes sensibles

Nous avons choisi d'illustrer ici l'importance de prendre en compte les spécificités de certains contextes applicatifs sensibles au travers des trois exemples de l'Internet des Objets, des systèmes industriels et des systèmes à base d'intelligence artificielle. Il va cependant de soi que d'autres contextes sensibles sont aussi à considérer, comme celui de la santé ou celui, transverse, de la robotique.

Sécuriser l'Internet des Objets (IoT)

Les attaques contre les dispositifs relevant de l'IoT (les objets connectés) sont relativement faciles, essentiellement car la sécurité n'est généralement pas prise en compte dès la conception de ces objets et des fonctionnalités qu'ils offrent. En outre, le nombre des objets démultiplie les possibilités d'attaques, qui peuvent avoir des conséquences particulièrement graves, tant pour les données personnelles que sur le monde physique, car les objets connectés sont déjà et seront de plus en plus présents dans tous les aspects de nos vies et dans tous les contextes dans lesquels nous évoluons (maison, bureau, voiture, ville, usine, hôpital, etc.).

Les défis de recherche sont ici nombreux. En premier lieu, il faut absolument prendre en compte la sécurité dès la conception des objets, de leur matériel, de leurs systèmes d'exploitation, de leurs capacités de communication courte distance et basse énergie. Comme les ressources de calcul disponibles sur ces objets sont restreintes, la frugalité et la légèreté des mécanismes de sécurité sont essentielles. Ceci vaut bien entendu pour les mécanismes cryptographiques, dont il faut étudier des versions adaptées. Un point particulièrement délicat réside dans la possibilité de mise à jour des logiciels s'exécutant sur les objets (par exemple, suite à la découverte d'une faille de sécurité) et à la sécurisation de ces mises à jour, qui doit certainement s'appuyer sur la cryptographie. Enfin, comme dans les contextes informatiques plus classiques, l'indispensable prévention sera sans doute insuffisante. Il faut donc étudier comment la supervision de l'IoT pourra être réalisée de manière efficace mais légère et autonome (de nombreux contextes d'usage ne disposent pas d'administrateur), afin de permettre la détection d'attaques ou de comportements anormaux de

certains objets de manière plus au moins massive, des centaines de millions d'objets pouvant être impliqués dans les attaques.

Sécuriser les systèmes industriels

Les systèmes industriels reposent de plus en plus, en particulier pour des raisons économiques, sur des mécanismes logiciels et des standards ouverts. Ils peuvent donc être attaqués, comme n'importe quel autre système d'information. Le contexte est bien entendu extrêmement sensible, les conséquences d'une attaque pouvant être catastrophiques. En outre, certains dispositifs actuels seront utilisés encore de longues années, alors qu'ils n'ont pas été sécurisés à la conception. Ils offrent peu de ressources de calcul, ce qui rend difficile voire impossible l'ajout de mécanismes cryptographiques de protection des échanges, par exemple. Leurs spécifications ne sont pas toujours publiques, ce qui rend les dispositifs de sécurité standards (*firewalls*, détecteurs d'intrusions) incapables de traiter leurs flux réseaux.

Les défis de recherche sont bien entendu liés à l'adaptation des mécanismes de sécurité à ce contexte très spécifique, qui nécessite notamment un fonctionnement en temps réel. La coexistence entre des dispositifs modernes sécurisés et des dispositifs anciens qui n'auront pas pu être modifiés doit être soigneusement étudiée ; les protocoles de communications sont particulièrement concernés, car il faudra assurer l'interopérabilité. Enfin, dans un contexte où il sera difficile d'intégrer de nouveaux mécanismes et dispositifs, la supervision apparaît essentielle : l'étude de mécanismes de détection efficaces et spécifiques, aptes à être déployés dans ce contexte sans le perturber, est donc cruciale.

Sécuriser en présence d'apprentissage machine

Les systèmes dits d'intelligence artificielle s'appuient souvent aujourd'hui sur l'apprentissage statistique. Deux grandes menaces sont apportées par ces systèmes. La première est relative à la protection des données personnelles : quelles informations sur les données d'apprentissage est-il possible de tirer d'un réseau de neurones entraîné sur ces données, selon que l'attaquant ait ou n'ait pas accès aux valeurs internes de ce réseau ? La seconde menace est relative à la confiance que l'on peut avoir dans les sorties de ces systèmes. On sait en effet que l'ajout à une image d'un bruit soigneusement choisi et indiscernable à l'œil nu peut entraîner une classification incorrecte de cette image et ainsi conduire à une prise de décision erronée (on parle d'apprentissage antagoniste, ou *adversarial learning*).

Un défi de recherche pour s'assurer de la protection des données d'apprentissage consiste à étudier comment ces données peuvent/doivent être modifiées avant stockage et utilisation. Bien entendu, cette modification ne doit pas (trop) impacter les éléments indispensables à l'apprentissage et donc à la réalisation de la tâche que l'on attend du réseau entraîné. On peut aussi noter ici de manière connexe qu'une autre piste de recherche consiste à étudier une forme d'apprentissage distribué, afin de ne pas avoir à stocker toutes les données d'apprentissage au même endroit et, par là même, de limiter les conséquences d'une attaque potentielle.

La lutte contre l'apprentissage antagoniste nécessite dans un premier temps de comprendre les faiblesses des stratégies d'apprentissage, afin de déterminer précisément les attaques possibles, leur mode opératoire, puis la manière de les contrer. Il convient également d'étudier comment la supervision des interactions internes entre les couches d'un réseau permettrait d'observer et de caractériser d'éventuels artefacts illégitimes. Une telle étude permettra aussi de comprendre comment rendre ces interactions entre couches plus robustes.

Prendre en compte l'humain et ses organisations

Dans les interactions intégrant humains et machines, l'humain comme la machine peuvent être l'attaquant, le vecteur ou la victime. Comme nous le décrivons dans l'introduction, il est donc crucial de maîtriser les interactions, coopérations, combinaisons entre les systèmes humains de traitement de l'information et les systèmes numériques. Les défis de la recherche sont ici multipliés par la diversité des champs disciplinaires concernés, allant des sciences dures aux sciences douces, comme les nomme Michel Serres. Nous présentons ici succinctement quatre défis qui nous semblent importants.

En lien avec la manière dont l'humain traite les informations, un premier défi concerne la compréhension des interactions sociales humaines dans le contexte d'évolution continuelle du média numérique et d'encapacitation numérique globale de la société. Par ailleurs, comme des biais cognitifs peuvent être induits (c'est-à-dire engendrés par manipulation) à l'aide des systèmes d'information numériques, l'instillation de dis-informations (souvent appelées *fake news*) constitue un champ d'étude. L'adaptation fine de ces dis-informations aux cibles humaines visées s'appuie en particulier sur l'usage des réseaux sociaux. Le scandale Cambridge Analytica en est un exemple avéré. Détecter et analyser ces phénomènes est important, mais les contre-mesures seront difficiles à prendre. Elles pourront s'appuyer en particulier sur les avancées issues des points que nous traitons ci-dessous.

Le deuxième défi concerne la compréhension et l'anticipation des impacts géopolitiques, économiques et sociétaux de la cybersécurité. Ces éléments sont bien élaborés par le monde anglo-saxon, moins voire beaucoup moins dans les pays latins et en particulier en France. Des travaux existent, mais il faut aujourd'hui savoir se préparer pour élaborer des stratégies au niveau national et savoir ensuite les défendre au niveau international, en cohérence avec nos alliés. La défense de nos valeurs, mais aussi de nos savoir-faire et de nos entreprises, est à cette condition. Avoir une représentation française étoffée, préparée et cohérente dans les instances de standardisation et de normalisation est un défi en soi.

Le troisième défi important, c'est l'éducation. Les utilisateurs, trop peu conscients des enjeux, sont en conséquence souvent le maillon faible de la chaîne globale de cybersécurité. Une seule réponse technique est insuffisante ; elle doit être accompagnée de la construction d'une culture forte de la cybersécurité. L'éducation en est donc une composante essentielle. Des efforts importants de sensibilisation et de diffusion des connaissances doivent donc être faits, et ce, à destination de tous les publics : citoyens (y compris les enfants et adolescents), techniciens, ingénieurs, experts en sécurité et décideurs économiques ou politiques. Le déficit de compétence en cybersécurité est un handicap majeur pour les souverainetés nationale, numérique, entrepreneuriale et individuelle. Dès l'école, chacun devrait être initié aux bases de l'informatique et de la cybersécurité. Tout au long de la vie, chaque citoyen devrait être (re-)sensibilisé aux « bonnes pratiques » et à la « cyber-hygiène ». Bien entendu chaque utilisateur professionnel devrait être capable d'appréhender les risques liés aux cyber-attaques dans son contexte de travail et devrait connaître les parades possibles ; il devrait donc être formé en conséquence. Les administrateurs systèmes devraient quant à eux être régulièrement formés aux nouvelles menaces et aux nouvelles parades. Enfin, le pays et l'Europe ont besoin de davantage d'experts en cybersécurité : même si des formations sont aujourd'hui proposées par de nombreuses institutions publiques ou privées, des efforts majeurs doivent encore être faits.

Dernier défi évoqué ici, le développement multidisciplinaire d'interactions homme-machine de qualité. Si la technique seule est insuffisante, comme nous venons de le souligner, elle est cependant indispensable. Elle doit être rendue la plus simple d'utilisation possible, les erreurs humaines étant l'une des principales sources des problèmes de sécurité. Ces erreurs sont aussi souvent imputables

à la médiocrité des interactions et des interfaces humains-machines. Ces dernières devraient toujours être conçues pour éviter les erreurs involontaires et s'assurer que l'utilisateur est bien conscient des conséquences de ses actions. La conception de tels systèmes demande encore des travaux de recherche interdisciplinaires entre experts informaticiens et en sciences cognitives.

Conclusion

Il n'y a pas de petit défi en cybersécurité **:** la solidité de la chaîne est celle de son maillon le plus faible. Pour autant, les défis scientifiques liés à chacun des maillons sont de difficultés et de conséquences très variées. Par exemple, l'utilisation de techniques dites d'intelligence artificielle ou de calcul quantique induisent et induiront des disruptions particulièrement importantes et visibles.

Concernant spécifiquement la recherche scientifique, la France a un système académique contribuant au meilleur niveau international à l'avancée des connaissances pour la cybersécurité. C'est tout particulièrement vrai dans les domaines de la cryptologie et des méthodes formelles [3]. Les avancées qui en sont ou en seront issues irriguent un tissu très riche d'entreprises petites, moyennes ou grandes, très bien reconnues internationalement pour leur compétences et leurs savoir-faire. Un défi organisationnel et culturel consiste à ce que les compétences académiques et les compétences d'innovations qui en sont issues collaborent et s'inter-stimulent plus efficacement et facilement, et à ce que les entreprises, les centres de recherche, les écoles et les universités collaborent et innovent ensemble.

À plusieurs reprises nous avons évoqué les valeurs sous-jacentes à notre société. Un défi global, concernant chacun des éléments mentionnés ici, est le développement des réflexions éthiques sur tous les aspects de la cybersécurité. Un tel travail devra puiser ses réflexions aux niveaux individuel, entrepreneurial, local, régional et national et se coordonner au niveau d'un CCNE (comité consultatif national d'éthique) des sciences, technologies, usages et innovations du numérique [4]. Il devra aussi irriguer les réflexions européennes et internationales dans une démarche permettant à toutes ces entités d'expliciter leurs hiérarchies de valeurs et permettant en particulier aux usages et innovations de s'appuyer sur des corpus de réflexions éthiques partageables et, si possible, consistants.

La réflexion que nous avons conduite dans cet article est, par essence de l'exercice, courte et nécessairement schématique et incomplète. Elle s'appuie, outre sur le Livre blanc d'Inria déjà cité, sur de nombreuses feuilles de route dont les lecteurs intéressés pourront continuer à s'enrichir [5]. Enfin, concluons en notant qu'au niveau européen, des projets comme SPARTA [6] visent à bâtir une vision synthétique globale, intégrant notamment l'analyse de feuilles de route au niveau mondial.

(3) https://www.allistene.fr/files/2018/03/VF_cartographie_2017-06-13.pdf
(4) Voir les travaux de la CERNA sur « La souveraineté à l'ère du numérique. Rester maîtres de nos choix et de nos valeurs » http://cerna-ethics-allistene.org/digitalAssets/55/55708_AvisSouverainete-CERNA-2018.pdf
(5) Par exemple : www.ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies, https://it-security-map.eu, etc.
(6) "Re-imagining the way cybersecurity research, innovation, and training are performed in the European Union", https://www.sparta.eu

La confiance numérique, une condition *sine qua non* du succès de l'adoption du *cloud*

Par **Marc DARMON**
Directeur général adjoint, Thales
Systèmes d'Information et de Communication sécurisés
et **Olivier KERMAGORET**
Directeur du Segment Services managés, Infrastructures critiques et *Cloud*

Le *Cloud Computing* est devenu, en l'espace d'une dizaine d'années, une véritable réalité économique et opérationnelle. Ainsi, selon le rapport « *Cloud* et Sécurité » (CXP, 2018), 40 % des infrastructures informatiques en France utilisent une architecture *Cloud*, un quart d'entre elles étant déployées dans une version publique. Pour autant, le *Cloud* reste encore un univers en fort développement, comme le montre une récente étude réalisée conjointement par Thales et Pierre Audoin Consultants qui fait état d'une croissance de 33 % en 2018. Ces différents types de *Cloud*, qu'ils soient publics, privés ou hybrides, ont désormais atteint un niveau de maturité suffisant pour nous permettre d'avoir du recul sur leurs avantages mais également d'apprécier les difficultés auxquelles il faut faire face lors d'un projet de migration d'une informatique dédiée vers un *Cloud* [1].

Le *Cloud*, un levier indispensable de la transformation numérique

Diminution des coûts, flexibilité, agilité, réduction du *time to market,* etc. De nombreux facteurs expliquent le succès du *Cloud*. Mais son atout majeur reste sans doute sa capacité à projeter l'entreprise dans l'automatisation de la production informatique de façon sécurisée (processus de type DevSecOps [2]), tout en proposant des services complets de type SaaS (*Software as a Service*) grâce auxquels les entreprises bénéficient de fonctions métiers mutualisées et à forte valeur ajoutée (CRM, outils et messageries collaboratifs, RH…). Le SaaS est devenu de fait le mode privilégié de consommation du *Cloud*, puisqu'il représenterait désormais 54 % du marché [3].

Par voie de conséquence, le *Cloud* est devenu un levier indispensable de la transformation numérique, au centre de la compétitivité des entreprises. Pour BPIfrance, une entreprise sur cinq est condamnée à disparaître si elle n'entame pas sa transformation d'ici trois ans. En effet, le *Cloud* est indispensable aux applications numériques, notamment lorsqu'elles s'appuient sur le *big data*, l'Internet des Objets ou l'intelligence artificielle, qui nécessitent des infrastructures hautement et instantanément évolutives. Il offre aussi la possibilité de tester ces nouvelles applications rapidement avec un investissement très faible.

La cybersécurité, le facteur « confiance » du *Cloud*

De ce fait, la cybersécurité du *Cloud* est un enjeu crucial, une impérative nécessité pour une transformation numérique réussie. Aujourd'hui, les chiffres parlent d'eux-mêmes : 95 % des failles

(1) « HySIO Flex : le cloud de Thales, Une expérience de dix ans riche d'enseignements ».
(2) De DevOps à DevSecOps, modèles de maturité.
(3) http://blog.markess.com/2018/07/tendances-cloud-computing-2020/

de sécurité dans le *Cloud* sont liées à son utilisation par les entreprises (déploiement d'architectures non sécurisées), 15 millions d'attaques sur les connexions ont eu lieu sur le premier semestre 2019 pour 400 000 réussies, 85 % des organisations ont été spécifiquement ciblées par des attaques et 45 % d'entre elles ont eu au moins un compte compromis dans le *Cloud*[4]. Le rapport de référence Symantec[5], basé sur les informations collectées par 123 millions de capteurs consignant chaque seconde des milliers d'incidents liés à des menaces dans cent cinquante-sept pays et territoires, fait état des grandes tendances suivantes :

- Les attaques de *formjacking* (ou piratage de formulaire) ont grimpé en flèche, avec en moyenne 4800 sites web compromis chaque mois.
- Les *ransomwares* délaissent les particuliers pour cibler les entreprises, dont les infections ont augmenté de 12 %.
- Plus de soixante-dix millions de fichiers ont été dérobés dans des compartiments S3 mal configurés, conséquence directe de l'adoption rapide du *Cloud*.
- Les chaînes logistiques restent des cibles faciles, avec une hausse de 78 % des attaques.
- Enceinte connectée, reine des cyberattaques : les appareils IoT constituent un point d'entrée majeur pour les attaques ciblées ; la plupart des appareils connectés sont vulnérables.

Malheureusement, la sécurisation des systèmes d'information est encore parfois perçue comme un coût, un mal nécessaire dont l'apport de valeur resterait à prouver. La cybersécurité est devenue, au gré d'attaques aux conséquences parfois dramatiques et de régulations toujours plus exigeantes, une condition *sine qua non* du succès des solutions numériques. Qui peut imaginer une voiture connectée et pilotée depuis un *Cloud* d'entreprise, vulnérable à n'importe quelle attaque ? La confiance que les utilisateurs portent à une solution numérique est un élément déterminant de son acceptation. Il n'y a pas de solution numérique sans confiance et il ne peut y avoir de confiance sans cybersécurité. En ce sens, la cybersécurité est devenue un différentiateur qui conditionne le succès de la transformation numérique. Gardons bien à l'esprit que les systèmes informatiques, désormais massivement interconnectés, sont attaqués en permanence. Plus les systèmes informatiques regorgent de données et de traitement, plus ils représentent un intérêt pour les attaquants, quelles que soient leurs motivations. La question n'est plus de savoir si ces systèmes seront attaqués un jour, mais quand et comment ils le seront, et quelle sera leur résilience.

On pourrait penser qu'il n'y a là rien de nouveau et que la cybersécurité dans le *Cloud* n'est jamais qu'un prolongement de la cybersécurité dans des environnements classiques. Certes, les familles de menaces sont les mêmes mais les caractéristiques du *Cloud* introduisent un changement de paradigme :

- La volatilité des ressources dans le *Cloud* rend nécessaire le déploiement automatique et instantané de dispositifs de cybersécurité (par exemple, la mise en place d'un outil de filtrage comme un *firewall*).
- Il est facile et rapide pour des utilisateurs de souscrire à des services *Cloud*, de développer et déployer des applications, mais les responsables sécurité ont besoin de garder la maîtrise de leurs systèmes et d'avoir une visibilité exhaustive et en temps réel des services utilisés.
- La surface d'attaque augmente, en particulier lorsque les services de *Cloud* sont accessibles directement *via* des adresses publiques.
- La responsabilité est partagée : une partie de la cybersécurité est assurée par le fournisseur de services de *Cloud*, alors que l'autre partie, souvent importante, reste sous la responsabilité de l'utilisateur. Il est impératif de maîtriser cette cartographie des responsabilités.

(4) https://www.proofpoint.com/us/threat-insight/post/cloud-attacks-prove-effective-across-industries-first-half-2019
(5) https://resource.elq.symantec.com/LP=6863?inid=symc_threat-report_istr_to_leadgen_form_LP-6863_ISTR-2019-report-main&cid=70138000001QvLeAAK

- L'utilisation du *Cloud* impose des processus et des outils spécifiques qui ne soient pas sous le contrôle de l'opérateur de *Cloud* et qui permettent de gérer la sécurité des données et des accès (chiffrements, gestion d'identité, gestion des clés…). Dans ce cadre, il est essentiel pour les entreprises de désigner un tiers de confiance capable de les accompagner dans le choix et la gestion de ces outils.
- La nécessaire « hyper-connectivité » pour accéder aux services *Cloud* peut ouvrir de nouvelles failles *via* les réseaux d'interconnexion et de nouvelles dépendances.

Multi-Clouds : une approche pragmatique

Il est maintenant clair que le marché s'oriente vers des solutions de *Cloud* hybrides, *multi-Clouds*, mixant *Clouds* privés et publics. La plupart des entreprises choisissent cette stratégie pour deux raisons simples : d'une part, la solution unique qui répond à tous les besoins n'existe pas, et, d'autre part, elle ne permet pas de prendre en compte le niveau de sensibilité des données et les contraintes de conformité associées.

Sur ces questions, le pragmatisme doit prévaloir. Des compromis sont nécessaires pour prendre en compte les enjeux et le rapport risque/bénéfice de chaque solution, avec quatre critères de décision : l'attrait du modèle d'affaire du *Cloud*, l'attrait de l'offre technique et fonctionnelle du *Cloud*, la dépendance à un fournisseur et la souveraineté des données.

Les deux premiers points figurent souvent parmi les préoccupations des organisations, même si les risques d'indisponibilités ne sont pas toujours identifiés. En effet, si les principaux fournisseurs de services de *Cloud* proposent des mécanismes pour assurer la disponibilité des applications, l'application elle-même doit être conçue pour mettre en œuvre ces mécanismes et s'intégrer dans les solutions de *Edge Computing* fournies par les opérateurs de *Cloud*. Par ailleurs, bien que les fournisseurs de *Cloud* public annoncent quelques niveaux de service (performance, disponibilité, temps de réaction et de résolution des incidents…), leur engagement est, dans les faits, très limité puisque les pénalités en cas de défaillance sont faibles voire nulles et les marges de négociation inexistantes. Les architectures doivent donc être conçues dans ce sens.

La deuxième grande question que doivent se poser les organisations en construisant leur feuille de route *Cloud* est la dépendance aux fournisseurs, le risque de *Vendor Lock-in*. Les plus grands *Clouds* publics offrent aujourd'hui un catalogue de services de haut niveau, les fameuses APIs, inégalées… et propriétaires ! Ces APIs sont un formidable accélérateur des nouveaux projets mais elles créent aussi une dépendance de fait avec un fournisseur. Avec leur utilisation, la réversibilité devient très théorique parce que très onéreuse. L'un des risques est la dépendance vis-à-vis d'acteurs qui modifient unilatéralement leurs grilles tarifaires ou leur modèle d'affaire. Ici, l'importance et la durée de vie du logiciel seront déterminantes. On n'aborde pas de la même manière un logiciel stratégique et un logiciel qui ne l'est pas, un logiciel d'utilisation temporaire et un logiciel qui durera plus de vingt ans.

Enfin, le dernier point, trop souvent sous-estimé par naïveté ou manque de sensibilisation, est certainement le plus crucial : il s'agit de celui de la souveraineté.

La souveraineté des données est entendue ici au sens du contrôle qu'une organisation, quelle qu'elle soit, doit avoir sur ses propres données. Il faut bien entendu penser souveraineté nationale, mais également souveraineté d'entreprise !

Traiter toutes les données de la même manière, avec un niveau de protection équivalent quelle que soit leur valeur ou leur sensibilité, n'a pas de sens. Un niveau de protection très important de toutes les données peut s'avérer contreproductif, car cela ne permettra pas à l'organisation concernée de bénéficier de tous les avantages du *Cloud*. À l'inverse, un niveau global de protection

faible fera peser bien trop de risques sur des données sensibles. L'analyse et le classement des données en fonction de leur sensibilité permettent donc de choisir des solutions de *Cloud* adaptées et de définir les justes mesures de protection. Ainsi, la richesse et la rapidité de mise en œuvre des solutions de *Cloud* publics sont séduisantes, mais elles peuvent être incompatibles avec le niveau de sensibilité de certaines données.

Les exemples de piratages massifs de données personnelles ou confidentielles sont quasi quotidiens car le *Cloud* offre, de fait, un large effet d'échelle en cas de vol de données. Des mesures de protection multiples peuvent permettre d'apporter une réponse globale efficace. Elles sont à la fois d'ordre organisationnel (définition et exécution d'une politique de sécurité, adoption de bonnes pratiques par les concepteurs, développeurs de solution, opérateurs en production, adoption d'une approche DevSecOps [6]) et d'ordre technique.

Parmi ces dernières, on peut citer en particulier le chiffrement systématique de toutes les données. Plusieurs solutions existent, par exemple VeraCrypt, orienté pour les besoins des particuliers, ou Vormetrics, que propose Thales à destination des entreprises. L'algorithme de chiffrement doit être suffisant pour résister aux attaques et les clés de chiffrement doivent être gérées dans une infrastructure de confiance indépendante du fournisseur de *Cloud*. Ainsi, le Chief Technology Officer de AWS, Werner Vogles, a indiqué, lors du AWS Summit de Berlin, en février 2019, la nécessité de ce chiffrement et d'une gestion indépendante des clés de chiffrement par la mise en place de solutions permettant le *Bring your own key* (BYOK). L'authentification des utilisateurs et la gestion de leurs droits doivent être assurées et l'activité tracée et supervisée de manière à détecter les tentatives d'accès non autorisées. Toutefois, le chiffrement des données n'est pas toujours possible, notamment dans les phases d'exploitation de ces données par des applications (modèle SaaS). L'anonymisation est une solution possible pour répondre en partie à ce défi.

Parmi les premières protections des environnements de Cloud figurent également la gestion d'identité et le contrôle d'accès (tel que le permet l'offre *Safenet Trusted Access*), afin de prévenir les risques d'intrusion. Ces mesures sont cruciales parce qu'elles sécurisent l'ensemble des environnements sur site et dans le *Cloud* et en particulier l'accès aux services, aux ressources et aux interfaces de programmation directement exposés sur Internet. Basées sur l'analyse des contextes d'utilisation, des populations d'utilisateurs ciblés, et de la sensibilité des applications auxquelles ces derniers accèdent, des politiques de sécurité *ad hoc* doivent être mises en place pour gérer le contrôle d'accès adapté, entre facilité pour l'utilisateur et niveau d'authentification nécessaire (telle que l'authentification forte multi-facteurs). La gestion des comptes à privilège doit être activée pour protéger les comptes d'administration, particulièrement sensibles du fait des droits étendus qui leur sont attribués.

Enfin, d'autres mesures techniques importantes s'appliquent à la protection des environnements de *Cloud*, comme les audits de code, les tests d'intrusion, les scans de vulnérabilité, la détection des menaces, les services de supervision de sécurité, etc.

L'impact du *Cloud Act* et des mesures à portée extraterritoriale

La question de la souveraineté des données dans le *Cloud* se double de risques supplémentaires liés aux lois extraterritoriales.

Le rapport établi par la commission d'enquête présidée par le député de Saône-et-Loire Raphaël Gauvin et intitulé « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises

(6) De DevOps à DevSecOps, modèles de maturité.

des lois et mesures à portée extraterritoriale » débute par ce constat très inquiétant :

> « Les États-Unis d'Amérique ont entraîné le monde dans l'ère du protectionnisme judiciaire. Alors que la règle de droit a, de tout temps, servi d'instrument de régulation, elle est devenue aujourd'hui une arme de destruction dans la guerre économique que mènent les États-Unis contre le reste du monde, y compris contre leurs alliés traditionnels en Europe. (…) Les entreprises françaises ne disposent pas aujourd'hui des outils juridiques efficaces pour se défendre… »

Suit une liste non exhaustive d'entreprises non Américaines condamnées très lourdement par les États-Unis au motif que leurs pratiques commerciales ne respectaient pas le droit américain, alors même qu'aucune de ces pratiques n'avait de lien direct avec le territoire des États-Unis et/ou que ces entreprises se conformaient au droit de leur pays : BNP Paribas, HSBC, Commerzbank, Crédit Agricole, Standard Chartered, ING, Bank of Tokyo, Royal Bank of Scotland, Siemens, Alstom, Télia, BAE, Total, Crédit Suisse et demain, peut-être, Airbus, Areva, etc.

Selon le rapport, ces enquêtes et condamnations mettent en exergue cinq problèmes fondamentaux :

- Elles sont contestables et violent la souveraineté des pays.
- Les sanctions prononcées sont disproportionnées et menacent la pérennité des sociétés étrangères visées.
- Les enquêtes sont conduites sous le contrôle des procureurs américains, eux-mêmes placés sous l'autorité directe du pouvoir exécutif.
- Les conventions d'entraide judiciaire et les règles de la coopération administrative sont systématiquement contournées.
- Surtout, les poursuites engagées semblent être motivées économiquement et les cibles choisies à dessein.

Le *Cloud Act* semble s'inscrire pleinement dans cette stratégie, en imposant, dans certains cas, aux fournisseurs de *Cloud* public et aux opérateurs de réseau d'origine américaine l'obligation de fournir, à la demande des autorités judiciaires américaines, les données d'un client qu'ils gèrent ou qui transitent sur leurs réseaux, quelle que soit leur localisation géographique. Le fournisseur ou l'opérateur à qui une telle obligation est faite peut aussi se voir interdit d'en informer son client.

Les éléments de sécurité informatique que nous avons mentionnés ne permettent pas de répondre à ce problème. Des réponses peuvent être trouvées dans des solutions de *Clouds* privés ou publics offerts par des tiers de confiance européens, qui échappent donc au *Cloud Act*. C'est d'ailleurs pour cette raison que le Comité Stratégique de Filière de l'industrie de sécurité travaille, à la demande de Bruno Le Maire, ministre de l'Économie et des Finances, à la mise à disposition d'un ensemble des solutions de *Cloud* de confiance performantes, compétitives et indépendantes, en France voire en Europe.

Du *Cloud* civil vers la Défense et les armées

La transformation *Cloud* dans le monde civil a un impact pressant sur le secteur de la Défense. En effet, les utilisateurs, dans tous les rôles, vivent au quotidien les bénéfices du *Cloud*. Mais comme le pose le général Crall du *Department of Defense* américain : "Can it operate successfully in an information-contested environment, when a sophisticated adversary – *e.g.* Russia or China – is jamming your transmissions and hacking your network?" Le *Cloud* civil doit donc s'adapter à l'environnement militaire. Des prérequis supplémentaires et spécifiques s'appliquent à la Défense. La sécurité est très cadrée avec des référentiels comme celui de l'OTAN qui imposent une ségrégation étanche des flux et du stockage d'information suivant le niveau de confidentialité.

À cette sécurité exacerbée se conjugue l'impératif de souveraineté nationale, le risque émanant du plus faible maillon de toute la chaîne « sécurité et souveraineté ».

Ainsi, le modèle de déploiement en *Cloud* privé se détache comme solution pour les données classifiées et la projection sur les théâtres. Il garantit la souveraineté et l'adaptation aux conditions d'usage, tout en offrant les bénéfices du *Cloud* –décloisonnement des données, mutualisation des ressources, omni-disponibilité des services – en environnement contrôlé.

Le *Cloud* offre de formidables capacités de flexibilité qui transforment profondément l'informatique et par là-même nos organisations et la relation des entreprises avec leurs clients. Cette profonde mutation crée de nouvelles dépendances et peut se transformer en cauchemar économique pour les entreprises ou les administrations concernées, sans la mise en œuvre d'une véritable stratégie de mouvement vers le *Cloud* intégrant dès sa conception la dimension cybersécurité. Il ne s'agit pas d'injonctions contradictoires ou d'un mur infranchissable, car les solutions existent. Mais c'est une condition impérative pour établir une confiance durable et une vraie promesse de valeur.

L'Internet des Objets modifie la cybersécurité : l'exemple de Linky

Par **Hervé CHAMPENOIS**,
Directeur du programme Linky chez ENEDIS

Le programme Linky, un poste d'observation privilégié du développement de l'Internet des Objets

Le déploiement des compteurs d'électricité Linky s'inscrit dans un phénomène bien plus large qui est celui du développement des objets connectés dans le monde. Ce développement est si rapide que l'on peine à dénombrer précisément ces objets connectés, même si on peut aujourd'hui estimer qu'ils sont aux alentours de vingt milliards – soit trois par humain ! L'essor de l'internet des objets s'explique par le développement de la communication sans fil – la 5G va encore amplifier le phénomène –, conjugué à la transformation numérique de la sphère privée et de la sphère professionnelle, et à l'augmentation des services autour des données individuelles et collectives.

Ce mouvement touche aussi bien les objets du quotidien – les smartphones, les montres, les véhicules, les réfrigérateurs, les trottinettes électriques, les box Internet…– que les applications professionnelles. L'installation de 35 millions de compteurs communicants à horizon 2021 en est donc une illustration parmi tant d'autres. Linky apporte de nouveaux services à nos clients tout en permettant d'améliorer la gestion du réseau exploité par Enedis pour de nouveaux développements du réseau (autoconsommation avec les panneaux solaires, véhicule électrique…). Aujourd'hui, environ deux Français sur trois sont déjà équipés du nouveau compteur. Et l'appropriation est bonne : plus de 85 % des clients se disent satisfaits de Linky. Nous constatons chaque mois une progression d'environ 10 % du nombre de clients abonnés aux services associés aux nouveaux compteurs : c'est une progression similaire à celle des abonnés à la fibre par exemple, et cela dit beaucoup de l'appétence de chacun pour les usages de cet objet connecté qui est l'allié du consommateur et de la transition énergétique. Il permet par exemple de suivre sa consommation d'électricité précisément alors que par le passé, nous ne disposions au mieux que d'une mesure tous les six mois.

Le succès de l'IoT au prisme de Linky

La finalité première de l'internet des objets, c'est d'apporter de nouveaux services pour les clients et des gains d'efficacité pour les entreprises – par exemple pour optimiser le suivi des flux logistiques ou la maintenance prédictive des infrastructures. Les champs d'application sont très larges, de la santé au divertissement en passant par la maison connectée dont le marché ne cesse de progresser et représente aujourd'hui environ 2 milliards d'euros par an en France. On le voit en particulier avec le développement des véhicules en partage (scooter, voiture, trottinettes, vélo) dont l'expansion repose sur deux objets connectés : le smartphone et le véhicule loué.

Avec le nouveau compteur, Enedis, entreprise de service public implantée dans tous les territoires, modernise le réseau de distribution d'électricité et améliore la qualité du service rendu aux Français, notamment pour les accompagner vers la transition énergétique.

Prenons quelques exemples : lorsque vous vous installez dans un nouveau logement dans lequel il est nécessaire de remettre en service suite au départ de l'occupant précédent, vous pouvez

désormais disposer de votre électricité rétablie en moins de 24 heures. Avec l'ancien compteur, cela pouvait prendre jusqu'à 5 jours. Cet été, ce sont près de 700 000 emménagements qui ont été simplifiés grâce à la mise en service à distance. Autre exemple : les pannes sont détectées plus rapidement ce qui permet de déclencher une opération de maintenance, parfois même avant que le client ne se rende compte que l'alimentation a été coupée ! Cette réactivité est notamment indispensable lorsqu'Enedis intervient pour rétablir l'électricité suite à une tempête ou autres événements climatiques de plus en plus fréquents. Les fournisseurs d'énergie peuvent également proposer aux consommateurs des offres plus avantageuses et mieux adaptées à leurs habitudes de consommation d'électricité. Enfin, avec Linky, nos clients peuvent s'engager à leur rythme dans la transition énergétique, en suivant – et donc en maîtrisant – au plus près leurs consommations ou encore en contribuant au développement des énergies renouvelables, par exemple à travers l'installation facilitée de panneaux photovoltaïques sur le toit de l'habitation pour consommer leur propre électricité.

Tous ces changements sont synonymes de simplicité et d'économies pour le client. Ils contribuent à faciliter la vie des gens ; cela explique le caractère attractif de l'Internet des Objets.

Une condition semble néanmoins indispensable pour que les clients adhèrent à ces nouvelles possibilités, c'est qu'ils aient confiance dans notre capacité à protéger leurs données et à garantir l'intégrité des infrastructures d'Enedis – réseau de distribution et systèmes d'information – en réponse à des cyberattaques. Les services apportés par l'internet des objets ne doivent pas occulter les nouveaux enjeux en matière de cybersécurité que soulève le développement de l'IoT.

L'Internet des Objets renforce-t-il l'exposition aux cyberattaques ?

La multiplication des objets connectés reliés à des systèmes plus ou moins centralisés conduit à multiplier le nombre de points d'entrée potentiels dans les systèmes des entreprises et des administrations. Prenons un exemple simple : en se connectant au matériel d'un client, des *hackers* peuvent remonter jusqu'aux systèmes du fabricant grâce aux informations que le matériel transmet quotidiennement. La corruption de l'ensemble de l'entreprise, de ses produits et réseaux peut s'effectuer en quelques heures, voire quelques minutes. Nous avons également en tête cette expérience menée en 2015 par des chercheurs américains qui ont développé un outil pour prendre le contrôle à distance d'une voiture connectée. Tout ceci peut attirer des *hackers* car les automobiles sont en train de se transformer en « smart cars » connectées.

Les cyberattaques qui passent par les objets connectés poursuivent en fin de compte les mêmes finalités que les cyberattaques classiques – accéder à des informations confidentielles, modifier des données à des fins malveillantes ou encore bloquer des systèmes d'information et les activités associées – mais leurs effets peuvent s'en trouver démultipliés. Avant, seuls les terminaux informatiques permettaient d'accéder aux systèmes d'information ; aujourd'hui certains objets connectés utilisés au quotidien, comme les smartphones, peuvent garder la mémoire précise des faits et gestes. Les informations collectées sont nombreuses et indiquent par exemple l'emplacement physique où se trouve l'objet connecté généralement associé à la personne qui l'utilise – même si cela doit être relativisé en ce qui concerne Linky, qui par défaut ne transmet à Enedis que la consommation à une maille quotidienne et ne peut distinguer les différents usages électriques à l'intérieur de l'habitation. L'internet des objets doit donc être accompagné de mesures permettant de réduire l'exposition aux cyberattaques, mais également leurs effets potentiels.

Enedis n'a pas attendu Linky pour intégrer les exigences les plus élevées en matière de cybersécurité. Les réseaux de distribution d'électricité sont en effet des infrastructures qui nécessitent une protection à la hauteur des enjeux associés.

IoT et cybersécurité : un changement de perspective

La cybersécurité repose sur trois grands piliers : la protection par conception des matériels, logiciels et canaux de communication, la surveillance de sécurité, et la capacité de réaction aux agressions. Pour autant le rôle et le comportement des utilisateurs demeurent cruciaux. Cette approche se décline naturellement sur l'internet des objets mais avec une amplification liée au champ d'application qui englobe une multitude d'objets et d'utilisateurs. C'est ce qui la rend plus large et plus exigeante en matière de réactivité.

Avec la démultiplication des objets connectés, il ne s'agit plus seulement de protéger et de défendre la « place forte » que représente le système d'information centralisé, mais également les faubourgs et la campagne environnante : la surveillance doit donc être adaptée, et nécessite une attention permanente. Cela implique de sécuriser l'objet connecté mais également les logiciels informatiques qui constituent le support de transmission, de stockage et de traitement de l'information. L'effort doit se concentrer alors dans la capacité à mettre sur le marché des objets modernes, performants tout en garantissant une protection adaptée à leurs usages dans un contexte de forte concurrence. L'ETSI (*European Telecommunications Standard Institute*) a par exemple récemment publié des standards techniques de base pour la sécurité de l'IoT, c'est une bonne chose qui traduit la prise en main du sujet « cybersécurité » dans le domaine des objets connectés.

Par ailleurs, dès lors que l'objet connecté est installé, sa supervision et la mise à jour des logiciels pour apporter des correctifs dans une logique de conformité représente un défi, à la fois parce que ces objets sont répartis dans de vastes espaces, mais aussi parce que le coût des mises à jour – et *a fortiori* des contrôles sur site – est significatif par rapport au coût unitaire de l'objet.

Ensuite, parce que la démultiplication des objets s'accompagne d'une démultiplication des utilisateurs. Toute personne qui possède un objet connecté doit être considérée comme partie prenante du processus global de sécurité. La sensibilisation des utilisateurs est donc un enjeu majeur, elle passe souvent par des choses simples – avoir un mot de passe suffisamment long, éviter de se connecter autant que possible sur des réseaux sans fil inconnus… – mais le nombre d'utilisateurs rend la tâche plus ardue. Cette sensibilisation vaut aussi bien pour le grand public que pour les salariés d'entreprises et d'administrations qui ont à traiter de plus en plus de données confidentielles. Elle nécessite d'adapter les processus internes et d'accompagner chaque utilisateur de données. Chez Enedis, nous avons par exemple mis en place un module pédagogique « conformité RGPD » que chaque salarié est tenu de suivre.

Répondre à ces nouveaux défis : l'exemple du déploiement de Linky

A l'aune de l'expérience Linky, trois axes nous semblent incontournables pour profiter des services qu'offrent les objets connectés tout en assurant le niveau le plus élevé possible de cybersécurité.

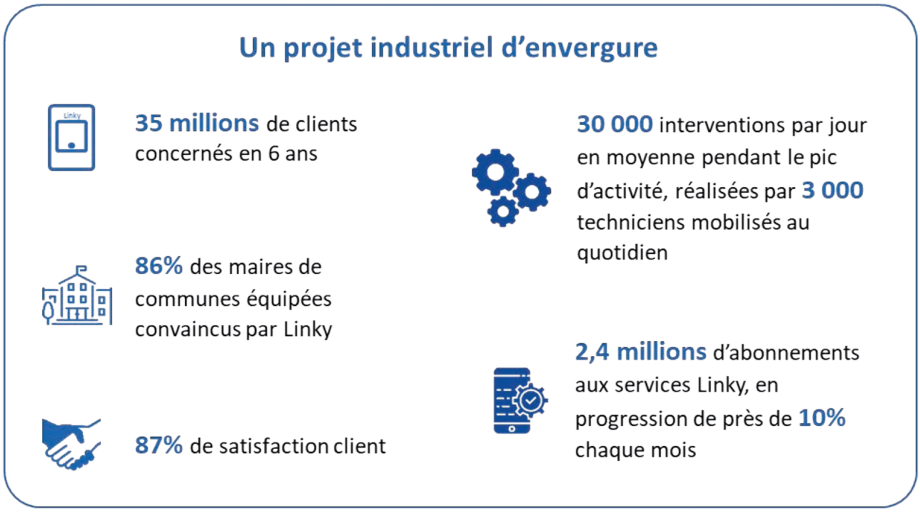
En premier lieu, la sécurité doit être pensée dès la conception de l'objet connecté. C'est l'approche *security by design*, que l'on pourrait traduire assez simplement par « mieux vaut prévenir que guérir ». C'est ce principe que nous avons appliqué pour construire le système Linky, pour garantir aussi bien la sécurité des données de nos clients que l'intégrité des infrastructures d'Enedis. Ce système est un tout qui va des compteurs jusqu'à nos systèmes d'information. A chaque niveau, des dispositifs anti-intrusion extrêmement robustes ont été prévus. La communication des données entre chaque partie est par ailleurs sécurisée à travers divers processus de chiffrement, et nos systèmes d'information sont isolés pour parer tout risque de contagion. Nous appliquons de surcroît un principe fondamental qui est au cœur de la doctrine de la CNIL (Commission nationale Informatique et Libertés) en matière

de protection des données : il s'agit du principe de proportionnalité. Les informations enregistrées et transmises par le compteur Linky sont strictement nécessaires au regard de la finalité de la collecte, qui est le comptage de consommations d'électricité. Autrement dit, les informations transmises par le compteur sont volontairement limitées et ne donnent que le minimum d'informations nécessaires sur le point de livraison en électricité. Ainsi, aucune autre information n'est véhiculée, ce qui d'ailleurs alourdirait inutilement le système.

En second lieu, la cybersécurité appliquée au domaine de l'IoT implique une approche dynamique car le contexte d'un jour n'est pas celui du lendemain. Cela demande de mobiliser des moyens importants – nous consacrons une part significative de nos efforts à la cybersécurité. Cette approche dynamique repose sur un système de supervision des objets connectés et d'audit efficace pour identifier toute amélioration et lancer d'éventuels correctifs. C'est pour cette raison que nous avons mis en place un service qui veille, 24 heures sur 24, au bon fonctionnement de cette chaîne communicante, en particulier pour détecter et juguler d'éventuels défauts. Nos équipes recherchent par ailleurs en permanence les évolutions à apporter dans le système. Si besoin, une mise à jour des mesures de protection peut être mise en place. Dans la même logique, des audits indépendants sont régulièrement menés dans nos infrastructures, à notre initiative ou à celle de nos parties prenantes, comme la CNIL ou l'Agence nationale de Sécurité des Systèmes d'Information (ANSSI).

Un dernier point nous semble fondamental, c'est que plus que jamais, avec l'essor des objets connectés, l'approche de la cybersécurité doit être collective et co-construite. Nous avons élaboré notre système de sécurité Linky en étroite collaboration avec la CNIL et l'ANSSI, qui nous délivre des certificats de conformité. Nos constructeurs sont associés à cette démarche car les chaînes de production doivent également être robustes en matière de cybersécurité, et nous communiquons en toute transparence auprès de nos clients pour leur expliquer l'usage qui est fait de leurs données et la façon dont elles sont protégées. Le tout sous l'œil des pouvoirs publics qui ont un rôle central à jouer pour créer un cadre juridique protecteur des informations et des systèmes – en particulier les plus stratégiques pour le pays –, mener des audits sur le terrain et sensibiliser la diversité des utilisateurs d'objets connectés, notamment le grand public.

Ces trois conditions doivent, nous semble-t-il, être réunies pour que l'Internet des Objets puisse effectivement concilier nouveaux services aux clients et aux entreprises, et protection de l'information. La protection efficace et démontrée de l'information représente un challenge passionnant et exigeant pour disposer de ces nouvelles technologies en toute sérénité.



Quelle régulation pour les acteurs privés dans le cyberespace ?

Par **Florian ESCUDIÉ**
Ministère de l'Europe et des Affaires étrangères

Le 12 novembre 2018 marque un tournant dans l'histoire récente de la régulation du cyberespace. La France accueillait, en effet, à cette date, deux événements importants – respectivement le Forum de Paris pour la Paix et le Forum sur la Gouvernance de l'Internet. Le Président de la République française y annonçait le lancement d'une initiative d'un genre nouveau, l'Appel de Paris pour la confiance et la sécurité dans le cyberespace.

Cet appel [(1)] réunissait pour la première fois des acteurs de natures différentes – États, entreprises, organisations de la société civile – qui s'engageaient à agir ensemble pour renforcer les normes internationales pertinentes et à faire respecter les droits des personnes et les protéger en ligne comme c'est le cas dans le monde physique. À travers cette approche dite « multi-acteurs », les soutiens de l'Appel de Paris désignaient plusieurs priorités, dont la prévention et la résilience face aux activités malveillantes en ligne, la protection de l'accessibilité et de l'intégrité d'Internet, la prévention des interférences dans les processus électoraux, la lutte contre les violations de la propriété intellectuelle par voie cyber, la lutte contre la prolifération des programmes et techniques cyber-malveillants, l'accroissement de la sécurité des produits et services numériques, la promotion de l'hygiène cyber ou encore l'interdiction du cyber-mercenariat et les actions offensives des acteurs non étatiques.

Jusqu'alors la sécurité dans le cyberespace était largement perçue comme relevant de la responsabilité des seuls États. Aux yeux de nombreux acteurs, il ne s'agissait pas tant de reconnaître que le rôle classiquement dévolu aux États par le droit international trouvait également à s'appliquer dans le cyberespace. Beaucoup pointaient, surtout, le développement par certains États d'outils et de techniques dans l'espace cyber à des fins offensives, parfois hors de tout cadre garantissant le respect du droit. L'affaire Snowden et la révélation de pratiques d'espionnage à grande échelle avaient, à cet égard, cristallisé les préoccupations et les critiques. Mettant en avant leurs responsabilités à l'égard de leurs clients, de nombreuses grandes entreprises du numérique étaient alors montées en première ligne pour dénoncer ces pratiques [(2)]. Dans le même temps, elles ne disaient rien de leurs propres responsabilités, alors même que la plupart des attaques conduites dans le cyberespace résultent de l'exploitation de vulnérabilités contenues dans des produits et services développés par ces mêmes entreprises.

Avec l'Appel de Paris, il ne s'agit plus de rejeter le blâme sur d'autres acteurs mais bien de rechercher ensemble les moyens d'assurer la stabilité du cyberespace et la protection de ceux qui s'y meuvent. Chaque soutien reconnaît ses responsabilités spécifiques et admet la pleine mise en œuvre du droit international dans le cyberespace de même qu'une régulation adaptée aux spécificités de cet espace. Sur cette base, il est possible d'envisager un approfondissement des règles régissant les rapports entre État et acteurs non étatiques dans l'espace cyber.

(1) À la date de la rédaction de cet article, 69 États, 361 entreprises et 149 organisations de la société civile avaient annoncé leur soutien à l'Appel de Paris.
(2) SMITH B. & BROWNE C.A. (2019), *Tools and Weapons. The promise and the peril of the digital age*, New York, Penguin Press.

Les acteurs privés occupent une place centrale dans l'espace de confrontation qu'est devenu le cyberespace

L'essor du numérique comme nouvel outil et espace de confrontation confère au secteur privé, notamment à un certain nombre d'acteurs systémiques, un rôle critique et une responsabilité inédite dans la préservation de la paix et de la sécurité nationale. Cette responsabilité découle d'abord de la nature même du cyberespace et du rôle qu'y jouent par construction les acteurs privés. Le « champ de bataille » est, en effet, en grande partie constitué de produits commerciaux grand public. Des attaques de grande envergure en exploitent les défauts (cf. faille du logiciel de comptabilité ME.DOC dans le cas de *NotPetya* en juin 2017).

Dans un contexte marqué par la numérisation croissante de nos sociétés, la surface d'attaque grandit à mesure que l'interconnexion des systèmes et des équipements se généralise. Les vulnérabilités exploitées par les attaquants peuvent également faciliter la constitution d'une infrastructure d'attaque importante. C'est ce qui s'est passé, par exemple, avec *Mirai* à l'automne 2016 et la constitution de *botnets* géants à partir de milliers d'objets connectés faiblement sécurisés et enrôlés pour mettre en œuvre une attaque massive par déni de service distribué (DDoS).

Mais si des entreprises peuvent être, malgré elles, liées à des actions malveillantes qui exploitent les faiblesses intrinsèques de leurs produits, parfois inconnues d'elles-mêmes (*zero-days*), il arrive aussi que des acteurs privés contribuent activement à des actions déstabilisantes. D'une part, les « armes » (logiciels intrusifs ou destructifs) sont, pour partie, produites par des entreprises privées sur un marché très faiblement régulé. Des services de « mercenariat » se développent, d'autre part, pour proposer à des clients, victimes d'attaques informatiques, des activités offensives destinées à récupérer des données dérobées en s'introduisant dans des systèmes informatiques tiers. Ces activités peuvent aller jusqu'à la conduite d'actions de représailles, dans une logique de légitime défense privée (*hackback*), aux effets hautement déstabilisateurs.

Il existe aujourd'hui une demande croissante de clarification des obligations incombant aux acteurs non étatiques dans le cyberespace. Cette demande émane d'abord des États, soucieux, à juste titre, de ne pas voir remis en cause leur monopole de la violence légitime, avec ce que cela pourrait entraîner en termes de déstabilisation des relations interétatiques. Mais, fait nouveau, le secteur privé lui-même est demandeur d'une clarification des règles. Il importe, dès lors, que les États répondent à cette attente, non sans associer étroitement les entreprises aux débats en cours sur la régulation du cyberespace.

La sécurisation des produits et des services numériques est un enjeu crucial pour la stabilité du cyberespace

Constat

De nombreuses attaques informatiques sont aujourd'hui rendues possibles par l'absence de mise à jour de sécurité de produits informatiques, pour certains largement répandus. Ce défaut de sécurité peut résulter de l'absence de correctifs (*patch*) pour des vulnérabilités pourtant connues ou bien, lorsque de tels correctifs existent, de leur insuffisante diffusion. En outre, les producteurs n'offrent pas systématiquement une assistance pour faire face à une attaque et faciliter le rétablissement du fonctionnement normal de leurs produits. Plus grave encore, les distributeurs et les intégrateurs diffusent parfois des produits dans des versions obsolètes ou non actualisables, voire diffusent des produits connus pour leur niveau de sécurité insuffisant.

De tels comportements ne sont pas acceptables : non seulement ils conduisent l'usager de ces produits à prendre, individuellement et malgré lui, des risques pour ses systèmes et ses données

mais ils risquent, plus largement, de fragiliser la stabilité de l'ensemble d'un écosystème, voire du cyberespace dans son ensemble, lorsqu'il s'agit de produits massivement utilisés (dimension systémique).

Aussi, c'est bien la responsabilité de tous les acteurs de la *supply chain* (de la conception à l'intégration, au déploiement, à la maintenance et à la gestion de la fin de vie) qui est engagée.

Solutions

Un consensus a peu à peu émergé parmi les États sur l'importance de poser au niveau international un principe de responsabilité des acteurs privés dans le renforcement de la stabilité et de la sécurité internationale du cyberespace. Cette proposition a d'ailleurs fait l'objet d'un accord lors des négociations conduites à l'ONU dans le cadre du groupe d'experts gouvernementaux (GGE) sur le cyberespace en 2017. Le rapport du GGE n'ayant finalement pu être adopté, faute d'accord entre États participants sur une autre question – celle des conditions d'application du droit international dans le cyberespace –, la diplomatie française avait fait le choix de poursuivre les travaux sur ce point, en lançant une initiative spécifique. Le ministre de l'Europe et des Affaires étrangères, Jean-Yves Le Drian, avait ainsi présidé un événement dédié à ce sujet en marge de l'assemblée générale des Nations Unies en septembre 2017. Cette initiative allait déboucher l'année suivante sur l'Appel de Paris mais aussi sur le lancement de discussions techniques dans le cadre de l'OCDE.

L'enjeu est de fixer un niveau d'exigence minimal de sécurité pour les produits et plus généralement pour les systèmes dans lesquels ils s'intègrent. Le recours à la certification de sécurité doit être encouragé, voire rendu obligatoire pour les composants critiques dans les secteurs sensibles.

Toutefois, une telle mesure ne saurait suffire et c'est un renforcement en profondeur de la culture de sécurité qui doit s'imposer aux entreprises. Celles-ci devraient être encouragées à prendre des mesures proactives pour maintenir de manière continue la sécurité de leurs produits (veille, équipes dédiées de revues de la sécurité, formation des équipes de développement, organisation de *bug bounty*, transparence dans la détection de failles de sécurité…). Les correctifs doivent être accessibles, le plus largement possible, même en l'absence de contrat de maintenance et dans un délai raisonnable, une fois la vulnérabilité portée à la connaissance du producteur.

La mise en œuvre d'actions offensives dans le cyberespace par des acteurs non étatiques doit être prohibée

Constat

Dans un contexte marqué par la multiplication et la sophistication d'attaques cyber visant spécifiquement les acteurs privés, quelles qu'en soient les motivations (espionnage économique, rançonnage, tentative de porter atteinte à la réputation, etc.), les entreprises sont incitées à développer des mesures de défense passive (pare-feu, antivirus, règles de cyber-hygiène). Force est toutefois de constater que de telles mesures, pas toujours bien appliquées d'ailleurs, n'offrent pas une garantie complète. En particulier, elles ne protègent que contre des menaces déjà identifiées. Par ailleurs, la perspective de recouvrir ses avoirs en cas d'attaque reste aléatoire. Si le dépôt d'une plainte est vivement recommandé, il ne peut jamais être garanti qu'une procédure judiciaire permettra d'identifier des responsables et d'obtenir réparation.

Des mesures de défense active peuvent, dès lors, être privilégiées par certains acteurs privés en complément des mesures de défense passive. Ces mesures (traçage de données, neutralisation de machines infectées contribuant à un *botnet*, dissémination de marqueurs fournissant des informations de serveurs tiers…) peuvent affecter le système informatique d'un tiers. Poussées à l'extrême, ces mesures peuvent aller jusqu'à inclure une réponse aux attaques (*hackback*) par des moyens (blocage, récupération de données, sabotage…) fortement intrusifs et s'apparentant à un

recours à la force dans le cyberespace. Pour ce faire, les acteurs privés concernés s'appuient soit sur leurs ressources et capacités propres, soit sur des sous-traitants dotés de capacités cyber-offensives (logique de mercenariat).

Disons-le franchement : la mise en œuvre d'actions offensives par des acteurs non étatiques n'est pas acceptable. Non seulement elle remet en cause le monopole de l'usage de la force par les États et est contraire au droit international, mais elle induit aussi des risques importants pour la stabilité du cyberespace. Imaginons, en effet, un acteur privé décidé à recouvrir des données dérobées par tous les moyens. Cet acteur, sur la base d'une attribution autonome, de la responsabilité de l'attaque à une entité tierce, pourra chercher à neutraliser des infrastructures d'attaque de l'attaquant présumé. Or, cette action peut avoir des effets non anticipés, escalatoires et forcément déstabilisateurs. En effet, l'attribution présente toujours un risque d'erreur et il appartient aux seuls États de l'assumer. Ensuite, les actions conduites en représailles peuvent induire de sérieux risques de dommages collatéraux. Enfin, ces actions, souvent sur le territoire d'un État tiers, peuvent conduire ce dernier, considérant que sa souveraineté est mise en cause, à répliquer.

Solutions

Comme le souligne la Stratégie nationale française de cyberdéfense [3], il convient de « *promouvoir la prévention de l'utilisation de capacités cyber offensives par les acteurs non étatiques et soutenir l'interdiction pour les acteurs non étatiques de conduire des activités offensives dans le cyberespace pour eux-mêmes ou pour le compte d'autres acteurs non étatiques, sauf dans des cas très précis et à condition que les actions techniques envisageables dans ce contexte soient strictement encadrées. […] De telles règles sont à définir précisément sur le plan technique afin de tracer une ligne claire, contrôlable et acceptable par tous* ». L'enjeu est donc de clarifier ce qui relève de l'action offensive – laquelle devrait être prohibée pour les acteurs privés, en toutes circonstances – et ce qui relève de la cyberdéfense active légitime – laquelle pourrait être autorisée, sous réserve d'un encadrement adéquat. Des discussions ont déjà été organisées, à l'initiative de la France, dans le cadre du Forum global de l'OCDE sur la sécurité numérique pour la prospérité. Ces travaux, complexes, prendront du temps. Il importe qu'ils puissent associer le secteur privé.

La commercialisation d'outils, logiciels ou techniques susceptibles d'être détournés à des fins malveillantes doit être encadrée

Constat

Ces dernières années, on a assisté à une prolifération de logiciels intrusifs et destructifs, développés et vendus par des entreprises privées. Ces outils constituent de véritables armes numériques. La difficulté de juguler ce phénomène tient aux caractéristiques de ce marché et des produits qui s'y échangent dont la finalité, offensive ou défensive, n'est pas toujours facile à discerner. Les risques posés par la prolifération de tels outils font consensus au niveau international [4].

Un début de régulation a néanmoins pu intervenir avec l'intégration des logiciels d'intrusion et des moyens de cryptologie à la liste des biens à double usage de Wassenaar depuis 2013.

Solutions

Un travail de définition a été engagé et devra se poursuivre. Il s'agit par exemple de savoir précisément ce qui constitue un logiciel d'intrusion. Au-delà, la question se pose d'un régime

(3) Secrétariat général de la Défense et de la Sécurité nationale (2018), *Stratégie nationale de la Cyberdéfense*, Paris, Economica.

(4) Ainsi, les travaux du Groupe d'experts gouvernementaux (GGE) de l'ONU ont pu aboutir en 2015 à la conclusion que les États devraient prévenir la prolifération des techniques et des outils malveillants.

d'autorisation de commercialisation plus strict pour les outils dont le potentiel de destruction les apparente à des matériels de guerre.

Conclusion

La sécurité dans le cyberespace et la stabilité de ce dernier ne sauraient relever de la responsabilité des seuls États. Le concours du secteur privé est indispensable. S'il n'appartient pas à ce dernier de fixer les règles, il a un rôle essentiel à jouer, d'une part, en promouvant des bonnes pratiques qui ont vocation à devenir des normes et, d'autre part, en contribuant aux discussions préalables à l'adoption de nouvelles règles juridiquement contraignantes.

La forme que doit prendre cette régulation est aujourd'hui loin d'être arrêtée. Selon les cas, elle pourra relever de l'obligation ou de l'encouragement, en fonction de la nature de la responsabilité imputable à l'entreprise. La régulation devra ainsi concilier impératif de sécurité et protection de l'innovation mais aussi tenir compte du rôle et de la taille des acteurs concernés (les acteurs jouant un rôle systémique, étant amenés à assumer plus de responsabilités).

HORS DOSSIER

Concurrence et numérique : entretien avec Bernard Benhamou

Secrétaire général de l'Institut de la Souveraineté Numérique

Propos recueillis par Jean-Pierre Dardayrol et Delphine Mantienne

Enjeux numériques : Les différents marchés du numérique ont-ils un degré concurrentiel satisfaisant pour le bon fonctionnement des économies ? Évoluent-ils dans le bon sens ?

Bernard Benhamou : La réponse simple est « non » ! Il est évident que la situation actuelle est la preuve patente d'un défaut de prévision par rapport à la concurrence sur les grands acteurs du numérique – mais pas seulement. Il y a un défaut évident de prise en compte des réalités du marché. Je vous donne un exemple : celui de la régulation des télécoms, que j'ai eu à connaître puisque j'ai eu l'honneur de travailler longuement avec l'ancien patron de l'ART (future ARCEP), M. Jean-Michel Hubert, lui-même artisan du dégroupage de la boucle locale en France. Il aura fallu une volonté politique très forte, à l'époque, pour mettre en place ce dégroupage, qui était une mesure novatrice, enviée par de nombreux pays, et même étudiée aux États-Unis. Il se trouve qu'il y avait là un *projet* pour la régulation du secteur. Désormais, on a une ARCEP qui est censée réguler les « tuyaux », mais qui est en permanence en friction avec les grands acteurs, comme en témoignent les très nombreux conflits d'acteurs télécoms avec les acteurs GAFA (Free *vs* YouTube sur le *peering* et les tarifs d'interconnexion…). Je crois qu'il nous faudra envisager une refonte dans les temps à venir pour prendre en compte le nouveau paysage industriel et technologique dans lequel nous sommes entrés. On ne peut plus se limiter aux seules notions de couverture, de connectivité, certes importantes avec le déploiement de la 5G – et bientôt peut-être de la 6G **:** il est évident qu'il nous faut avoir une meilleure compréhension des mécanismes qui sont à l'œuvre en termes de capacité d'innovation, de modèle économique, de saturation du marché par certains acteurs. On n'a plus comme référentiel absolu le *prix*, qui était la donnée fondamentale en termes concurrentiel envisagée jusqu'à présent. Si le dégroupage de la boucle locale était un des leviers pour aboutir à un prix moins élevé pour le consommateur, aujourd'hui, face à des services internet massivement « gratuits », la notion de prix n'a plus le même sens et n'a plus le même caractère de « boussole » pour les acteurs de la régulation.

EN : Edward Snowden était très présent dans la presse ces derniers temps. Pour lui, la domination des GAFA n'a qu'une raison : l'absence de solutions alternatives.

BB : C'est vrai et faux. J'ai un immense respect pour Edward Snowden et je regrette infiniment que nos autorités n'aient jamais envisagé de lui donner le droit d'asile. Je pense effectivement qu'il y

a un problème d'alternatives mais plus généralement, il y a un problème de *politique industrielle*, ce terme ô combien essentiel qui a été tellement dévalorisé dans l'esprit de très nombreux responsables aujourd'hui. L'économiste Mariana Mazzucato disait que le secret le mieux gardé de l'État américain, c'est de voir à quel point il est *interventionniste* dans le domaine des technologies. Elle précisait même qu'il n'y a pas une seule innovation, depuis l'iPhone, l'IA, l'écran tactile, le WiFi et l'Internet lui-même… – en somme, toutes les grandes innovations auxquelles on fait référence quotidiennement avec les GAFA – qui n'ait été subventionnée massivement par les crédits fédéraux ou locaux des États-Unis. Par définition, je crois qu'il y a effectivement un problème d'alternatives et de place possible pour des alternatives – *locales*, comme le disait Snowden : on n'est pas forcé de faire des choses aussi grandes – mais je citerai aussi Tommaso Valletti, économiste en chef de la direction de la concurrence de la Commission européenne : « Facebook a induit la Commission européenne en erreur lors du rachat de WhatsApp… ». Parce que Facebook s'est présenté comme respectueuse du RGPD, et qu'elle devait assurer la séparation et de la non-communicabilité des données personnelles entre ces différentes plateformes, pour au final faire exactement le contraire… Le résultat est de rapprocher ainsi les services Facebook, Instagram et WhatsApp du tentaculaire service chinois WeChat. Cela nous rappelle ce qui s'était passé lorsque Microsoft avait été sommé de séparer Internet Explorer de Windows, et avait fait cette remarque extraordinaire aux responsables de la Commission européenne : « Nous n'avons plus le code que vous nous avez demandé. Ce code évolue tout le temps, nous ne l'avons plus… ». C'était une réponse inouïe, et cela revenait à intégrer les deux logiciels de manière telle que la séparation – structurelle ou fonctionnelle – apparaisse comme impossible.

Je précise que l'Europe a déjà eu l'occasion de faire valoir son « muscle » en termes de régulation antitrust au début des années 2000, lors du rapprochement prévu entre General Electrics/Honeywell qui aurait eu pour conséquence de créer un quasi-monopole sur les turbines d'avion. À l'époque, face à ces deux sociétés américaines, l'Europe avait empêché la fusion. Aujourd'hui, face aux acteurs technologiques, je ne perçois plus une volonté similaire dans ce domaine.

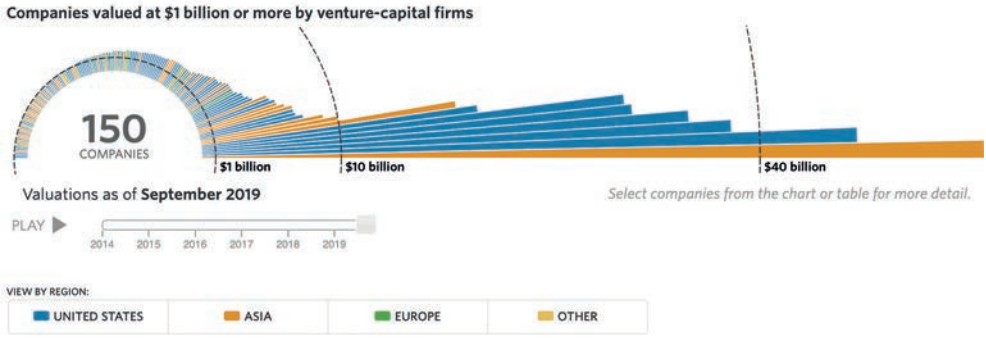
Je crois qu'en plus d'une absence de vision, on assiste à une forme de laisser-faire poussée à ses extrêmes, qui a mené les Européens à établir des monopoles de fait qui n'étaient en rien des monopoles naturels, ou réagir souvent trop tardivement à des abus de position dominante. Plutôt que d'agiter le marteau de la sanction *ex post*, qui requiert énormément de temps, je serais favorable, comme le réclament certains parlementaires, à ce que soient prises des mesures « conservatoires » qui empêcheraient ce type de fusions, avant même que les armées de juristes de ces sociétés n'aient épuisé toutes les voies de recours.

Là où les télécoms constituaient un marché qui s'était structuré sur plus d'une centaine d'années, la rapidité qui caractérise désormais les industries technologiques a pris de court une partie des observateurs et des régulateurs et n'a pas été analysée avec la lucidité qu'elle requérait pour que l'Europe ne soit pas placée dans une situation de vassalisation, jusqu'à devenir une « colonie numérique de deux autres continents », selon les termes de la sénatrice Catherine Morin-Desailly. Je fais partie de ceux qui pensent que ce n'était en rien une fatalité.

EN : Le droit de la concurrence et les procédures associées ont-ils la souplesse et l'adaptabilité requises pour répondre aux enjeux du numérique ?

BB : Je pense qu'il faut établir dans ces domaines des lois temporaires, se donner des possibilités de « revoyure » pour être en mesure d'adapter ces lois. Nous ne parlons pour l'instant que de capacités de concurrence industrielle, mais il y a d'autres questions qui concernent l'État en tant que régulateur ! Ce sont évidemment des questions de libertés publiques, de protection des citoyens, de protection des libertés, et on va bien au-delà de la vision des données personnelles que l'on avait il y a quelques années. On a maintenant une obligation de monter en puissance sur

la régulation comme sur la politique industrielle. Le cœur de mon propos aujourd'hui est le fait qu'il n'est de *régulation* que s'il y a une *stratégie*. Si notre régulation est de se conformer à la doxa anglo-saxonne du marché libre et non-faussé, cela ne fonctionne pas, cela ne permet pas de créer des alternatives. La preuve en est que nous Européens sommes encore à nous poser des questions sur le fait de comprendre pourquoi nous n'avons pas de licornes qui soient en mesure de devenir des acteurs de taille internationale.



Source : *Financial Times*

Vu notre puissance en termes de capacité de marché et l'excellence de notre recherche et de nos filières de formation, l'absence des pays européens dans les grands acronymes que l'on cite – les GAFA, les NATU ou les BATX –, n'est pas un fait lié au seul hasard du développement industriel. Le rapport Villani faisait ainsi état de l'excellence de la recherche française en matière d'intelligence artificielle, se réjouissant que M. Yann Le Cun soit le responsable de la recherche IA chez Facebook… De mon côté je ne saurais m'en réjouir, mais bien plutôt me désoler que l'on n'ait pas su retenir de retenir ces talents d'exception au sein d'entreprises européennes. Quand on voit ces entreprises (et ces fonds d'investissement) extra-européens qui viennent faire leur « shopping » auprès des PME ou les start-up, ou directement au CNRS ou plus précocement encore dans les écoles ou dans des laboratoires ; cela n'est pas arrivé par hasard : Le démantèlement de nos filières clefs, stratégiques dans ces domaines, le fait qu'il n'y ait pas un seul fabricant, aujourd'hui, de taille conséquente, de téléphones mobiles, le fait qu'on n'ait pas de plateformes, qu'il n'y ait pas d'OS européen, etc., c'était une chose qui n'était pas du tout inéluctable. Je crois que l'on a habillé *ex post* une forme de renoncement ou de molle résignation, en une forme d'inéluctabilité de l'évolution du paysage industriel dans ce domaine. Si l'on doit refonder le droit à la concurrence dans ces domaines, c'est en ayant clairement une ambition stratégique et politique.

Il s'agit aujourd'hui de se maintenir à égale distance des deux risques technologiques auxquels nos sociétés sont confrontées. Le premier est celui que l'universitaire américaine Soshana Zuboff [(1)] appelle le « capitalisme de surveillance » dans lequel les GAFA devenus « hyper-dépendants » aux données des usagers deviennent des instruments économiques au service d'une société qui réduit chaque jour le libre arbitre des individus-consommateurs. Le second volet de ce risque est la vision chinoise des technologies du Crédit social qui permettent de mettre en place la surveillance et la manipulation des individus à l'échelle du quart de l'humanité… Cette surveillance prend appui sur la notation du comportement de chaque individu, et lorsque cette note est trop basse, elle empêche les citoyens chinois d'accéder à toutes les libertés fondamentales, liberté de déplacement,

(1) Professeure émérite à la Harvard Business School et auteure de *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, 2019.

accès au crédit, accès à une promotion professionnelle. Or, ces deux anti-modèles technologiques et politiques sont déjà à l'œuvre et se renforcent l'un l'autre…

Par défaut de compréhension des mécanismes à l'œuvre, nos acteurs européens sont déjà confrontés à cette ubérisation. C'est vrai de la télévision (Canal+ diffusant Netflix), c'est vrai de la distribution (Monoprix et Amazon, Auchan…). Et cela pourrait aussi devenir le cas pour le secteur automobile. Ainsi, Dieter Zetsche, le PDG de Daimler, déclarait qu'une automobile devenait désormais « un smartphone avec quatre roues autour… ».

Face à ces évolutions technologiques, nous, Européens, avons non seulement vocation, mais aussi l'*ardente* nécessité de créer une troisième voie respectueuse des principes et valeurs des citoyens européens. Or, le problème est qu'à l'heure actuelle nous n'en prenons pas le chemin parce que l'effort politique nécessaire pour aider à redessiner ce paysage industriel est évidemment considérable. Mais à défaut c'est l'ubérisation progressive de l'ensemble de nos filières industrielles qui se mettra en place par un effet domino d'un secteur vers l'autre… les prochains secteurs visés pouvant être ceux de la banque, de l'assurance ou encore de la santé…avec des conséquences sociales et politiques encore plus importantes que par le passé.

EN : Les évolutions actuelles de la gouvernance et des réglementations du numérique en Europe (vie privée, sécurité, propriété intellectuelle, etc.) vont-elles avoir un effet significatif sur le caractère concurrentiel des marchés ?

BB : Oui, elles *ont eu* un effet significatif sur la structuration des marchés, sur le caractère concurrentiel. Le RGPD, par exemple (avec tout le respect que j'ai pour ce long travail), n'est qu'une première phase, c'est-à-dire que le RGPD a été conçu à une époque où les réseaux sociaux s'étaient développés, certes, mais pas autant, et à une époque où il n'y avait pas toutes sortes d'objets connectés : enceintes connectées, voiture connectée, maison connectée, bientôt vêtements, aliments, et même médicaments connectés… Les problématiques et l'accélération de l'effet de réseau que cela pose, sont désormais tout autres. Il faut des mises à jour de ces textes, à la fois le RGPD et le règlement e-Privacy, pour intégrer la régulation des nouvelles technologies de l'Internet des objets, qui représente encore l'un des angles morts de la régulation actuelle. J'ai par exemple eu l'occasion de plaider, lors des différentes réunions ministérielles européennes, pour un droit au « silence des puces », c'est-à-dire pour la capacité de déconnexion de chaque appareil, de chaque dispositif, par l'utilisateur, pour éviter qu'un appareil ne parle sans (ou contre) le consentement de son utilisateur. On en est très loin aujourd'hui, mais je pense qu'il faudra aller vers une préoccupation *by design* de l'architecture technologique des objets connectés, de manière à intégrer en amont la protection de la vie privée – et non pas attendre que des mastodontes produisent des technologies qui introduisent des effets pervers de façon systémique.

Il faudra aussi refonder les textes sur la concurrence, sur les politiques industrielles, sur le *Small business Act* (i.e. la capacité des administrations à orienter une partie de la commande publique vers de *petites* entreprises innovantes). Je pense qu'il est plus que jamais nécessaire de remettre sur la table cette mesure, souvent retoquée par le passé par nos partenaires européens (et en particulier britanniques). Il est en effet impératif que les PME aient d'emblée des clients solvables, pas seulement des financements aléatoires, pour être en mesure d'améliorer rapidement leurs produits et leurs services. Pour de nombreux juristes européens, le S*mall Business Act* pourrait même être déployé au niveau français pour les achats publics innovants sans contrevenir au droit européen.

EN : L'économie numérique ne connaît pas de frontières. Y a-t-il une gouvernance, une coopération et une convergence internationales satisfaisantes dans la définition et l'application des règles de concurrence ? Quels premiers pas pourrait-on faire ? Quelle serait la « bonne assiette » ? Géographique ? Géopolitique ?

BB : Nos autorités nationales sont légitimement sourcilleuses sur les questions de souveraineté et de défense. Étant fédéraliste, cela ne me choquerait pas qu'une politique européenne pour les technologies soit mise en place conjointement avec nos partenaires. Mais pas dans le périmètre actuel des pays de l'Union, et donc certainement pas à 27 mais plutôt à partir d'un noyau dur de pays européens. D'ailleurs, lorsqu'il a été question de remplacer le logiciel Palantir à la DGSI, il était question d'un projet *franco-allemand*. Je ne dis pas qu'à lui seul le moteur franco-allemand serait suffisant, mais je penche pour la théorie des cercles concentriques **:** les signataires initiaux du traité pourraient avoir des initiatives communes dans des secteurs stratégiques (santé, contrôle environnemental ou encore dans le domaine des transports).

Il s'agit de développer une politique industrielle à l'échelle européenne, et aussi d'établir d'autres mécanismes de financement que les PCRD… La préoccupation essentielle était alors de favoriser la montée en puissance des Licornes. Or, il n'y a pas de projets européens sur ces domaines qui aient abouti. La preuve en est : tous les leaders que nous avions dans ces secteurs ont été décapités. Il nous faut donc refonder les mécanismes de financement européens de l'innovation.

La fondation X-Prize, aux États-Unis, a eu l'occasion de créer un mode de financement innovant dans le domaine des technologies de la santé connectée. Il s'agissait de créer une technologie de diagnostic médical portable pour les non-professionnels. Ils ont appelé ce concours « Tricorder » (en référence à Star Trek). Le principe en était le suivant : « Nous voulons que cette technologie puisse exister, prouvez-nous que vous pouvez la mettre au point… et les gagnants se partageront 15 millions de dollars. » Au lieu de financements multiples qui souvent ne débouchent sur aucune percée technologique, il convient d'établir des mécanismes nouveaux, de mettre en place le ciblage de la commande publique vers les PME les plus innovantes et enfin d'établir des règles, y compris des mesures conservatoires, pour éviter les dérives des plus grandes entreprises… Il s'agit évidemment d'une forme de révolution culturelle pour les financeurs, mais aussi pour les acteurs publics et l'ensemble de l'écosystème technologique européen.

Je pense que nous avons une opportunité étrange, née des différents scandales (Snowden, Cambridge Analytica et autres), qui est liée au fait que l'on se rend compte que ce modèle économique centré sur les données personnelles et le micro-profilage (ou micro-targeting) est liberticide, économiquement prédateur et politiquement dangereux puisqu'il favorise des mouvements radicaux, populistes, etc. : je crois que l'Europe doit créer les technologies de la troisième voie, c'est-à-dire des technologies qui préservent la vie privée, notre vision de notre évolution démocratique. Il s'agit aussi de préserver de notre modèle européen de civilisation ! Je citerai d'ailleurs le patron des affaires juridiques de la Commission européenne Paul Nemitz : « La protection des données pourrait devenir une possibilité de rebond pour les industries européennes ». Même la très sévère revue du MIT disait il y a quelques mois que sur la protection de la vie privée et sur les technologies financières (*open-banking*), les Européens étaient les mieux placés. Pourquoi ? Parce que l'on a justement cet avantage lié à notre tradition dans ces domaines. Au lieu de le vivre cette protection des données personnelles comme des contraintes insurmontables, il faut la concevoir comme un levier pour les pays européens, une marque de fabrique, un label, qui pourrait effectivement aider à développer cette troisième voie en Europe.

EN : Comment la politique de la concurrence et celle de l'innovation pourraient-elles s'appuyer et s'enrichir mutuellement ?

BB : Lorsque l'on envisage les innovations technologiques on évoque souvent le mythe de l'entrepreneur solitaire et l'impression qu'elle vient uniquement de la sphère privée pour peu qu'elle dispose de financements (et de financeurs) adéquats. Or, c'est loin d'être entièrement vrai. Les acteurs publics jouent par exemple un rôle extraordinairement important dans l'écosystème technologique américain. Je pense que l'agence militaire américaine (DARPA, qui a financé les

premiers travaux de l'Internet) et les fonds d'investissement publics (comme In-Q-Tel, le fonds de la CIA qui a financé à son origine la société Palantir) est l'exemple même de structure que l'on aurait dû étudier plus attentivement en France et en Europe, et dont on ne s'est pas assez inspiré dans le passé. Je crois au rôle fondamental et structurant de la commande publique européenne nationale et aussi locale lorsqu'elle est encadrée par des textes qui mettent en œuvre une stratégie cohérente pour ces technologies.

EN : Quelles relations les politiques de souveraineté et de concurrence peuvent-elles entretenir ?

BB : Je dirais qu'il y a un champ passionnant qui est train de s'ouvrir, autour des nouvelles formes de régulation et de gouvernance des technologies. La situation était beaucoup plus simple avant l'émergence des grandes plateformes. Les enjeux sont devenus aujourd'hui infiniment plus complexes. Tous ceux qui travailleront sur ces questions auront des métiers passionnants, aussi bien dans l'entreprise que dans la sphère publique. Je crois qu'il y a une vraie plus-value liée à la réflexion dans ces domaines et au fait d'effectuer une veille stratégique fine sur les évolutions de ce que l'on nomme désormais les filières et les technologies de la souveraineté numérique (cybersécurité, technologies financières, énergie ou encore transports), sur ce que font nos homologues européens ou au-delà, dans ces domaines, pour imprimer une caractéristique européenne au droit de ces secteurs.

EN : Quelles lectures conseilleriez-vous à nos lecteurs sur ces sujets ?

BB : Je recommanderais 3 ouvrages parus ces derniers mois et qui analysent (chacun sous un angle différent) les évolutions actuelles du paysage économique et technologique ainsi que leurs conséquences politiques et sociales :

- *The Curse of Bigness : Antitrust in the New Gilded Age*, de Tim Wu ;
- *The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power,* de Shoshana Zuboff ;
- et enfin, *Future Politics. Living Together in a World Transformed by Tech,* de Jamie Susskind.

Vers une école du *risque numérique* ?

Par **Jean-François CÉCI**
Université de Pau

Denis Cristol (2014) définit ainsi l'*homo numericus,* cet acteur [1] des sociétés hyperconnectées qui « s'informe, joue et achète en ligne, fréquente des cybercafés, est victime de cyber-attaques, se fait voler son identité numérique, s'inscrit en masse sur des réseaux sociaux numériques, cherche un conjoint *via* Internet, signe des pétitions en ligne, partage de la musique et des photos, travaille à distance mais aussi apprend et enseigne en ligne ». *L'homo numericus* baigne donc dans un écosystème numérique capacitant [2] ses actes au quotidien. Au-delà de ce qui a été décrit de ses habitudes numériques, il pratique aussi la musique en ligne, la VoD [3], réalise ses formalités administratives à distance, gère son patrimoine numérique (ses photos et vidéos, ses papiers, ses livres…), voire vit son deuil en ligne [4] et se déconnecte de manière volontaire [5], tout en gérant (ou pas) les traces qu'il laisse au fil de ses errances physiques et numériques. Il s'agit là, bien entendu, d'une vision optimiste et chaque acteur est différent face au *pharmakon* [6] numérique, à la fois remède et poison, voire drogue. Nos sociétés hyperconnectées ne peuvent plus s'en passer, tant il rythme, outille, mesure, amplifie, égaie, connecte, mémorise le moindre instant de nos vies. Nous devons alors apprendre à vivre en symbiose avec et dans cet écosystème numérique, pour en annuler le poison, limiter la drogue et développer le remède. Cela commence manifestement par une éducation *au* numérique et *par* le numérique de qualité, dès les plus jeunes âges, dans une approche écologique respectueuse des divers stades de développement de l'individu. Nous proposons donc d'esquisser ce qu'on pourrait nommer une *culture numérique*, après avoir détaillé les principaux bienfaits, problèmes et risques alimentant les nombreuses controverses autour du numérique. Puis nous conclurons sur l'utilité d'une École introduisant cette culture numérique, et au-delà des apports positifs, d'une *École du risque numérique*.

Les bienfaits du Numérique

Notre expérience sensible au monde est vécue à travers l'usage de nos cinq sens, de manière analogique, selon des phénomènes continus dans le temps et l'espace. Dans ce monde-là, rien ne se perd, tout se transforme selon la loi de conservation de la masse et de l'énergie. Pourtant, dans l'écosystème numérique, la numérisation du signal est toujours affaire de compromis entre la

(1) Concernant l'écriture inclusive, nous invitons le lecteur à considérer que le masculin inclut le féminin et est utilisé sans discrimination.
(2) Au sens de Latour et de ses « objets actants » ou encore « capacitants », donnant un pouvoir d'action (Latour et Biezunski, 2010).
(3) VoD : de l'anglais *Video on demand*, ou vidéo à la demande, est un service proposé par les chaînes de TV (et fournisseurs comme Netflix), permettant de choisir le programme visualisé et de se libérer des contraintes horaires de sa diffusion programmée.
(4) Des sites comme http://www.votredeuilenligne.com/ proposent des « packs commémoratifs » pour permettre aux familles éparpillées d'« informer, partager, soutenir, témoigner, rappeler l'arbre généalogique… », autour d'un espace numérique commun. Il s'agit donc d'un mémorial numérique au défunt, mémorial dans les deux sens du terme : un écrit illustré pour garder le souvenir et un monument virtuel pour se recueillir.
(5) Jauréguiberry F. (2013), *Déconnexion volontaire aux technologies de l'information et de la communication*. https://hal.archives-ouvertes.fr/hal-00925309
(6) Bernard Stiegler définit ainsi le pharmakon : « C'est à la fois le remède et le poison selon Platon, lequel dit aussi que toute technique est un *pharmakon*, c'est-à-dire que toute technique peut servir soit à construire, à élaborer, à élever le monde, soit à le détruire (comme Oppenheimer l'a dit à propos de la bombe atomique, mais c'est vrai de n'importe quelle technique). » (Stiegler, 2007)

qualité du signal (donc de sa dégradation volontaire et de sa restitution, comme pour la musique ou la vidéo) et son poids numérique (en octet et ses dérivées, le kilo-octet, le méga-octet…). Qui dit poids numérique à la hausse, dit temps de transmission plus long, espace de stockage plus grand, temps de traitement allongé. Sur cette base, le quotidien des acteurs que nous sommes nous renseigne sur les bienfaits du numérique, quand le compromis est bien trouvé. Nous communiquons davantage, plus loin, plus vite, partout. Nous gagnons du temps, de l'argent et de l'espace de vie, tant les médias que nous utilisons le plus souvent se dématérialisent, et donc coûtent un peu moins tout en prenant moins de place sur nos étagères. Il en est ainsi de la musique, des livres et journaux, des films, etc. Notre patrimoine culturel tend à se « résumer » à une simple clé USB (ou à un espace de stockage en ligne), tant nos loisirs, souvenirs et papiers administratifs deviennent faciles à archiver et transmettre au format numérique. Au-delà du classique smartphone et d'Internet, le numérique est présent partout, dans tous les asservissements de machines, dans tous les automatismes. Il apporte de la sécurité et de la maniabilité dans tous nos véhicules (avions, voitures…), voire une conduite autonome [7]. La robotique profite largement du potentiel du numérique et la manutention de charges lourdes ou la réalisation des tâches domestiques seront bientôt confiées à des robots (Moley [8] est un robot chef-cuisinier pouvant préparer plus de deux mille plats). La biomécanique nous redonne une mobilité perdue *via* des prothèses (de jambes pour l'exemple) indétectables sous des vêtements, tant la démarche est naturelle [9]. Pour continuer dans le domaine de la médecine, des progrès considérables sont imputables au numérique : imagerie médicale, télémédecine, robots chirurgiens, etc. Le numérique contribue donc à sauver des vies ou à les prolonger, y compris au sein du corps humain *via* des implants (cardiaque, capteurs, caméra vidéo en capsule endoscopique, etc.).

Les domaines du loisir et de la culture profitent aussi de l'arrivée du Numérique [10] dans nos vies, en mettant à la portée de tous une infinité de supports, ressources et médias divers, permettant de développer facilement sa culture scientifique, littéraire, musicale, cinématographique, politique et autres, à l'envi. D'ailleurs, selon André Tricot [11], « la durée de lecture quotidienne est passée de 1 h 46 en 1972 à 4 h 30 en 2010, dont 30 mn de correspondance numérique, soit une progression de plus de 250 % » ! Nous n'avons donc jamais autant lu, en moyenne bien sûr. En simplifiant, nous pourrions y voir un gain potentiel dans le domaine de la culture et de l'apprentissage, imputable au Numérique. Nous pourrions continuer longtemps cette énumération des apports positifs du Numérique. En cela, il a gagné son droit à être qualifié d'évolution majeure, voire de révolution dans certains secteurs, dont la médecine. Mais toute médaille a son revers…

Les problèmes et risques du Numérique

Le Numérique apparaît à la fin du XX^{e} siècle, dans un monde hypermoderne, pollué et fortement basé sur la surconsommation de produits et d'énergies. Les inégalités de tous ordres sont importantes aussi bien pour l'accès aux études qu'au travail (fort taux de chômage [12]), et donc aux

(7) Voir cette vidéo de la Renault SYMBIOZ. Ce « démo car » donne un aperçu de l'automobile en 2023. *Auto Moto* la teste sur autoroute et lui fait même passer les péages en mode autonome
https://www.youtube.com/watch?v=WLjIsZMSQBQ
(8) Voir
https://www.youtube.com/watch?v=kjU8DLZY6xE&list=PLYb44pAPY8xgnITKU0R3kI9eXp0Evs8gJ&index=4&t=0s
(9) Voir la vidéo étonnante de Hugh Herr, l'homme « bionique » qui fait de l'escalade après avoir perdu ses deux jambes
https://www.youtube.com/watch?v=rEKe_SHtqaI
(10) Le numérique avec un « N » désigne la vision écosystémique de l'ère numérique dans laquelle nous vivons (le « faire société à l'ère numérique »), et renvoie aux concepts de culture numérique et de citoyenneté numérique. Il inclut aussi le numérique en tant qu'outil et support.
(11) Informations présentes sur sa projection lors d'une conférence au CANOPE de Montpellier, en 2017, page 11.
(12) La fin des années 1990 a vu un taux de chômage exceptionnellement haut, avec plus de 12 %
https://www.ladocumentationfrancaise.fr/dossiers/emploi/chiffres-cles.shtml

moyens financiers nécessaires pour assurer une « bonne vie » dans ce type de monde. Sans en être à l'origine, le Numérique hérite d'une part de ces maux de société, puisqu'en tant qu'écosystème, il accompagne nos vies. Alors, aux solutions qu'il apporte, s'ajoutent les problèmes physiques, écologiques, éthiques, institutionnels, politiques qu'il génère, par la transition qu'il impulse. En effet, comme toute technologie, le Numérique apporte son lot de risques, avec lesquels nous apprenons à vivre au quotidien, comme le décrit Ulrich Beck (2015) dans sa « société du risque », une société dans laquelle le risque devient partie intégrante de nous-même, et où aussi bien sa gestion que sa prévention deviennent une nécessité économique, sociale et politique. Prenons un exemple : la voiture a permis de se déplacer plus facilement, de trouver du travail dans un rayon plus large, de voyager, etc. Mais cette technologie a aussi apporté du risque dans notre société, à voir le nombre de morts sur les routes [13], la pollution dans les villes, l'encombrement des cités. À ce risque socialisé et conscientisé, est donc venue se greffer une politique nationale de cadrage et de prévention : permis de conduire, port de la ceinture obligatoire, gestion de la pollution par restrictions de circulation, mesures technologiques (pot catalytique, contrôle technique), diminution de la vitesse (80 km/h), contrôles de vitesse, etc. Nous utilisons nos véhicules au quotidien sans forcément penser à tout cela, car nous avons intégré et accepté ce risque d'accident et de pollution, contre service rendu. Il en est de même avec le Numérique pour lequel la société a intégré nombre d'usages socialisés, voire normalisés (*e.g.* l'email, les réseaux sociaux, la recherche d'informations, la consommation culturelle). Pour autant, comme phénomène récent et de dimension mondiale, il est loin d'être facile à encadrer et à intégrer socialement, tant les risques sont nombreux, pas forcément conscientisés, ni maîtrisés. Devrions-nous envisager une (auto-) école du (risque) numérique, pour former le citoyen et acteur numérique de demain à conduire et se conduire dans ce nouvel écosystème numérique ? Comme pour la conduite automobile, l'*homo numericus* devrait-il aussi passer son permis de conduire digital avant de trop s'élancer dans cet écosystème numérique, ne pas oublier de mettre sa ceinture de sécurité digitale, savoir entretenir son véhicule digital pour en assurer la sécurité et pour minimiser son empreinte écologique et personnelle, mais aussi, apprendre à ralentir dans cette société de l'accélération généralisée où l'urgence devient un symptôme [14] et le stress une maladie d'époque ? En ce qui concerne la conduite automobile, tout cela ne relève pas de l'autodidaxie et du libre arbitre ; alors il semble raisonnable de penser que l'intégration sociale du Numérique doive également être accompagnée, voire encadrée, autour d'une culture numérique nationale à constituer et à intégrer dans les programmes scolaires. Nous y reviendrons.

Voyons à présent les principaux risques auxquels l'humanité est confrontée avec les TIC [15], de manière croissante depuis plus d'une vingtaine d'années.

Les principaux risques en rapport avec la dimension socio-politique

- Surconsommation énergétique : les infrastructures d'Internet (*datacenters*, nœuds de réseau, serveurs…) consomment une importante part de l'énergie électrique mondiale (entre 6 et 10 % [16], quelle que soit leur utilisation.
- Carence en métaux rares : les appareils électroniques utilisent des métaux rares et précieux (graphite, cobalt, indium…), dont l'extraction est extrêmement polluante [17].

(13) En janvier 2019, selon l'Observatoire national interministériel de la Sécurité routière (ONISR), 238 personnes sont décédées et 5 036 personnes ont été blessées.
(14) Aubert N. (2014), *Le Culte de l'urgence : la société malade du temps,* Paris, Flammarion.
(15) TIC : technologies de l'information et de la communication.
(16) Voir cet article du CNRS
https://lejournal.cnrs.fr/articles/numerique-le-grand-gachis-energetique
(17) Voir le livre *La Guerre des métaux rares - La face cachée de la transition énergétique et numérique* de Guillaume Pitron.

- Pollution électronique (les matériels) : les appareils électroniques sont à obsolescence rapide, comme par exemple les smartphones que nous changeons « en moyenne tous les 2 ans, alors que dans 88 % des cas, ils sont encore en état de fonctionner [18] ». De plus, la majorité d'entre eux finissent dans un tiroir et ne sont pas recyclés. Enfin, le recyclage des appareils électroniques est coûteux.
- Taylorisation des emplois à l'extrême, automatisation : l'accélération généralisée et la course à la compétitivité engagent un élan de rentabilité et donc de délocalisation ou d'automatisation (robotisation) de l'emploi. Le Numérique déclasse certains métiers en facilitant cette automatisation. Le gouvernement prévoit que 15 % des salariés français pourraient en l'espèce être aujourd'hui remplacés par un robot [19]. Quoi qu'il en soit, il est évident pour tous que des métiers apparaissent [20] (les métiers de la cybersécurité par exemple, autour d'universités qui se spécialisent) et que d'autres disparaissent (tourneur, cordonnier…).
- Creusement des inégalités (d'accès aux matériels, réseaux et ressources) : est évoqué ici le coût des équipements et abonnements pour accéder au Numérique et aux formations nécessaires pour être un citoyen (de cet écosystème) numérique, cet *homo numericus* avec son *permis de conduire digital*.
- Ubérisation : la « destruction créatrice » de Joseph Schumpeter (1942) décrit la disparition de secteurs d'activités suite à l'apparition de nouvelles activités économiques. L'ubérisation est un néologisme pour décrire ce processus, en référence à l'entreprise Uber qui a organisé à l'échelle planétaire un service en ligne de voiturage avec chauffeur, en concurrence directe avec les taxis. L'ubérisation vient bouleverser la mise en relation client-fournisseur ainsi que la distribution des services, avec un coût de revient bien plus bas, rendu possible avec le Numérique.
- Facilitation du terrorisme, des trafics et de la dépravation : Internet est un fabuleux moyen de communication planétaire et instantané. Assez peu sécurisé dans sa version de base, il s'adjoint de techniques annexes pour frôler l'intraçabilité. Dès lors, avec un serveur proxy [21] et un navigateur comme Tor browser [22], n'importe qui peut devenir intraçable, voire accéder au dark web, cet Internet de l'illégalité non référencé par les moteurs de recherche sur lequel on trouverait de « tout » : des médicaments et substances illégales, ou des armes, jusqu'à la traite d'êtres humains, de services sexuels, d'organes et de « contrats » ou actes terroristes [23].
- Piratage informatique : il s'exerce à toutes les échelles, du petit pirate informatique, qui extorque (ou sextorque, puisque cela s'appelle la sextorsion) [24] quelques centaines d'euros à sa victime en lui faisant croire qu'il possède des enregistrements de sa webcam assez éloquents, jusqu'au

(18) Voir communiqué de l'ADEME
https://presse.ademe.fr/2017/09/smartphones-des-telephones-pas-si-smart-pour-lenvironnement.html?hilite=%27smartphone%27
(19) Voir « l'effet de l'automatisation sur l'emploi : ce que l'on sait et ce qu'on ignore »
https://www.strategie.gouv.fr/publications/leffet-de-lautomatisation-lemploi-quon-sait-quon-ignore
(20) Une longue liste de ces métiers du « futur » est disponible ici :
https://www.levif.be/actualite/sante/quels-metiers-vont-apparaitre-d-ici-2030/article-normal-362615.html?cookie_check=1551440077
(21) Un serveur proxy masque l'adresse Internet de l'internaute, en fournissant la sienne. Il sert d'intermédiaire et rend difficile le traçage.
(22) Tor browser est un navigateur basé sur un protocole intraçable Tor, utilisant un réseau de serveurs dédiés. Le principe de Tor est développé au milieu des années 1990 par l'armée américaine, dans le but de protéger les communications des écoutes et analyses de trafic.
https://www.torproject.org/projects/torbrowser.html.en
(23) Voir « Dans les coulisses du dark web » :
https://www.lesnumeriques.com/vie-du-net/dans-coulisses-dark-web-a3893.html
(24) Voir cet article sur la « sextorsion : comment vous prémunir d'un chantage à la webcam (faussement) piratée » :
https://www.cnetfrance.fr/news/sextorsion-comment-vous-premunir-d-un-chantage-a-la-webcam-faussement-piratee-39871971.htm

piratage de plus grande envergure visant une multinationale (Amazon par exemple) qui ne peut se permettre d'être « hors ligne » trop longtemps, tant le chiffre d'affaires à la minute est élevé [25]. Le piratage à visée politique est aussi connu pour manipuler les foules lors d'élections (*e.g.* Cambridge Analytica [26]). Enfin, les laboratoires de recherche appliquée, les agences de trading à haute fréquence, les banques, les services gouvernementaux, sont autant de cibles potentiellement intéressantes pour du piratage de haut vol et de l'espionnage industriel.

- Désinformation : l'arrivée du Web 2.0 au début du XXIe siècle a mis à la portée de tous un potentiel médiatique voisin des plus grands médias de l'époque : diffuser sur une échelle large (voire mondiale) de la vidéo, du son, de l'hypertexte. Dès lors, chaque individu internaute peut avoir sa chaîne de télévision, son journal en ligne, sa radio. D'une information publiée par une autorité reconnue, l'information provient de tous à présent et tout le monde en produit au quotidien, avec plus ou moins de justesse et de pertinence, voire avec des erreurs flagrantes [27], de la mauvaise foi et de la malveillance (les *fake news*). Il devient donc de plus en plus difficile de s'y retrouver et de qualifier une information, d'où l'apparition d'une nouvelle discipline scolaire et citoyenne, l'EMI : l'éducation aux médias et à Internet. Cette discipline s'insère progressivement dans le programme de formation du collège jusqu'à l'université et de nombreux enseignants en font leur cheval de bataille pour structurer leurs enseignements [28], montrant l'importance d'un permis de conduire digital, tout comme le baccalauréat est un permis d'étudier.

Les principaux risques en rapport avec la dimension sanitaire

- L'exposition aux ondes : l'humanité baigne dans une atmosphère d'ondes radios depuis le milieu du XXe siècle et l'avènement des radios libres, de la radio civile, de la radiotéléphonie, de la télévision, des satellites, etc. Or, les hyperfréquences émises par nos téléphones portables se rapprochent de celles utilisées dans nos fours à micro-ondes, dont la propriété est de provoquer un échauffement des cellules par agitation moléculaire, si la source est proche. Cet échauffement pourrait causer des tumeurs cancéreuses [29] chez les usagers intensifs de téléphones portables (lors d'appels surtout). L'Agence nationale de Sécurité sanitaire de l'Alimentation, de l'Environnement et du Travail reconnaît depuis le 27 mars 2018 les symptômes liés à l'électrohypersensibilité (EHS) [30], sans reconnaître un lien de causalité avec l'exposition aux ondes électromagnétiques. L'EHS [31] (la maladie) est donc reconnue et traitée, mais la cause n'est pas avérée. Cette même agence pointait déjà dans son rapport de 2016, concernant les enfants, « des effets possibles sur les fonctions cognitives et le bien-être », qui la

(25) Prenons l'exemple du chiffre d'affaires 2017 d'Amazon : 178 milliards de dollars, correspondent à 20,3 millions de dollars par heure, ou encore 339 000 $/min ou 5 640 $/s.

(26) Voir par exemple :
https://www.lemonde.fr/pixels/article/2018/03/18/comment-une-entreprise-proche-de-la-campagne-de-trump-a-siphonne-les-donnees-de-millions-d-utilisateurs-de-facebook_5272744_4408996.html

(27) Un exemple bien connu lors de la préparation au C2i (certificat informatique et Internet) : le site qui décrit le rond rouge :
http://site.ulco.free.fr/c2i/

(28) Comme en témoigne, dans Ouest France, Rachid Zerrouki, enseignant en Segpa à Marseille :
https://www.ouest-france.fr/medias/point-de-vue-que-peut-l-ecole-face-aux-fake-news-6237999

(29) Voir un rapide tour d'horizon de cette controverse dans la revue *Sciences et Avenir* :
https://www.sciencesetavenir.fr/sante/e-sante/les-ondes-des-portables-sont-elles-dangereuses_129232

(30) Voir les recommandations de l'agence Anses :
https://www.anses.fr/fr/content/hypersensibilit%C3%A9-aux-ondes-%C3%A9lectromagn%C3%A9tiques-amplifier-l%E2%80%99effort-de-recherche-et-adapter-la

(31) Les personnes atteintes de cette pathologie sont sensibles à l'exposition aux radiofréquences (entre autres) des téléphones portables, antennes relais et autre wifi. Les principaux symptômes reconnus sont : maux de tête, troubles du sommeil, nausées, irritabilité, fourmillements dans les doigts. Voir :
https://www.sciencesetavenir.fr/sante/electrosensibilite-que-dit-la-science_29437

conduisaient à préconiser « un usage modéré et encadré » de ces technologies [32]. La prudence est donc toujours de mise.

- Les troubles du sommeil : d'après une enquête réalisée dans un contexte pédagogique [33], 26 % des collégiens équipés de téléphones portables [34] le gardent allumé et connecté près d'eux la nuit, notamment car la moitié des parents des 8-13 ans ne cadrent pas la conservation du mobile dans la chambre la nuit. Alors que la quantité de sommeil recommandée [35] pour les 6 à 13 ans est de 9 h à 11 h, 17 % des CE2-CM2 s'endort après 22 h et 20 % des collégiens après 23 h en semaine, montrant un déficit de sommeil de 1 à 3 h par jour imputable en grande partie aux écrans (smartphone principalement). Sylvie Royant-Parola, docteur psychiatre spécialiste des troubles du sommeil, précise que « chez l'enfant, un déficit de sommeil peut entraîner des troubles de la croissance. Sur le plan cognitif, il peut perturber l'acquisition du langage. […] Autre conséquence : les troubles de l'attention. Les enfants sont alors soit fatigués, soit en état d'hyperactivité. Mais, dans les deux cas, ayant du mal à suivre en classe, ils peuvent rencontrer des difficultés scolaires [36] ».
- L'attention, ses troubles et son économie : comme évoqué, les troubles de l'attention sont souvent liés au manque de sommeil. Toujours selon Sylvie Royant-Parola : « Le manque de sommeil altère le cerveau des adolescents en diminuant le volume de matière grise. Avec des effets sur l'attention, la concentration et la capacité à réaliser des tâches simultanées. » Les troubles de l'attention pourraient donc être une conséquence du manque de sommeil, potentiellement générée par un usage tardif des écrans, tout comme l'hyperactivité précitée. L'attention, en elle-même, est un filtre permettant de se concentrer sur une tâche, y compris dans un environnement perturbateur. Selon Jean-Philippe Lachaux (2015), nos capacités attentionnelles s'affirment jusqu'à vingt ans, puis se stabilisent pour décliner après soixante ans, selon notre activité cérébrale. Nous devons donc apprivoiser et entraîner notre attention en résistant à ce qui peut la troubler (*e.g.* les notifications incessantes de nos smartphones peuvent provoquer des troubles de l'attention), et résister aux circuits faciles de la récompense par une orientation volontaire de l'attention. Il s'agit donc d'une capacité qui se développe, qui s'exerce et non pas d'un capital génétique déterminé. L'École doit-elle également accompagner le développement de cette capacité attentionnelle à l'ère de la distraction numérique ? Quoi qu'il en soit, une économie se développe autour de l'attention, l'économie de l'attention dans laquelle nous plongent malgré nous les TIC. En effet, les applis, les jeux, les sites Internet et réseaux sociaux utilisent de nombreuses stratégies pour nous rendre captif, nous retenir le plus longtemps possible, nous faire revenir souvent. Tristan Harris, ingénieur « philosophe produit » chez Google, va même jusqu'à dire que « des millions d'heures sont juste volées à la vie des gens [37] »et que « les entreprises de la Silicon Valley nous manipulent pour nous faire perdre le plus de temps possible dans leurs interfaces ». Yves Citton, professeur de littérature, adopte

(32) Rapport de l'Anses « Exposition des enfants aux radiofréquences : pour un usage modéré et encadré des technologies sans-fil » :
https://www.anses.fr/fr/content/exposition-des-enfants-aux-radiofr%C3%A9quences-pour-un-usage-mod%C3%A9r%C3%A9-et-encadr%C3%A9-des-technologies
(33) Voir cette enquête concernant 219 élèves de primaire et 407 élèves de lycées en 2015 :
http://sommeilenfant.reseau-morphee.fr/wp-content/uploads/sites/5/2018/08/synthese-enqueteecransetsommeiljda-v8-160312090506.pdf
(34) Selon cette enquête, 28 % des CM1-CM2 et jusqu'à 82 % des 6e-4e sont équipés de portables.
(35) Voir :
https://www.sleepfoundation.org/excessive-sleepiness/support/how-much-sleep-do-we-really-need
(36) Voir :
https://www.la-croix.com/Famille/Parents-et-enfants/enfants-besoin-regularite-2018-01-23-1200908168
(37) Voir :
https://www.nouvelobs.com/rue89/rue89-le-grand-entretien/20160604.RUE3072/tristan-harris-des-millions-d-heures-sont-juste-volees-a-la-vie-des-gens.html

un point de vue plus optimiste, car bien que militant pour que la « sur-sollicitation de notre attention devienne un problème à mettre au cœur de nos réflexions éthiques, de nos réformes pédagogiques et de nos luttes politiques », il ne voit pas le Numérique nous condamner « à une dissipation abrutissante ». Il pose pour cela « les fondements d'une écologie de l'attention », pour raison garder autour de la « suroccupation qui nous écrase » (Citton, 2014). Cette écologie de l'attention, à l'ère de la distraction numérique, pourrait venir compléter notre culture numérique nationale et figurer au rang des compétences à acquérir pour obtenir le permis de conduire digital.

- L'hyperconnexion, la déconnexion et le *burn out* : pour montrer le lien entre ces concepts et les définir, nous nous appuyons sur la recherche DEVOTIC coordonnée par Francis Jauréguiberry (2014). En ce qui concerne l'hyperconnexion, «il semble qu'une hyperconnexion aux TIC (c'est-à-dire le fait d'être toujours connecté) suscite en retour un désir de déconnexion. […] C'est parce qu'il y a trop de branchements, trop de connexions, trop d'interpellations, trop de simultanéité, trop de bruits et trop d'informations qu'un désir de déconnexion apparaît ». Parmi les principaux résultats obtenus autour de la déconnexion volontaire, celle-ci « relève alors d'une volonté de ne pas se laisser aspirer par un tourbillon non maîtrisé d'informations et de communications. […] La déconnexion apparaît presque toujours dans des situations de saturation, de trop-plein informationnel, de débordement cognitif, de harcèlement ou de surveillance, dans lesquelles l'individu se sent dépassé ou soumis. […] La déconnexion n'est jamais irréversible, mais toujours ponctuelle, partielle et située dans des contextes de saturation ou de débordement. Il ne s'agit pas de renoncer aux TIC, mais d'essayer d'en maîtriser l'usage en instaurant des coupures, des sas temporels, des mises à distance ». Enfin, quand la déconnexion échoue, et mène potentiellement à « des cas extrêmes de *burn out,* le rejet des TIC fait partie intégrante d'une attitude de défense ultime qui permet à l'individu de survivre quand il ne peut plus lutter. […] À l'image d'un disjoncteur qui saute lorsque l'intensité électrique devient trop importante, la déconnexion est ici purement réactive » (Jauréguiberry, 2013). En France, suite à la loi El Khomri du 8 août 2016 relative au travail [38], un droit à la déconnexion professionnelle du salarié est mis en place, précisant « la possibilité, en dehors de ses heures de travail, de se couper temporairement des outils numériques lui permettant d'être contacté dans un cadre professionnel (smartphone, Internet, email, etc.), selon des modalités définies à l'échelle de l'entreprise [39] ». Nous citons en exemple le cas de l'entreprise automobile Volkswagen, qui dès 2011, a imposé pour cela à ses salariés un blocage de leur boîte mail entre 18 h 15 et 7 h.
- L'addiction aux écrans : le Larousse médical définit l'addiction comme un « processus de dépendance plus ou moins aliénant à des toxiques ou à des comportements. L'addiction est un processus par lequel un comportement humain permet d'accéder au plaisir immédiat tout en réduisant une sensation de malaise interne. Il s'accompagne d'une impossibilité à contrôler ce comportement en dépit de la connaissance de ses conséquences négatives [40] ». La définition évoque alors les addictions bien connues comme l'alcool, le tabac, les stupéfiants et psychotropes ou encore l'alimentation. Puis est évoqué le « besoin irrépressible et excessif de comportements tels que le jeu pathologique (jeux d'argent et de hasard ou jeux vidéo), l'utilisation permanente de l'Internet ou du téléphone… ». Même les rapports sexuels ou les achats compulsifs peuvent relever de l'addiction selon cette définition. Nous voyons apparaître une distinction entre les addictions pharmacologiques (avec substances) et comportementales

(38) Voir :
https://droit-finances.commentcamarche.com/faq/52536-loi-el-khomri-loi-travail-ce-qui-change
(39) Voir :
https://droit-finances.commentcamarche.com/faq/56221-droit-a-la-deconnexion-definition-et-exemple
(40) Voir :
https://www.larousse.fr/encyclopedie/medical/addiction/185204

(sans substance), ces dernières étant dans notre registre d'étude ici. Selon le Collège universitaire national des Enseignants d'Addictologie, « les addictions comportementales se caractérisent par l'impossibilité de contrôler un comportement (*e.g.* pratique des jeux de hasard et d'argent ou des jeux vidéo, activités sexuelles, usage d'Internet, achats, exercice physique) et la poursuite de ce comportement malgré la survenue de conséquences négatives [41] ». Cependant, en dehors de la seule addiction aux jeux de hasard et d'argent *(gambling disorder)* aussi appelée « jeu pathologique » et reconnue officiellement dans les classifications internationales, pour les autres « selon les données scientifiques actuelles, des recherches sont encore nécessaires afin de déterminer si ces troubles peuvent véritablement être considérés comme des addictions, et si oui, quels en sont les critères diagnostiques » *(ibid.)*. L'enjeu tourne donc autour de la définition des critères diagnostiques pour voir si ces pratiques relèvent de l'addiction ou non. Plutôt que de parler d'addiction, Serge Tisseron préfère parler de « toxicité » du produit [42], du jeu, de l'écran, toxicité qu'il faudrait doser et indiquer plutôt que de parler d'addiction. De plus, comme aucun sevrage ni rechute n'est constatable autour des usagers pathologiques, il est difficile de parler d'addiction. Enfin, le psychologue fait la distinction biologique entre les circuits du plaisir et de l'addiction, ces derniers ne relevant pas des mêmes interactions hormonales. Le débat n'est pas tranché pour l'heure sur l'addictivité des écrans, d'Internet ou des jeux vidéo. Outre la controverse sur l'addiction ou la toxicité des TIC, les ressentis et représentations des utilisateurs sont intéressants sur ces questions : se sentent-ils addicts aux écrans ? D'après l'enquête Common Sense "Technology Addiction [43]", menée en 2016 auprès de 1 200 parents et leurs adolescents, 59 % des parents pensent que leurs adolescents sont addicts [44] à leur smartphone et 50 % de ces mêmes adolescents confirment ce ressenti. À l'inverse, 27 % des parents interrogés se sentent addicts à leurs smartphone, ce que confirment 28 % de leurs adolescents qui estiment leurs parents addicts. Il semblerait que le vécu familial soit suffisamment explicite pour que les représentations de l'addiction au smartphone soient ici bien partagées et précises. De plus, 66 % des parents pensent que leurs adolescents passent trop de temps sur leur mobile, ce qui est confirmé par 52 % des adolescents concernés. Cela crée d'ailleurs des disputes et tensions plusieurs fois par semaine (pour 43 %), voire journalières pour 36 %. L'addiction aux écrans apparaît donc comme un nouveau phénomène social autour de sensations et représentations personnelles et sociales, mais surtout autour de l'usage plus ou moins raisonné que nous faisons des écrans, et de la manière dont cet usage interfère avec notre entourage, donc est relatif au contexte.

Nous proposons de relativiser les effets délétères du Numérique et des écrans, évoqués ci-dessus, en rappelant que la plupart de ces risques sanitaires (comme le retard de sommeil et ses effets induits), peuvent être aussi imputés à des activités non numériques, comme la lecture de livres papier pour les lecteurs chevronnés, écouter ou jouer de la musique, peindre, dessiner ou encore pratiquer l'astronomie et en d'autres temps, le radio-amateurisme, le modélisme, etc. De tout temps et quelle que soit l'activité pratiquée avec passion, les heures ne sont pas comptées et cela peut se ressentir sur le sommeil, ou les relations avec autrui. Le Numérique offre donc une magnifique possibilité de se distraire et de « passer le temps », comme bien d'autres activités, mais à ne pas confondre et interpréter comme une injonction à surconsommer. Nous voyons donc plutôt cela comme une question d'usages, appelant à une « écologie » de ces usages, pour

(41) Voir :
http://www.cunea.fr/sites/default/files/ecn77.pdf
(42) Voir :
https://www.huffingtonpost.fr/serge-tisseron/jeux-video-addiction_b_5117191.html
(43) Common Sense. (2016), "Technology Addiction: Concern, Controversy, and Finding Balance" https://www.commonsensemedia.org/research/technology-addiction-concern-controversy-and-finding-balance
(44) Nous ne rentrons pas dans le débat de l'adéquation du mot « addict » : traduction libre du document d'enquête.

reprendre le terme d'Yves Citton, ce qui nous ramène aussi à leurs toxicités dans le regard de Serge Tisseron et à « l'étude philosophique du *pharmakon* » de Bernard Stiegler. Pratiquer cette écologie des usages en neutralisant la toxicité inhérente aux écrans et aux TIC nécessite une culture propice à cet écosystème numérique. C'est cette forme de culture-là (nous l'appellerons *culture numérique écologique*) qu'il serait sans doute utile de définir à l'échelle nationale et de partager entre citoyens numériques.

Une culture numérique écologique

Un pan de notre héritage culturel concerne ce nouveau compagnon de route qu'est le Numérique depuis environ vingt-cinq ans. Notre culture, au sens sociologique de « ce qui est commun à un groupe d'individus », s'en est donc enrichie et tout comme nous exprimons une culture musicale ou une culture artistique, nous pouvons à présent parler de l'émergence d'une culture numérique française (et mondiale). En première approche, « la culture numérique serait donc l'intégration dans la culture, liée au développement des techniques numériques, de changements potentiels ou effectifs dans les registres relationnels, sociaux, identitaires, informationnels et professionnels. Elle se rapproche de la culture informationnelle car elle repose sur l'échange d'informations. Elle s'en distingue car son centre n'est pas l'information mais le réseau social et l'individu qui échange cette information » (Devauchelle, Platteaux et Cerisier, 2009). Dix ans plus tard pour Dominique Cardon (2019), directement sur la première de couverture de son dernier livre pour en montrer toute l'importance, « si nous fabriquons le numérique, il nous fabrique aussi. Voilà pourquoi il est indispensable que nous nous forgions une culture numérique ». Nous comprenons l'imparfait de l'indicatif final comme une incitation à forger une culture qui n'existe pas encore, ou en devenir. Une culture semble émerger sous nos yeux, la culture numérique. Nous la qualifierons d'écologique, autour d'une nouvelle manière de faire société dans cet écosystème numérique hyperconnecté, au sein duquel nous devons redécouvrir l'humain et ses besoins de déconnexion, d'introspection, de réflexion, de temps longs. Nous devons apprendre à couper momentanément « les ponts » dans un monde où « la permanence du lien à l'autre est désormais la norme [(45)] », même en mobilité. Cette culture numérique écologique est constituée de nombreuses prises de conscience et de bien davantage : « savoir parler aux machines et les comprendre, savoir interagir avec le monde à travers elles (ouvrir une fenêtre sur le monde), savoir se développer et apprendre tout au long de sa vie, être un citoyen numérique responsable et apte à protéger sa vie numérique et son patrimoine numérique. Vivre cette culture numérique écologique consiste aussi à prendre le meilleur des deux mondes [(46)], et à coexister de manière équilibrée entre un univers physique tangible, aléatoire, analogique, complexe et un écosystème numérique algorithmique, adaptatif, douillet et prévisible… pour *in fine,* réapprendre à nous retrouver avec nous-mêmes et vivre en harmonie avec les autres dans un monde connecté » (Céci, 2019A).

Une citoyenneté numérique

La citoyenneté est la « situation des personnes à qui on a, dans un État, reconnu la plénitude de leurs droits civiques [(47)] » ; elle s'exerce pleinement chez l'individu à la majorité, par la responsabilité

(45) Jauréguiberry F. et Lachance J. (2016), *Le Voyageur hypermoderne*, Érès.
(46) Même s'il est de bon ton d'adhérer à une vaste communauté scientifique affirmant que l'écosystème numérique et le monde physique ne font qu'un seul et même monde, nous pensons qu'une dualité existe dans la présence cognitive et physique que nous y accordons. Ne pouvant être actif dans l'un et l'autre en même temps (comme poster une actualité sur Facebook en conduisant), nous devons faire le choix d'agir dans l'un ou dans l'autre. Cela nous laisse à penser qu'il n'est pas aberrant ici de parler de deux mondes.
(47) Tiré de la définition du *Larousse*.

de ses actes et de ses choix, ainsi que l'accomplissement des devoirs inhérents (travail, impôts, vote, défense, justice...). « Être citoyen, en 2018, c'est nécessairement exercer ce rôle en prenant en compte le numérique, qu'on y soit acteur ou non. L'école n'a donc d'autre choix que de former des hommes et des femmes qui sauront relever les défis de cette ère numérique » (Petit, 2018). La citoyenneté s'exerce autour d'une culture commune et d'un territoire. Nous parlerons donc de *citoyenneté numérique* pour faire référence à une citoyenneté, qui s'exerce dans un État où une culture numérique nationale est partagée. Pour que la société « élabore » le citoyen numérique de demain, cet *homo numericus* habile avec les technologies et apte à exercer sa citoyenneté numérique, le préalable est de définir cette culture numérique commune et former les futurs citoyens pour qu'ils l'adoptent et l'intègrent dans leurs droits et devoirs, ainsi que dans leur mode de vie.

À défaut, la jeunesse se construit dorénavant *via* une seconde naissance « par le numérique » à l'adolescence, puis se constitue son propre *habitus* numérique, sans sédimenter les notions nécessaires à la citoyenneté dont il est question ici, ou encore en faisant abstraction de certaines réalités sociales nécessitant un encadrement sociétal et scolaire adéquat. Le quart de vie numérique [(48)] des jeunes appelle donc à être encadré *a minima,* pour les aider à s'épanouir dans un monde de plus en plus connecté.

Vers une école du risque numérique ?

Pour vivre pleinement sa citoyenneté numérique, le citoyen doit être en capacité d'intégrer cette culture numérique commune, une fois celle-ci définie. Cela passe logiquement par de la formation continue pour les citoyens actuels, et par l'École pour les citoyens du futur, de manière continue et transversale [(49)], tout comme le français est pratiqué dans toutes les matières. Une fois formés à l'école des bienfaits et risques numériques, les néo-citoyens du futur pourront alors passer leur permis de conduire digital et s'élancer en toute sécurité sur les routes et autoroutes de l'information, avec le véhicule digital correspondant à ce permis [(50)].

Reste à définir cette culture numérique commune, la plus écologique [(51)] possible et nous conclurons par la vision englobante du Conseil de l'Europe pour qui la citoyenneté numérique « désigne le maniement efficace et positif des technologies numériques (créer, travailler, partager, établir des relations sociales, rechercher, jouer, communiquer et apprendre), la participation active et responsable (valeurs, aptitudes, attitudes, connaissances) aux communautés (locales, nationales, mondiales) à tous les niveaux (politique, économique, social, culturel et interculturel), l'engagement dans un double processus d'apprentissage tout au long de la vie (dans des structures formelles, informelles et non formelles) et la défense continue de la dignité humaine [(52)] ». L'enjeu à

(48) « Les jeunes de notre étude passent en moyenne 5h40/jour sur écrans. Cela représente 2 060 h/an en moyenne ou encore 90 jours. Autrement dit, ces jeunes passent en moyenne un quart de leur vie sur écrans. Une année scolaire équivaut à environ 1 000 h de cours, valeur variable suivant le niveau scolaire. Chaque année, ces jeunes passent donc deux fois plus de temps sur leurs écrans qu'à l'école.» (Céci, 2019B).

(49) Une enquête menée sur Pau en 2017, auprès de 5 établissements, avec un total de 792 répondants élèves de la 6e à M2 (en classe complète) et 153 enseignants des mêmes classes, montre que « l'intégration pédagogique du numérique à l'École est globalement faible » (Céci, 2019B).

(50) Pix est un service public en ligne, « créé pour répondre à ce défi de société. Sa mission est d'amener chacun d'entre nous à cultiver ses compétences numériques et à valoriser ses acquis, et ce tout au long de sa vie ». En cela, il amène un début de réponses aux problématiques évoquées. Voir : https://pix.fr/

(51) Écologique, au sens donné au paragraphe 4, c'est-à-dire la plus respectueuse possible de l'être humain et de son humanité.

(52) La citoyenneté numérique, Conseil de l'Europe :
https://www.coe.int/fr/web/digital-citizenship-education/digital-citizenship-and-digital-citizenship-education

venir est donc bien de définir cette culture numérique nationale et de former le citoyen numérique de demain, pour qu'il soit pleinement usager du potentiel et conscient des risques, à la fois de l'écosystème numérique et du monde dans lesquels nous vivons à présent.

Bibliographie

AUBERT N. (2014), *Le Culte de l'urgence: la société malade du temps,* Paris, Flammarion.

BECK U. (2015), *La Société du risque: sur la voie d'une autre modernité,* Paris, Flammarion.

CARDON D. (2019), *Culture numérique,* Sciences Po.

CÉCI J.-F. (2019A), « Apprentissage du et par le numérique : la formation des jeunes générations à un juste usage du numérique », *Annales des Mines, Enjeux numériques* n°6
http://www.annales.org/enjeux-numeriques/2019/resumes/juin/15-en-resum-FR-AN-juin-2019.html#15FR

CÉCI J.-F. (2019B), « Analyse des pratiques numériques des enseignants, du collège à l'université, au prisme du genre », IJARTech (International Journal of Applied Research and Technology)
https://hal.archives-ouvertes.fr/hal-01994895

CITTON Y. (2014), *Pour une écologie de l'attention,* Seuil.

COMMON SENSE (2016), *Technology Addiction: Concern, Controversy, and Finding Balance*
https://www.commonsensemedia.org/research/technology-addiction-concern-controversy-and-finding-balance

CRISTOL D. (2014), *Former, se former et apprendre à l'*ère numérique *: le social learning,* Issy-les-Moulineaux, ESF.

DEVAUCHELLE B., PLATTEAUX H. & CERISIER J.-F. (2009), « Culture informationnelle, culture numérique, tensions et relations », *Les Cahiers du numérique,* 5(3), pp. 51-69.

JAURÉGUIBERRY F. (2013), « Déconnexion volontaire aux technologies de l'information et de la communication », rapport ANR DEVOTIC : https://hal.archives-ouvertes.fr/hal-00925309

JAURÉGUIBERRY F. (2014), « Présentation », *Réseaux,* n°186(4), pp. 9-13.

JAURÉGUIBERRY F. & LACHANCE J. (2016), *Le Voyageur hypermoderne*, Érès.

LACHAUX J.-P. (2015), *Le Cerveau funambule : Comprendre et apprivoiser son attention grâce aux neurosciences,* Paris, Odile Jacob.

LATOUR B. & BIEZUNSKI M. (2010*), La Science en action : introduction à la sociologie des sciences,* Paris, Découverte/Poche.

PETIT B. (2018), *Construire sa citoyenneté à l'*ère numérique*,* Éducation Canada
https://www.edcan.ca/articles/construire-sa-citoyennete-a-lere-numerique/?lang=fr

SCHUMPETER J. (1942), *Capitalisme, socialisme et démocratie*
http://www.ecoleliberte.fr/wp-content/uploads/2016/05/Schumpeter.pdf

STIEGLER B. (2007), « Questions de pharmacologie générale. Il n'y a pas de simple *pharmakon* », *Psychotropes,* vol. 13(3), pp. 27-54.

Résumés

06 Le modèle français de cybersécurité : priorité à la défense

Guillaume POUPARD

Alors que la cybersécurité est désormais une priorité stratégique pour de nombreux Etats, la France continue de faire entendre une voix indépendante et équilibrée à l'international. Cela tient principalement à son modèle de cybersécurité, qui sépare strictement les activités cyber offensives et les activités de sécurité numérique, largement confiées à l'agence nationale de la sécurité des systèmes d'information (ANSSI). Interministériel et protecteur, ce modèle original a permis l'élaboration de législations ambitieuses et la construction d'une politique publique de cybersécurité globale, au profit des administrations, des entreprises et aussi des citoyens. Depuis dix ans, face à une menace numérique qui n'a cessé de croître et de se diversifier, face aux stratégies offensives et parfois hégémoniques des puissances cyber de ce monde, le modèle français a démontré toute sa pertinence. Il s'agit aujourd'hui de tirer pleinement parti des opportunités qu'il offre, notamment en structurant enfin un écosystème français de la cybersécurité pour associer l'ensemble des architectes de la société numérique.

11 La cybersécurité sort (enfin) de son ghetto technique

Nicolas ARPAGIAN

La consumérisation des outils de piratage a accompagné l'intensification des usages numériques. Dès lors que les technologies de l'information sont de plus en plus utilisées pour créer, valoriser, stocker et partager des données, les capacités de cyberattaques ont suivi la même progression. En se banalisant, ces outils malveillants ont des effets bien au-delà de la communauté des seuls techniciens de l'informatique. Juristes, investisseurs, analystes financiers… : ils sont de plus en plus nombreux à demander des comptes quant au niveau de protection. Cette diffusion dans toutes les strates des organisations publiques et privées s'explique en outre par une dépendance accrue à la disponibilité des données et des systèmes d'informations. Charge ensuite aux consommateurs et aux commanditaires de faire leurs choix de prestataires ou de technologies en prenant en compte, ou pas, les exigences de la cybersécurité... qui génèrent naturellement des coûts et des contraintes supplémentaires. Ces choix techniques doivent être éclairés par les obligations juridiques toujours croissantes, les dépenses nouvelles et les processus induits par une indispensable qualification des informations produites et de ceux qui peuvent y accéder et les manipuler. Une refonte managériale et stratégique qui va donc bien au-delà de la seule mise en conformité à des règles sécuritaires.

18 Que cherchent les hackers ?

Julie GOMMES

Les hackers, peu importe leurs capacités techniques ou leur âge, vont avant tout agir non pas selon leur profil, mais bien en fonction d'objectifs qui peuvent varier selon les groupes auxquels on s'intéresse. Toutefois, il n'est pas exclu que ces groupes, parfois très éloignés en termes de motivations, se rassemblent au hasard d'une opération, un schéma auquel on assiste de plus en plus souvent.

25 La sensibilisation : une arme défensive majeure
Jérôme NOTIN

Lors de nos usages quotidiens des outils numériques, dans notre environnement personnel comme dans le cadre professionnel, nous sommes en permanence confrontés à de la cybermalveillance. Pour nous en prémunir, deux piliers complémentaires doivent être construits : les outils techniques de protection et la sensibilisation de chacun. Quel est le dispositif construit par le gouvernement pour, entre autres, porter des actions de sensibilisation à grande échelle ? Quelles sont les cibles de choix des cybercriminels ? Pourquoi la sensibilisation est-elle nécessaire ?

29 Cyberdéfense : l'humain au cœur de l'efficacité opérationnelle. Mettre à l'épreuve son dispositif de défense est indispensable pour progresser
Vincent RIOU

Pour améliorer sa défense face aux cybermenaces, est-il opportun de continuellement augmenter ses dépenses en empilant des solutions vendues comme « miracles » dans son infrastructure informatique ? Pas si sûr… Dans un contexte de cyberguerre totalement asymétrique, il convient de replacer l'humain au cœur du dispositif de cybersécurité : mise à l'épreuve par des opérations de *Red Teaming*, entraînement régulier des équipes opérationnelles et managériales, mise en place de stratégies déceptives visant à tromper l'ennemi, sensibilisation de l'ensemble du personnel. Connais ton ennemi et connais-toi toi-même… les bases de l'Art de la Guerre.

33 Prévenir et détecter
Jacques DE LA RIVIÈRE

L'hétérogénéité des systèmes d'information, la migration des données dans le *Cloud* ou encore le nomadisme sont autant de paramètres qui rendent difficile la définition du périmètre de protection des entreprises. À cela s'ajoute la professionnalisation de la cybercriminalité qui rend les menaces plus nombreuses et polymorphes. Dans cet environnement sinueux, et alors que les analystes des Centres d'Opérations de Sécurité (SOC) et experts de la sécurité du *Cloud* sont des denrées rares, il est logique de vouloir utiliser la technologie pour automatiser des tâches de détection, d'évaluation et de réponse. Plusieurs solutions se dessinent aujourd'hui, à la fois innovantes et complémentaires, mais chacune avec des limites : le SOAR (*Security Orchestration, Automation and Response*), la CTI (*Cyber Threat Intelligence*) et enfin l'intelligence artificielle et plus spécifiquement le *machine learning*.

38 Souveraineté numérique et sécurité nationale
Claire LANDAIS et Julien BARNU

Notre souveraineté numérique, autrement dit notre capacité à rester maîtres de nos choix et de nos valeurs dans une société numérisée, recouvre trois enjeux complémentaires :
• préserver les composantes traditionnelles de notre souveraineté, à une époque où le numérique tend à remettre en question les monopoles régaliens – ce qu'on pourrait appeler la « souveraineté à l'ère du numérique » ;
• disposer dans le cyberespace d'une capacité autonome d'appréciation, de décision et d'action : il s'agit ici d'une « souveraineté dans l'espace numérique » ;

• maîtriser nos réseaux, nos communications électroniques et nos données, ce que l'on pourrait qualifier de « souveraineté sur les outils du numérique ».

42 Protection des infrastructures critiques : 5 ans après la loi

Yves VERHOEVEN

A partir de 2008, l'Etat français a anticipé l'aggravation du risque lié aux cyberattaques contre les opérateurs, publics et privés, d'infrastructures critiques pour la défense et la sécurité nationale, l'économie et la société. Afin de limiter ce risque, des démarches d'assistance ont été entreprises par l'Etat vis-à-vis des opérateurs les plus critiques. Néanmoins, face à l'ampleur des travaux à mener, l'Etat a dû mettre en place, *via* la loi de programmation militaire de 2013, un cadre réglementaire pour imposer un niveau minimum de cybersécurité sur l'ensemble des systèmes d'information critiques pour la défense et la sécurité nationale. La mise en œuvre de cette réglementation a fait de la France un pays pionnier en matière de cybersécurité des infrastructures critiques. Cette réglementation innovante a en outre permis des développements internationaux multiples, notamment en inspirant la directive 2016/1148 de l'Union européenne (dite « directive NIS ») concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

47 Retour sur la genèse de la cyberdéfense militaire

Didier TISSEYRE

Depuis 2011, le ministère de la Défense, puis des Armées, et en particulier le Commandement de la cyberdéfense, son bras armé, construisent un modèle agile et efficace de cyberdéfense pour conduire des opérations dans un nouvel espace de confrontation. Aujourd'hui, la plupart des luttes de pouvoir, des crises et des conflits contemporains connaissent un développement dans l'espace numérique. Les armées doivent appréhender le combat cybernétique comme une fonction stratégique à part entière dont les effets se combinent aux autres dans une manœuvre globale. Le combat dans le cyberespace est de nature asymétrique, hybride, parfois invisible et en apparence indolore. Pourtant, l'emploi de l'arme cyber est susceptible de porter gravement atteinte aux capacités et aux intérêts souverains des États. Pour protéger, défendre et agir face à ces cyber-menaces, la cyberdéfense française s'est construite grâce à la volonté gouvernementale et à sa prise en compte dans les lois de programmation militaire successives. Confrontée à des adversaires, des ennemis, ou des concurrents dotés de capacités informatiques offensives, la France a bénéficié d'un ambitieux plan d'actions ministériel, fondé sur une doctrine et une organisation renouvelées, permettant à nos forces de se déployer et de conduire, face à cette menace, le combat numérique. Cette montée en puissance franchit une étape majeure en 2017 avec la création, par décret, du Commandement de la cyberdéfense (COMCYBER). La cyberdéfense demeure une priorité très forte du ministère des Armées avec l'ambition de donner à la France les moyens de construire un outil à la hauteur de ses ambitions opérationnelles et d'assurer pleinement sa cybersécurité. L'inauguration par la Ministre des Armées le 3 octobre dernier à Rennes du premier bâtiment entièrement dédié à la conduite des opérations cyber, témoigne de cette dynamique qui permet à la France de rayonner et lui confère un statut de cyber-puissance.

52 Nouveaux rôle et enjeux pour l'Etat dans la lutte contre la cybercriminalité
Thierry DELVILLE

L'innovation a toujours profité aux criminels avant même de toucher le grand public. La digitalisation de la société que nous vivons depuis ces dernières décennies n'échappe pas à cette règle et les cybercriminels bénéficient d'un contexte très favorable pour commettre leurs méfaits. La course aux textes pour adapter le droit au numérique et incriminer des pratiques souvent nouvelles, l'insuffisante harmonisation du droit sur le plan international, la difficulté persistante à mesurer le phénomène et donc à le connaître …tels sont quelques-uns des enjeux auxquels doit faire face l'Etat pour relever le défi de mieux lutter contre une délinquance qui opère sa propre révolution numérique. A ces difficultés, s'ajoutent des questions de coordination et de dialogue étroits entre les acteurs étatiques et privés, tant la cybercriminalité se situe au croisement des enjeux de souveraineté, de protection économique, de renseignement et de défense nationale. Assurer la sécurité et la justice dans l'espace cyber apparaît plus que jamais l'occasion de penser autrement la mobilisation de la société en matière de prévention, de détection et de répression d'agissements de plus en plus lourds sur la vie quotidienne des Français.

57 À la poursuite des cybercriminels
Jacques MARTINON

Le cybercriminel a pour caractéristique singulière de s'adapter en temps réel aux évolutions de l'environnement numérique, afin d'en exploiter les failles techniques et de détourner les nouveaux usages légitimes en opportunité d'obfuscation voire d'ingénierie sociale au détriment des victimes. Il bénéficie de plus d'un écosystème criminel en voie de professionnalisation (*Cybercrime as a Service*) facilitant grandement la logistique et la diversification des cyberattaques, dont les modèles économiques sont parfois extrêmement travaillés (par exemple, les rançongiciels). Symétriquement, les acteurs judiciaires de lutte contre la cybercriminalité doivent adapter rapidement leurs stratégies, méthodes et organisations afin d'améliorer leur efficacité. La France n'a initié véritablement ce mouvement qu'en 2015, dans les suites du rapport de référence sur la cybercriminalité, *Protéger les internautes*, élaboré sous l'égide du procureur général Marc Robert. Des progrès indéniables ont été réalisés, mais la poursuite de ces efforts est essentielle afin de consacrer un véritable levier judiciaire redouté par les cybercriminels et activable dans le champ de la cyberdéfense.

63 Innovation et startups cybersécurité en France : le début de l'embellie ?
Gérôme BILLOIS et Jules HADDAD

La menace cybersécurité évolue rapidement et avec la tension que connaît actuellement le marché des compétences en cybersécurité, les actions manuelles doivent petit à petit laisser place à l'automatisation. Cette nécessité d'innover favorise la création de startups dans le domaine de la cybersécurité à l'échelle internationale. Cette année montre un écosystème de plus en plus dynamique avec de la croissance et des signaux positifs pour sa transformation. Ces signaux s'observent chez les clients qui commencent à prendre des risques, pour le marché qui se déverrouille en termes d'investissement et pour les startups qui sont de plus en plus innovantes et se penchent sur des sujets pertinents. Cependant, ces startups font face à des challenges comme les difficultés à recruter, le manque de prise de risque, ou une stratégie marketing peu efficace qui se répercute sur leur capacité à vendre. Finalement cette transformation de l'écosystème peut se concrétiser si tous les acteurs se

mobilisent : les startups doivent apprendre à se vendre, les clients doivent être enclins à prendre des risques et le marché doit favoriser le développement de ces jeunes pousses.

71 Le RGPD au service de la cybersécurité

Par Jean LESSI

Que ce soit pour les personnes physiques ou pour les organismes privés et publics comme pour la société dans son ensemble, la mise en application du Règlement général pour la protection des données (RGPD) représente un indéniable renforcement de l'ambition de sécurisation des données personnelles. Comment ? Par la mise en place de procédures spécifiques à respecter par les organismes en matière de sécurité de leurs données (notification à l'autorité de contrôle, information des personnes), en complément de l'ancienne obligation de sécurité remontant à 1978, dans un contexte de sanctions renforcées en cas de violation de ses principes. Et au-delà de ce qui est prévu dans le texte, par ses effets induits en termes de sensibilisation accrue du public à la protection des données et d'éducation au numérique), le RGPD doit nous conduire à nous donner les moyens de cette ambition.

75 Une agence au cœur de la cybersécurité européenne

Par Jean-Baptiste DEMAISON

Alors que la plupart des États membres ne disposaient pas encore d'agence dédiée aux enjeux de cybersécurité, l'Union européenne a créé l'ENISA (*European Network and Information Security Agency*) en 2004. Chargée, en particulier, de soutenir le développement des capacités de cybersécurité des États, l'agence a vu son champ de compétence grandir avec le développement d'un cadre européen de régulation de plus en plus ambitieux, consacré en 2013 par l'adoption d'une stratégie européenne de cybersécurité. Quinze ans après la création de l'ENISA, le règlement *Cybersecurity Act* a confirmé son caractère incontournable et renforcé ses missions au-travers de la création d'un cadre, unique au monde, de certification de sécurité numérique en Europe. Une nouvelle ère, pour une nouvelle agence. Toutefois, des défis demeurent : quel modèle pour le passage à l'échelle de l'action de l'UE en matière de cybersécurité ? Quelle prochaine législation pour une Europe numérique plus sûre ? Quel rôle pour l'ENISA face à la multiplication des initiatives cyber sectorielles ?

80 Le cyber en assurance, un risque presque comme les autres ?

Benjamin DUCOS et Luc DE LIGNIÈRES

Le marché de l'assurance cyber est encore une niche à l'échelle mondiale. Mais soutenu par les nouveaux usages, la réglementation et des incidents cybers de plus en plus fréquents, ce marché est désormais en croissance significative. Face à la demande de couvertures solides, les assureurs doivent structurer des contrats de qualité disposant de haut niveau de garanties : la modélisation des risques, le savoir-faire actuariel et la connaissance fine du risque cyber sont quelques-uns des atouts des grands assureurs mondiaux. Mais l'assurance cyber présente également des particularités techniques notables… En outre, les assureurs doivent se protéger contre ce risque cyber qui ne connaît pas de frontières, et qui pourrait avoir sur eux un effet incapacitant.

88 Défis de la recherche scientifique en cybersécurité
Claude KIRCHNER et Ludovic MÉ

Sécuriser un système d'information, c'est assurer la confidentialité, l'intégrité et la disponibilité des ressources qui y sont stockées et des services qui y sont offerts. A cette fin, on doit à la fois protéger ces ressources et services, mais aussi détecter d'éventuelles attaques et y réagir efficacement. Si la sécurité des systèmes et la protection des données personnelles ont globalement progressé durant ces vingt dernières années, beaucoup reste à faire, tant dans la mise en œuvre opérationnelle que dans les phases amonts de recherche et développement. Dans cet article, nous nous intéressons aux défis de recherche scientifique que lancent la protection de nos systèmes d'information, la détection des attaques contre ces systèmes et la réaction à ces attaques, sans oublier les défis liés à la connaissance de la menace, à la sécurité de certains domaines particulièrement sensibles, ou aux aspects humains, économiques et sociétaux de la sécurité.

100 La confiance numérique, une condition *sine qua non* du succès de l'adoption du *cloud*
Marc DARMON et Olivier KERMAGORET

Le *cloud* est un élément central dans la mise en œuvre d'une trajectoire de transformation numérique. Il apporte des avantages de compétitivité, de *time to market* et de scalabilité à grande échelle, conditions indispensables aux solutions d'IA, de Big Data, d'IOT et de DevSecOps inhérentes aux SI d'aujourd'hui. L'adoption du *cloud* est donc une réalité. 40 % des SI d'entreprises sont déployés sur des solutions de *cloud* privées et publiques avec un rythme de croissance de déploiement de 31 %. L'adoption de ces technologies doit aller de pair avec une stratégie globale de sécurisation de la donnée, nouvel or noir du XXIe siècle. En effet, il n'y a pas de solution numérique sans confiance et il ne peut y avoir de confiance sans cybersécurité. Les réponses sont multiples et reposent en premier lieu sur des architectures hybrides privées et publiques capables de fournir une solution aux différentes classifications de données, aux contraintes légales de type RGPD et au *Cloud Act*. Ces solutions doivent aussi inclure des dispositifs techniques comme la gestion des identités dans un environnement MultiCloud, le chiffrement de données, les architectures de sécurité virtuelles et la maîtrise de la résilience des systèmes. Enfin, l'accompagnement en termes de services managés pour assurer la réversibilité, le niveau de qualité et de maintien en condition de sécurité liés à l'utilisation du *cloud*, se révèle central dans le déploiement de cette stratégie.

106 L'Internet des Objets modifie la cybersécurité : l'exemple de Linky
Hervé CHAMPENOIS

L'installation de 35 millions de compteurs Linky par Enedis s'inscrit dans un mouvement plus large de développement de l'internet des objets (IoT). Celui-ci s'explique par les nouveaux services qu'apporte l'IoT aux consommateurs et aux entreprises. Dans le cas de Linky, ces services sont multiples, au bénéfice des clients et de la transition énergétique. Cette dynamique soulève de nouveaux enjeux en matière de cybersécurité. La multiplication des objets connectés reliés à des systèmes centralisés conduit à multiplier le nombre de points d'entrée potentiels dans les systèmes des entreprises et des administrations. Pour répondre à ces enjeux, nous identifions trois axes : une approche *security by design* qui implique de penser la sécurité dès la conception de l'objet connecté ; la supervision de ces objets tout au long de leur vie ; et la collaboration étroite entre toutes les parties prenantes de la cybersécurité.

110 Quelle régulation pour les acteurs privés dans le cyberespace ?
Par Florian ESCUDIÉ

L'essor du numérique comme nouvel espace de confrontation confère au secteur privé, notamment à un certains nombres d'acteurs systémiques, un rôle critique et une responsabilité inédite dans la préservation de la paix et de la sécurité nationale. Perçue jusqu'à récemment comme relevant de la responsabilité des seuls Etats, la sécurité dans le cyberespace et la stabilité de ce dernier sont désormais largement vues comme un enjeu concernant directement les acteurs privés. Il existe ainsi aujourd'hui une demande croissante de clarification des obligations incombant aux acteurs non étatiques dans le cyberespace. Lancé en novembre 2018 à l'initiative de la France, l'Appel de Paris pour la confiance et la sécurité dans le cyberespace identifie plusieurs axes en vue d'une meilleure régulation du rôle de ces acteurs. Il s'agit notamment de lutter contre la prolifération des programmes et techniques cyber malveillants, d'accroître la sécurité des produits et services numériques ou encore d'interdire le cyber-mercenariat et les actions offensives conduites par des acteurs non-étatiques. Des travaux sont actuellement conduits dans différentes enceintes, telles que l'OCDE, pour approfondir les modalités d'une régulation efficace à cet égard.

HORS DOSSIER

115 Concurrence et numérique. Entretien avec Bernard Benhamou, Secrétaire général de l'Institut de la Souveraineté numérique
Propos recueillis par Jean-Pierre Dardayrol et Delphine Mantienne

La concurrence dans l'économie numérique et l'application du droit de la concurrence aux différents secteurs de l'économie numérique sont deux sujets qui connaissent un regain d'intérêt en Europe et aux États-Unis, qu'il s'agisse de questions générales (effets économiques des oligopoles du secteur numérique, effets de la numérisation des entreprises) ou de la situation concurrentielle des différents segments du secteur numérique. Aujourd'hui, on entend deux musiques différentes et parfois dissonantes, l'une mettant en avant le caractère satisfaisant de la situation présente, l'autre les évolutions préoccupantes résultant de la limitation de la concurrence dans le secteur et les effets induits négatifs sur l'ensemble de l'économie. Nous avons interrogé Bernard Benhamou sur sa vision de la situation actuelle, des évolutions récentes, et sur les actions qui lui paraîtraient utiles, tant en matière de droit de la concurrence qu'en ce qui concerne l'articulation de la politique de la concurrence avec d'autres politiques majeures.

121 Vers une école du *risque numérique* ?
Jean-François CÉCI

Nous proposons d'esquisser l'émergence d'une *culture numérique*, au prisme des principaux bienfaits, problèmes et risques alimentant les nombreuses controverses autour du numérique. L'individu vit dorénavant dans une société et un monde connectés : cela nous renvoie-t-il vers une forme de *citoyenneté numérique* ? La citoyenneté et l'École étant intimement liées, avons-nous l'utilité d'une École introduisant cette culture numérique, et au-delà des apports positifs, d'une École du *risque numérique* ?

Abstracts

06 The French model of cybersecurity: Priority for defense
Guillaume POUPARD

Whereas cybersecurity is now a strategic priority for several countries, France's point of view is independent and balanced mainly because of its cybersecurity model, which makes a clear separation between two sorts of activities: on the one hand, cyberoffensives and, on the other, security in digital technology. The latter is mostly entrusted to ANSSI, the national security agency of information systems. This original, interministerial model of protection has enabled the country to draft ambitious laws and public policies about global cybersecurity in behalf of public administrations, firms and citizens. By coping with an ever increasing number of ever more variable digital threats and with the offensive, sometimes hegemonic strategies of the world's cyberpowers, this model has, for ten years now, proved pertinent. We must take advantage of the opportunities it provides by forming a French ecosystem of cybersecurity that will associate all architects of the digital society.

11 Cybersecurity (finally) leaves its technical ghetto
Nicolas ARPAGIAN

Piracy weapons are being commodified like consumer goods as digital technology is more intensely put to use. Once information technology increasingly serves to produce, enhance, store and share data, the risks of cyberattacks increase just as much. By becoming more common, malware of all sorts has effects far beyond the community of computer engineers. Ever more legal experts, investors, financial analysts… are demanding accountancy in matters of protection. Spreading through all layers of private and public organizations, this demand stems from our growing dependency on data and information systems being available. It is up to consumers and procurement services to choose their providers of technology and digital services by taking into account cybersecurity requirements, which obviously add to costs and come with drawbacks. These technical choices must be based on information about the growing number of legal obligations and about the expenses and processes necessary for evaluating the information produced and deciding who may have access to data and use them. This managerial and strategic overhaul leads us far beyond the simple question of compliance with security rules.

18 What are hackers looking for?
Julie GOMMES

Regardless of their technical capacities or age, hackers mainly undertake actions as a function not of their profiles but of their objectives, which vary depending on the group. Let us not forget, however, that these groups, despite sometimes quite different motivations, can come together at random for an operation, a pattern we ever more often come across.

25 Awareness, a major weapon of defense
Jérôme NOTIN

During our everyday uses of digital technology in our personal and occupational environments, we are constantly faced with cyberactions motivated by criminal intent. To protect ourselves,

two complementary pillars have to be set up: the technical tools for protection and the awareness of each and everyone. What is the government doing to raise awareness on a large scale? What targets do cybercriminals choose? Why is awareness necessary?

29 Cyberdefense: The human factor at the center of operational efficiency — testing defenses is indispensable for making progress
Vincent RIOU

To improve our defenses and cope with cybermenaces, is it worthwhile to continually lay out more funds while piling up solutions sold as "miracles" for the computerized infrastructure? Of course not. In a context of totally asymmetrical cyberwarfare, the human factor should be placed back at the center of cybersecurity arrangements: testing operations by red teams, training operational and managerial teams, adopting misleading strategies to deceive the enemy, raising the personnel's awareness of cyberthreats…. Know your enemy and know yourself — the very basis of the art of warfare.

33 Preventing and detecting
Jacques DE LA RIVIÈRE

The heterogeneity of information systems, the migration of data toward the cloud and nomadism make it hard for firms to define their perimeter of protection. Added to this is the professionalization of cybercriminality with more numerous and variegated menaces. In this sinuous environment — a context where the analysts of centers of security operations and the experts in cloud security are scarce resources — it is logical to want to use technology to automate the tasks of detection, evaluation and response. Several solutions are arising, both innovative and complementary but each with its limitations: security orchestration, automation and response (SOAR), cyberthreat intelligence (CTI) and artificial intelligence, specifically machine learning.

38 Digital sovereignty and national security
Claire LANDAIS & Julien BARNU

Our digital sovereignty — our capacity for remaining the master of our choices and values in a digitized society — has three complementary aspects. First of all, preserve the traditional constituents of sovereignty during an era when digital technology tends to undermine state monopolies: what might be called "sovereignty during the digital era". Secondly, have in cyberspace an autonomous capacity for making evaluations, decisions and launching actions: "sovereignty in digital space". Thirdly, control our networks, electronic communications and data, which could be described as "sovereignty over digital tools".

42 Protecting critical infrastructures: Five years after an act of law
Yves VERHOEVEN

As of 2008, the French government was aware of the growing risks of cyberattacks against the public and private operators and infrastructures that are critical for our society, economy and national defense and security. To limit these risks, state authorities offered assistance to firms, in particular those in the most critical fields. Given the scope of what was to be done however, the state set up, under a military program act in 2013, a regulatory framework for imposing a minimum level of cybersecurity on all information systems critical to national

defense and security. Implementing this regulation has made France a pioneer in the cybersecurity of critical infrastructures. This innovative form of regulation has had several international developments. It has inspired the EU's Directive on the Security of Network and Information Systems with its measures for a high joint level of security for networks and information systems in the European Union.

47 A review of the origins of cyberdefense in France
Didier TISSEYRE

Since 2011, the Ministry of Defense and the Armed Forces (in particular its armed wing, the Cyberdefense Command) has built an agile, efficient model of defense for conducting operations in the new battle space of the digital realm, where most power struggles, crises and conflicts now have an extension. The armed forces must realize that cybercombat is a full-fledged strategic function that is to be combined with other global maneuvers. Combat in cyberspace is inherently asymmetrical, mixed, sometimes invisible and apparently painless. Nevertheless, cyberweapons can seriously damage the capacities and interests of sovereign nation-states. To protect, defend and act when faced with such menaces, the government's determination and the passage of successive program acts for the armed forces have enabled France to build up its cyberdefenses. Faced with adversaries, enemies, or rivals equipped with an offensive capacity in information systems, France's ambitious plan of ministerial actions, based on a new doctrine and organization, enables our forces to be deployed and conduct digital combat. This was taken a step farther in 2017 with the creation, by decree, of COMCYBER, the Cyberdefense Command. Cyberdefense is still a top priority for the Ministry of the Armed Forces, the goal being to endow France with the means for building a tool on par with its operational ambitions and to fully ensure the country's cybersecurity. On 3 October 2019, the Ministry of the Armed Forces inaugurated in Rennes the first building fully devoted to cyberoperations, this being evidence of a trend that will enable France to stand out thanks to its status as a cyberpower.

52 The fight against cybercriminality: The state's new role and the issues
Thierry DELVILLE

Innovations have always benefitted criminals before reaching the public. The digitization of society during the past decades is no exception to this: the context is propitious for cybercriminals to benefit from the offenses they commit. The race to adapt the law to digital technology and incriminate new behaviors, an insufficient international harmonization of the law, the persistent difficulty of gauging and knowing the phenomenon…these are a few of the issues that the government must address to fight more effectively against a delinquency that is undergoing its own digital revolution. Added to these difficulties are questions about closer coordination and dialog between state authorities and private parties. Cybercriminality raises the stakes related to sovereignty, economic protection, intelligence and national defense. Seeing to security and justice in cyberspace is more than ever the occasion to rethink how to mobilize society so as to prevent, detect and repress actions that weigh ever more heavily on our fellow citizens' everyday lives.

57 In pursuit of cybercriminals
Jacques MARTINON

What characterizes cybercriminals is their adaptation in real time to changes in the digital environment so as to take advantages of technical flaws and turn legitimate uses into an

opportunity for obfuscation or even social engineering to the detriment of their victims. They also benefit from a criminal ecosystem that, by becoming professional (cybercrime as a service), very much facilitates the logistics and diversification of cyberattacks. Some attacks have extremely well-crafted business models (*e.g.*, ransomware). In parallel, judicial authorities must quickly adapt their strategies, methods and organization in order to fight more effectively against cybercriminality. France did not really begin its own adaptation till 2015 following a landmark report on protecting cybernauts from cybercriminality. Despite the undeniable progress, it is necessary to pursue these efforts and hone judicial tools that, dreaded by cybercriminals, can be put to use for the purpose of cyberdefense.

63 Innovation and startups in cybersecurity in France: The upturn?
Gérôme BILLOIS & Jules HADDAD

Cybersecurity menaces are evolving fast, the labor market for skills in cybersecurity is now tense, and manual interventions must gradually be replaced with automation. This need for innovations is stimulating the formation of startups in cybersecurity on the international scale. We now observe an ever growing ecosystem and positive signs of its transformation: clients are now willing to take more risks; the market is increasingly investment-friendly; and startups are ever more innovative. However startups face problems: difficulties with recruiting, the lack of risk-taking, or their not very efficient marketing strategies with repercussions on their sales. If all parties become active, this transformation can be realized: startups must learn to sell; clients, to take risks; and the market, to stimulate the growth of startups.

71 The EU's General Data Protection Regulation at the service of cybersecurity
Jean LESSI

Whether for physical persons, private and public organizations, or society as a whole, the application of the EU's General Data Protection Regulation (GDPR) definitely expresses the determination to make personal data secure. How? By establishing specific procedures that data security organizations have to follow (notifying regulatory authorities, informing individuals), by completing the security obligations instituted in 1978, and by more heavily sanctioning violations. Beyond its provisions, the GDPR has spinoffs: a rising public awareness of data protection and of the need for digital literacy. Now to provide the means for achieving the GDPR's ambitions…

75 An agency at the heart of European cybersecurity
Jean-Baptiste DEMAISON

Whereas most EU member states have not yet set up a cybersecurity agency, the European Union founded the European Network and Information Security Agency in 2004. In charge of developing the capacity of member states in cybersecurity, ENISA's scope of action has been broadened under a more ambitious EU framework regulation that led to the adoption in 2013 of a European cybersecurity strategy. Fifteen years after ENISA's creation, the Cybersecurity Act has confirmed this agency's indispensable role and bolstered its assignments by setting up a system, unique in the world, for certifying cybersecurity in Europe. A new era is opening for an agency with new duties. Nonetheless, questions are still standing. What model to follow to upgrade EU actions in cybersecurity? What is the next legislative step for more digital security in Europe? How should ENISA respond to the many initiatives being undertaken in several sectors?

80 Cyberinsurance, a risk nearly like the others?
Benjamin DUCOS & Luc DE LIGNIÈRES

"Cyberinsurance" is still a niche market worldwide. Given new uses, regulations, and ever more frequent incidents, this market is growing strongly. To respond to the demand for solid coverage, insurance companies must draft quality contracts with high guarantees. Among the assets of the big, global insurance firms are their actuarial know-how, granular knowledge of cyberrisks and the models of risks they have built… but cyberinsurance has noteworthy technical particularities. Furthermore, insurers must protect themselves against cyberrisks, which ignore borders and could incapacitate them.

88 Scientific research in cybersecurity
Claude KIRCHNER & Ludovic MÉ

Making information systems secure means ensuring the confidentiality, integrity and availability of the system's resources and services. Both resources and services must be protected; eventual attacks, detected; and efficient actions, undertaken. While global progress has been made in the security of information systems and the protection of personal data during the past twenty years, much is yet to be done, both in operations and upstream in research and development. This article focuses on scientific research related to the protection of information systems, the detection of attacks against them and the reaction to these attacks. It does not fail to mention the challenges related to: security in certain very sensitive domains; the human, societal and economic aspects of cybersecurity; and our knowledge of these menaces.

100 Digital confidence, indispensable for the cloud's success
Marc DARMON & Olivier KERMAGORET

The cloud, a key element in the digital transition, brings competitive advantages, thus improving time-to-market and scalability on a large scale. These conditions are indispensable to artificial intelligence, big data, the Internet of things and the DevSecOps inherent in contemporary information systems. The cloud has, in fact, been adopted: 40% of corporate information systems rely on a cloud, and the pace of growth is strong. The adoption of cloud technology must be coupled with a global strategy for making data (the new black gold) secure. There will be no "digital solution" without confidence; and no confidence, without cybersecurity. The many responses to this situation depend on the architecture's (mixed, private, public) capability of finding solutions for various classes of data and in compliance with legal requirements (as under the Cloud Act and the EU's GDPR). Technical arrangements are also necessary, such as the management of identifications in a multicloud environment, data encryption, virtual architectures of security and control of the system's resilience. Managed services must also be provided for reversibility, quality and maintenance of security. This followup turns out to be the key to deploying a cloud strategy.

106 The Internet of things modifies cybersecurity: The example of Linky
Hervé CHAMPENOIS

The installation in France of 35 million smart electricity meters (Linky) by Enedis is part of a broader trend toward the Internet of things (IoT), which will bring new services to

consumers and firms and, in the case of Linky, for the energy transition. This trend raises new cybersecurity issues. The proliferation of the devices connected to centralized systems is going to multiply the number of potential points of entry into the information systems of firms and public administrations. Three axes are examined for finding solutions: a security-by-design approach, which implies overhauling security from the phase of design of connected devices; the supervision of these devices throughout their life cycle; and close collaboration between all stakeholders in cybersecurity.

110 Regulations for private actors in cyberspace?

Florian ESCUDIÉ

As a new space for conflicts, digital technology confers on the private sector (in particular, certain systemic actors) a critical role and an unprecedented responsibility for peace-keeping and national security. Perceived till recently as the responsibility of nation-states alone, cybersecurity and a stable order in cyberspace are now widely perceived to be issues that directly concern private actors, whence a growing demand for clarifying their obligations. In November 2018, France launched an appeal for developing confidence and security in cyberspace that identifies several axes for better regulating the role of private actors. The principal intent is to fight against the proliferation of programs and techniques with criminal intent, to increase the security of digital products and services, and to forbid offensive actions undertaken by private actors and the use of mercenaries. Work is under way in various settings, for instance the OECD, to work out efficient regulations on this topic.

Miscellany

115 Competition and digital technology

Bernard BENHAMOU, secretary-general of the Institut de la Souveraineté numérique, interviewed by Jean-Pierre DARDAYROL & Delphine MANTIENNE

Competition in the digital economy and the application of competition law in various sectors of this economy are two topics that have aroused interest in Europe and the United States: both in general (questions about the economic effects of oligopolies in the digital economy and the impact of digitization on firms) or in particular (questions about the competitive situation of segments in the digital economy). Two dissonant voices are heard, the one satisfied with the current situation, the other worried about the trends stemming from a limitation of competition in certain segments and the negative side-effects on the whole economy. Bernard Benhamou has been asked about his views on the current situation and recent trends, and about the actions that he deems useful in relation to competition law and to the articulation of competition policy with other major policies.

121 Toward a school of digital risks?

Jean-François CÉCI

The emergence of a "digital culture" is described in terms of its major benefits, problems and risks, which fuel several controversies. The individual now lives in a "connected" society and world. Does this lead to a form of "digital citizenship"? Since citizenship is closely related to the educational system, are our schools capable of introducing this digital culture, not just its positive aspects but also the related risks?

Ont contribué à ce numéro

Nicolas ARPAGIAN est Directeur de la Stratégie et des Affaires publiques d'Orange Cyberdefense (Groupe Orange). Il enseigne à l'Ecole Nationale Supérieure de la Police (ENSP) et intervient à l'Ecole Nationale de la Magistrature (ENM). Il est administrateur du GIP ACYMA qui gère la plateforme gouvernementale Cybermalveillance.gouv.fr, et membre du Conseil d'Orientation de l'Institut Diderot. Il a fondé et dirigé le Cycle « Sécurité Numérique » à l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ), établissement public placé auprès du Premier ministre. Nicolas Arpagian est l'auteur d'une vingtaine d'ouvrages/publications parmi lesquels : *Distortions, Rumours, Untruths, Misinformation and Smears* (2019, World Scientific, Singapour), *La Cybersécurité* (2018, Presses Universitaires de France, Collection Que Sais-Je ?), *Quelles menaces numériques dans un monde hyperconnecté* ? (2018, Institut Diderot), *Cyberguerre, longtemps annoncée, désormais r*éalité *? (2018, Rapport Ramsès, IFRI-Dunod), « Vers une cyberguerre froide entre Moscou, Washington… et la Silicon Valley* » (2017, *Revue des Deux Mondes*), « *Europe de la sécurité numérique :* très juridique, mais guère technologique, et encore insuffisamment économique » (2016, Réalités Industrielles), *Rapport moral sur l'argent dans le monde* (2016, AEF – Caisse des Dépôts et Consignations), *The Turn to infrastructure in Internet governance* (2016, Palgrave MacMillan US), *Observation : Pratique et Enjeux* (2015, Editions Omniscience), *Influentia* (2015, Editions Lavauzelle), *Sécurité privée, enjeu public* (2015, Editions Armand Colin), *L'*État, la Peur et le Citoyen – Du sentiment d'*insécurité à la marchandisation des risques* (2010, Editions Vuibert), *La Cyberguerre – La guerre numérique a commencé* (2009, Editions Vuibert), *Pour une stratégie globale de sécurité nationale* (2008, Editions Dalloz), *Liberté, Égalité… SECURITE* (2007, Éditions Dalloz).
→ ***La cybersécurité sort (enfin) de son ghetto technique***

Julien BARNU est un ancien élève de l'École polytechnique et ingénieur en chef des Mines. Il a rejoint en 2013 l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en tant que chef de projet, en charge de la politique de cybersécurité des activités d'importance vitale, puis en tant que directeur de cabinet du directeur général, Guillaume Poupard, de janvier 2016 à juillet 2018. Il assure depuis le 1er août 2018 la fonction de Conseiller industrie et numérique de la secrétaire générale de la défense et de la sécurité nationale, Madame Claire Landais.
→ ***Souveraineté numérique et sécurité nationale***

Bernard BENHAMOU est actuellement secrétaire général de l'Institut de la Souveraineté Numérique (ISN). Il est aussi enseignant sur la gouvernance de l'Internet à l'Université Paris I-Panthéon Sorbonne. Il a exercé les fonctions de délégué interministériel aux usages de l'Internet auprès du ministère de la Recherche et du ministère de l'Économie numérique (2007-2013). Il a coordonné la première conférence ministérielle européenne sur l'Internet des Objets lors de la Présidence française de l'Union européenne de 2008. Il a été le conseiller de la délégation française au Sommet des Nations unies sur la Société de l'Information (2003-2006). Il a aussi créé les premières conférences sur l'impact des technologies sur les administrations à l'ENA en 1998. Enfin, il a été le concepteur de « Passeport pour le Cybermonde », la première exposition entièrement en réseau créée à la Cité des Sciences et de l'Industrie en 1997.
→ ***Concurrence et numérique : entretien avec Bernard Benhamou***

Côme BERBAIN est directeur de l'innovation et du véhicule autonome à la RATP. Ingénieur du corps des Mines et docteur en cryptologie, son parcours alterne entre entités privées (Orange, Trusted Logic) et publiques (ministère de la Défense, Agence nationale de la sécurité des systèmes d'informations,

direction interministérielle du numérique) dans les domaines de la transformation numérique et de la cybersécurité. En 2017 et 2018, il est conseiller au cabinet du secrétaire d'Etat chargé du numérique où il porte les sujets de transformation numérique de l'Etat et de confiance numérique.
→ ***Introduction***

Gérôme BILLOIS est associé dans la practice cybersécurité et confiance numérique du cabinet Wavestone.
→ ***Innovation et startups cybersécurité en France : le début de l'embellie ?***

Jean-François CÉCI est enseignant en Humanités, culture et communication numérique à l'Université de Pau et des Pays de l'Adour. Praticien-chercheur, il expérimente les pédagogies actives, l'évaluation par les pairs et l'usage efficient du numérique éducatif. Il mène des recherches en sociologie du numérique et de l'éducation au sein du laboratoire Passages (UMR 5319). Il s'intéresse plus particulièrement à la transition de la forme scolaire à l'ère du numérique, du collège à l'université. Dans le milieu associatif pour la refondation de l'Ecole, il est administrateur à l'An@e (Association nationale des acteurs de l'école), éditrice du site http://www.educavox.fr. Comme directeur du service numérique, chargé de mission TICE puis conseiller numérique, il a participé à la vision stratégique et au pilotage politique et technique de son université, en matière de numérique éducatif.
→ ***Vers une école du* risque numérique *?***

Hervé CHAMPENOIS entre chez EDF GDF Services en 1991, puis devient chef de division études et travaux des réseaux électriques et gaziers dans la région de Lyon. En 1999, il rejoint l'agence d'Ajaccio d'EDF GDF en Corse en charge de l'exploitation des réseaux électriques, des interventions clientèles et des travaux. En 2002, il est nommé adjoint au directeur en charge de l'exploitation des réseaux électriques et gaz de Franche Comté. En 2005, il intègre EDF SEI en Guadeloupe comme directeur adjoint en charge du domaine financier et de la production (déconstruction de centrale, traitement des îles du Nord). Il devient directeur régional Bourgogne à ERDF en 2009 et met en place la nouvelle organisation d'ERDF en région. En 2014, il rejoint la Présidence d'Enedis (ex-ERDF) comme directeur de cabinet du Président durant quatre ans. Depuis septembre 2018, il est le directeur du Programme Linky.
→ ***L'Internet des Objets modifie la cybersécurité : l'exemple de Linky***

Marc DARMON est diplômé de l'école Polytechnique et de Telecom ParisTech. Il a débuté sa carrière chez Alcatel en 1988 et a occupé successivement les fonctions d'ingénieur d'études, de chef de service technique, de responsable lignes produits, et enfin de Directeur du département Réseaux. Il rejoint le groupe Thales en 1998, au sein de l'entité Thales Communications, en tant que Directeur du Département « Réseaux d'Infrastructure ». En 2000, il devient Directeur Général de l'Unité « Réseaux » de Thales Communications. En 2002, il est nommé Vice President Strategy & Advanced Systems de Thales Communications. De 2004 à 2006, il occupe les fonctions de Directeur Général de l'Unité « Systèmes Interarmées » regroupant les domaines réseaux de communications et de radio/télédiffusion, les systèmes de commandement, renseignement et sécurité. De 2006 à 2008, Marc Darmon est Directeur Général de Thales Communications. En 2009, il devient Directeur Général Adjoint du groupe Thales, Directeur Général de la Division Naval de Thales. En 2010, Marc Darmon est nommé Senior Vice President, Directeur de l'Audit et du Contrôle Interne du Groupe Thales. Au 1er septembre 2012, Marc Darmon devient Senior Vice President, Systèmes C4I de Défense et Sécurité et, à ce titre, membre du Comité Exécutif de Thales. Il est, depuis 2013, Directeur général adjoint, Systèmes d'Information et de Communication Sécurisés de Thales. Marc Darmon est également, depuis septembre 2014, Président du Conseil des Industries de la Confiance et de la Sécurité (CICS), et, depuis 2018, Président du Comité

Stratégique de Filière « Industrie de Sécurité ».
→ ***La confiance numérique, une condition* sine qua non *du succès de l'adoption du* cloud**

Thierry DELVILLE est diplômé de l'Ecole Nationale Supérieure de Police (ENSP) de Lyon (1994), et ancien auditeur du National Executive Institute du FBI (Etats Unis). Après avoir été chef de Circonscriptions dans le Val d'Oise et en Seine Saint Denis jusqu'en 1998, il devient adjoint puis chef du bureau des systèmes d'informations et des télécommunications à la direction centrale de la Sécurité Publique (DCSP). En 2005, Thierry Delville est chargé de créer le Service des Technologies de la Sécurité Intérieure (STSI). Il contribue à ce titre au pilotage des grands projets technologiques (réseau Acropol, modernisation des centres d'information et de commandement), à la mise en place de partenariats et à développer l'implication de la Police Nationale dans la Recherche en sécurité. En 2009, il devient Directeur des services techniques et logistiques de la Préfecture de Police de Paris. En 2014, Thierry Delville devient Délégué ministériel aux industries de sécurité, puis par décret paru le 24 janvier 2017 voit ses attributions étendues avec la création de la délégation aux industries de sécurité et à la lutte contre les Cybermenaces. Depuis novembre 2018, Thierry Delville est associé au sein du cabinet PwC France où il est responsable du développement d'un pôle de cyber intelligence. Ce pôle réunit des expertises multiples afin de proposer une approche de sécurité globale aux entreprises. L'entité cyber intelligence de PwC France mobilise ainsi les compétences de plus de 150 experts en matière de cybersécurité, de sûreté, d'intelligence économique, de gestion de crise et investigations.
→ ***Nouveaux rôle et enjeux pour l'Etat dans la lutte contre la cybercriminalité***

Jean-Baptiste DEMAISON est président du conseil d'administration de l'ENISA depuis 2016, réélu à ce poste en octobre 2019. Préfigurateur d'une plateforme d'innovation à l'ANSSI, il est conseiller auprès du sous-directeur de la stratégie. Il est également, depuis octobre 2019, rapporteur auprès de Michel Van Den Berghe, chargé par le Premier ministre d'une mission de préfiguration d'un Campus Cyber de dimension internationale en France. Jean-Baptiste Demaison enseigne depuis 2015 la cybersécurité à Sciences Po au sein de la *Paris School of International Affairs*. Précédemment, il a été chargé de mission puis coordonnateur pour les affaires politiques européennes et internationales de l'ANSSI. Il a notamment piloté la négociation de la directive NIS et a été désigné expert auprès de l'ambassadeur français pour le numérique dans le cadre des négociations de trois groupes d'experts gouvernementaux de l'ONU sur la cybersécurité. Jean-Baptiste Demaison a également travaillé pour l'Institut de recherche stratégique de l'Ecole militaire, ainsi que pour le ministère des affaires étrangères en Égypte, en tant que directeur adjoint de la filière francophone de la faculté de sciences politiques et d'économie de l'université du Caire. Il est diplômé de Sciences Po Toulouse et titulaire d'un master 2 en affaires politiques internationales de l'Université d'Auvergne.
→ ***Une agence au cœur de la cybersécurité européenne***

Benjamin DUCOS est responsable de la Gestion des risques de l'information pour le Groupe AXA, une fonction de 2e ligne de défense, destinée à garantir que les décideurs d'AXA gèrent de manière optimale les risques sur les données, la technologie et l'innovation. Au cours des vingt dernières années, ses expériences l'ont amené à créer ou transformer des fonctions de sécurité, de sûreté, de gestion des risques mais également d'informatique avec le souci permanent de la création de valeur. Comme enseignant vacataire à Sciences Po Grenoble et dans plusieurs autres instituts, il aide étudiants et professionnels à renforcer leur posture dirigeante, leur leadership, pour concevoir et gérer des organisations agiles en matière de sûreté, de cybersécurité, et capables de faire face à des situations d'exception. Benjamin Ducos est diplômé en Sciences Politiques et il est titulaire d'un Master en Sécurité. Il a également été formé à l'IMD en Suisse, et en France à HEC et à l'IHEDN.
→ ***Le cyber en assurance, un risque presque comme les autres ?***

Florian ESCUDIÉ est Sous-directeur des Affaires stratégiques et de la Cybersécurité au Ministère de l'Europe et des Affaires étrangères depuis mai 2017. Avec son équipe, il est impliqué dans la préparation de la politique française relative à la sécurité et à la défense européennes, aux engagements militaires dans les zones de crise et aux enjeux de cybersécurité. Entré au ministère en janvier 2004, Florian Escudié a d'abord été rédacteur « OTAN / Défense européenne » au sein de la Sous-direction des Affaires stratégiques (2004-2007). Il a ensuite été nommé Premier Secrétaire au sein de l'Ambassade de France à Berlin (2007-2010), puis représentant français au Comité des orientations opérationnelles au Quartier général de l'OTAN à Bruxelles (2010-2013). De retour à Paris, il a été successivement Chargé de mission pour le G7 et le G20 auprès de la Directrice générale de la mondialisation du Ministère des Affaires étrangères (2013-2015) puis Sous-directeur des affaires économiques internationales (2015) avant d'être appelé au cabinet du Ministre (Laurent Fabius puis Jean-Marc Ayrault) en tant que conseiller chargé de la diplomatie économique, des affaires globales et du développement (2015-2017). Florian Escudié est ancien élève de l'Ecole normale supérieure (Paris), diplômé de l'Institut d'études politiques de Paris et titulaire d'une maîtrise d'histoire de l'Université Panthéon-Sorbonne.
→ ***Quelle régulation pour les acteurs privés dans le cyberespace ?***

Julie GOMMES est senior manager en cybersécurité, spécialisée dans la gouvernance de la sécurité de l'information. Elle est auditeur certifiée ISO/CEI 27001, maîtrise l'analyse de risques et la sécurisation des systèmes mais touche aussi à des domaines techniques, notamment *via* des tests d'intrusion informatiques ou des audits de sécurité physiques dans des datacenters ou des zones sécurisées d'entreprises. Entrée dans le domaine de la sécurité suite à une reconversion, Julie Gommes a exercé pendant plusieurs années en tant que RSSI, notamment sur un système d'information Diffusion Restreinte. Elle intervient régulièrement sur les questions de piratage, *hacking*, protection des données, gouvernance de la sécurité lors de conférences en France (Futurapolis, Nuit du Hack…), à l'étranger (Inde, Pologne, Autriche, Canada…) ou dans le cadre de masterclass, à l'instar de celle organisée en 2017 à Tallin par l'Union Européenne. Ses sujets de prédilection sont les suivants : outils de cryptographie utilisés par les djihadistes, sécurité informatique pour les journalistes, gestion de la sécurité au quotidien, conformité *vs* sécurité.
→ ***Que cherchent les hackers ?***

Jules HADDAD est consultant senior dans la practice cybersécurité et confiance numérique du cabinet Wavestone.
→ ***Innovation et startups cybersécurité en France : le début de l'embellie ?***

Olivier KERMAGORET, 45 ans, a débuté sa carrière dans les technologies d'ERP dans le domaine du *retail* de 1997 à 1999, après sa formation initiale en ingénierie des systèmes d'information. Il a ensuite rejoint en 2000 la division IT du Groupe AREVA et a occupé des postes d'ingénieur d'études, d'architecte des SI puis de directeur de projets de développement de logiciels C4I pour le Ministère de la Défense français. De 2008 à 2011, il a développé pour le compte d'AREVA l'activité d'infrastructures informatiques sécurisées pour des industries sensibles dans le domaine de l'énergie (EDF, RTE, ENGIE…). Il a complété sa formation initiale par des diplômes de l'UFR de Sciences Politiques de Paris et de la London Business School. Olivier Kermagoret a rejoint le groupe Thales en 2013 pour développer les activités de transformation dans le domaine IT et assure depuis 2017 le rôle de directeur du segment « services managés infrastructures critiques et *Cloud* », activité de transformation digitale de pointe, incluant les projets de *move to cloud*, de sécurisation des infrastructures et de services d'infogérance à valeur ajoutée.
→ ***La confiance numérique, une condition*** **sine qua non** ***du succès de l'adoption du*** **cloud**

Claude KIRCHNER est directeur de recherche émérite d'Inria dont il a été directeur scientifique de 2010 à 2014. Ses intérêts et contributions scientifiques portent d'une part sur les fondements logique et sémantique pour la conception et la mise en oeuvre de systèmes numériques fiables et sécurisés et d'autre part sur les enjeux sociétaux, scientifiques et éthiques de la numérisation globale de nos sociétés. Docteur d'Etat de l'université de Nancy en 1985, à partir de 1992 il a créé et dirigé une équipe-projet Inria à Nancy puis dirigé de 2007 à 2010 le centre de recherche Inria Bordeaux – Sud-Ouest. Il a été lauréat avec l'équipe Eureca de la médaille d'argent du CNRS en 1987 et colauréat du grand prix de l'Académie des Sciences 2002 au titre de la fondation culturelle Franco-Taïwanaise. Il a présidé de 2003 à 2008 les conseils scientifique et d'évaluation des programmes du ministère puis de l'ANR en sécurité informatique. Claude Kirchner a été président du COERLE, comité opérationnel d'éthique d'Inria et son référent à l'intégrité scientifique jusqu'à fin 2018. Depuis 2018, il est membre du CCNE pour les sciences de la vie et de la santé et depuis 2019, président de la CERNA, commission de réflexion sur l'éthique de la recherche en sciences et technologies d'Allistene. Il est également membre du comité de prospective de la CNIL, du COTSS de Renater et du conseil scientifique de l'ANSSI. Il a présidé le comité de pilotage du CCSD en charge de l'archive ouverte nationale HAL et de la mise en œuvre de services pour la science ouverte tel qu'episciences.org. Il co-dirige l'initiative franco-japonaise de coopération en cybersécurité.
→ ***Défis de la recherche scientifique en cybersécurité***

Jacques DE LA RIVIÈRE est Président, Co-fondateur de Gatewatcher. Après des études d'ingénieur à l'ESIEA, il débute sa carrière chez Mahindra Satyam en Inde en tant que chef de projet offshore. Il poursuit ensuite en tant qu'analyste risque de risque de crédit dans une grande banque française puis Ingénieur Commercial chez ADNEOM et BK Consulting sur des projets d'optimisation des flux dans le *trading* haute fréquence. En 2015, il s'associe à Philippe Gillet pour créer Gatewatcher, solution de détection de menaces avancées en temps réel. Gatewatcher s'adresse en premier lieu aux organismes d'importance vitale (OIV), identifiés par la LPM 2014-2019, et équipe les principales banques françaises en France et à l'international.
→ ***Prévenir et détecter***

Claire LANDAIS est Secrétaire générale de la défense et de la sécurité nationale depuis le 5 mars 2018. Elle est diplômée de l'Ecole supérieure des sciences économiques et sociales, de l'Institut d'études politiques de Paris et de l'Ecole Nationale d'Administration (promotion « Averroès », 2000). Elle est Conseillère d'Etat depuis 2000, travaillant à la section du contentieux, puis à la section des travaux publics. Mme Landais devient Commissaire du Gouvernement à la section du contentieux du Conseil d'Etat en 2007, puis exerce les fonctions de Directrice des affaires juridiques du ministère de l'éducation nationale et du ministère de l'enseignement supérieur et de la recherche à partir de 2008. Après avoir exercé de nouveau dès2010 à la section du contentieux au Conseil d'Etat en tant que Rapporteur public, elle devient en 2012 Directrice des affaires juridiques du ministère de la défense et ce jusqu'en 2017, lorsqu'elle prend pour un an les fonctions d'Assesseur à la section du contentieux du Conseil d'Etat. Mme Landais est Chevalier de l'Ordre national du mérite et Commandeur des Palmes académiques.
→ ***Souveraineté numérique et sécurité nationale***

Jean LESSI est né en 1982. Il est diplômé de l'ENA (Promotion « Willy Brandt », 2007-2009), de l'Institut d'études politiques de Paris (Master affaires publiques) et de l'Université Paris-II Panthéon-Assas (Licence de droit). Au Conseil d'Etat, il a occupé successivement les fonctions de rapporteur à la section du contentieux, puis à la section sociale, de responsable du Centre de recherches et de diffusion juridiques et enfin de rapporteur public à la section du contentieux (1ère

chambre). En 2013, il a été secrétaire général de la Commission pour la transparence financière de la vie politique jusqu'à la création de la Haute autorité pour la transparence de la vie publique. Il exerce depuis mai 2017 les fonctions de secrétaire général de la CNIL.
→ ***Le RGPD au service de la cybersécurité***

Luc DE LIGNIÈRES est ingénieur de formation, et actuaire certifié de l'Institut des Actuaires. Il a exercé toute sa carrière en assurances dommages au sein du Groupe AXA, où il a occupé différents postes opérationnels de responsabilité en France puis au Canada avant de s'orienter vers la gestion des risques en 2011. P&C Chief Risk Officer du Groupe AXA depuis 2015, il a en charge le suivi des risques d'assurance dommages sur l'ensemble des entités du Groupe, soit le risque de souscription, le risque de réserves et le risque de catastrophes (naturelles et du fait de l'homme). Dans ce cadre, il a supervisé la mise en place d'une modélisation interne du risque Cyber en assurance pour le Groupe AXA, devenu avec l'acquisition de l'assureur et réassureur américain XL Catlin en 2018, l'un des leaders mondiaux de l'assurance Cyber.
→ ***Le cyber en assurance, un risque presque comme les autres ?***

Jacques MARTINON, magistrat de l'ordre judiciaire, a débuté sa carrière en tant que juge d'instruction dans différentes juridictions (Senlis, Bobigny), avant de rejoindre la direction des affaires criminelles et des grâces (DACG) au ministère de la Justice. Chef de la mission de lutte contre la cybercriminalité, il a participé aux travaux de la Revue Stratégique de la Cyberdéfense (février 2018, SGDSN) et contribue à la comitologie instaurée (C4, Centre de Coordination des Crises Cyber). Il prépare diverses dépêches de politiques pénales en matière de cybercriminalité, et représente la France au sein du réseau européen EJCN (*European Judicial Cybercrime Network*). Enfin, il a participé au groupe pluridisciplinaire de hauts fonctionnaires sur la régulation des réseaux sociaux, en collaboration avec la société Facebook (rapport rendu en mai 2019).
→ ***À la poursuite des cyber-criminels***

Ludovic MÉ, enseignant-chercheur à Supélec de 1988 à 2014, puis à CentraleSupélec de 2015 à 2017, est en détachement chez Inria depuis début 2018 et il occupe depuis mars 2019 le poste d'adjoint au Directeur Général Délégué à la Sciences, en charge du domaine de la cybersécurité. Son domaine de recherche de prédilection est la sécurité réactive (détection d'intrusions, corrélation d'alertes). Il s'est néanmoins également intéressé à la sécurité des réseaux auto-organisés (ad hoc, P2P) et à la virologie informatique. Dans ces domaines, il est auteur ou co-auteur de plus de soixante-dix communications nationales et internationales. Il a encadré à ce jour quinze doctorants (2 thèses en cours) et a par ailleurs été directeur de thèse de quatorze autres étudiants. Ludovic Mé a animé de 1997 à 2011 l'équipe de recherche en sécurité des systèmes d'information et réseaux (équipe SSIR, EA 4039), puis de juillet 2011 à avril 2016, il a été responsable de l'équipe projet « Cidre », commune à Supélec, à Inria, au CNRS et à l'Université de Rennes 1 (Cidre est une équipe de l'UMR IRISA). Ludovic Mé a en outre été de septembre 2008 à septembre 2015 responsable de la majeure de 3e année de Supélec dédiée à la sécurité informatique. De janvier 2015 à février 2019, il a été délégué scientifique du centre Rennes Bretagne Atlantique de Inria. Ludovic Mé a été de 2002 à 2018 membre du comité de pilotage du symposiu RAID (*International Symposium on Research in Attacks, Intrusions and Defenses*, anciennement *Recent Advances in Intrusion Detection*). Il est depuis sa création membre du comité de pilotage de la conférence RESSI (rendez-vous de la Recherche et de l'Enseignement en Sécurité des Systèmes d'Information). Il a été membre de 2004 à 2012 du comité éditorial de la revue JCV (*European Research Journal in Computer Virology*). Il a été membre du conseil d'évaluation du domaine SSI de la DGA (2006-2012), du conseil pour les activités SSI d'EdF (2010) et du Conseil Scientifique du Conseil Supérieur de la Formation et de la Recherche Stratégique (2011-2013). Il pilote depuis 2016 le comité d'experts en STIC du collège d'experts du dispositif de protection du patrimoine scientifique et technique de la nation (PPST).

Ludovic Mé est ingénieur Supélec (1987), docteur de l'Université de Rennes 1 (1994) et titulaire d'une HDR de cette même université (2003).
→ ***Défis de la recherche scientifique en cybersécurité***

Jérôme NOTIN est impliqué dans la sécurité numérique depuis de nombreuses années. Il dispose d'expériences dans la création et la direction d'entreprises. Il a rejoint l'ANSSI en mai 2016 en qualité de préfigurateur du dispositif et a été nommé en mars 2017 directeur général du GIP ACYMA lors de sa création. Il est par ailleurs ancien gendarme auxiliaire (94/10 PSIG de Blois) et chef d'escadron de la réserve citoyenne cyberdéfense de la gendarmerie.
→ ***La sensibilisation : une arme défensive majeure***

Guillaume POUPARD est ancien élève de l'école polytechnique, promotion X92. Ingénieur de l'armement en option recherche, il est titulaire d'une thèse de doctorat en cryptographie réalisée sous la direction de Jacques Stern à l'Ecole normale supérieure de Paris et soutenue en 2000. Il est également diplômé de l'enseignement supérieur en psychologie. Il débute sa carrière comme expert puis chef du laboratoire de cryptographie de la Direction centrale de la sécurité des systèmes d'information (DCSSI). Cette direction sera transformée en 2009 pour devenir l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Il rejoint en 2006 le ministère de la défense, toujours dans le domaine de la cryptographie gouvernementale puis de la cyberdéfense. En novembre 2010, il devient responsable du pôle « sécurité des systèmes d'information » au sein de la direction technique de la Direction générale de l'armement (DGA), responsable de l'expertise et de la politique technique dans le domaine de la cybersécurité. Le 27 mars 2014, il est nommé directeur général de l'ANSSI. Marié, il est père de trois enfants.
→ ***Le modèle français de cybersécurité : priorité à la défense***

Vincent RIOU dirige les activités cyberdéfense de CEIS, société spécialisée en conseil en stratégie, intelligence économique et cybersécurité. Après onze ans d'expérience en responsabilité de programmes de guerre électronique et de renseignement à la Direction Générale pour l'Armement, Vincent Riou a rejoint le groupe Steria *où il assuré pendant 5* ans la direction des activités « Défense et Sécurité ». *Chez* CEIS depuis 2012, il a d'abord été en charge du business développement de la société. Vincent Riou est également CEO de bluecyforce, premier centre d'entraînement européen en cyberdéfense, créé avec la société Diateam. Ingénieur des corps de l'armement, il est titulaire d'un diplôme d'ingénieur de l'ENSTA Bretagne et d'un master d'administration des entreprises de l'IAE. Il est également auditeur de la 47e session nationale de l'IHEDN « *Armement et Economie de Défense* ».
→ ***Cyberdéfense : l'humain au cœur de l'efficacité opérationnelle***

Le général de division aérienne **Didier TISSEYRE** est né le 14 septembre 1966. Sa carrière est marquée par des postes opérationnels et techniques, de commandement et d'expert, dans les domaines des systèmes d'information et de communication, de la cyberdéfense, de la simulation opérationnelle, du développement capacitaire et de la formation. Officier du corps des mécaniciens, issu de la promotion 1987 « Général Boichot » de l'École de l'Air, il est également ingénieur de l'École nationale supérieure de techniques avancées, option recherche opérationnelle, et breveté de l'École de guerre en 2003. Il a tenu des postes en unités et en états-majors au sein de l'armée de l'Air, de structures interarmées (état-major des armées et direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense) ou internationales (représentation militaire auprès du comité militaire de l'OTAN). Projeté au Tchad en 2006 à la tête des systèmes d'information de l'opération Épervier, il a participé à de nombreux exercices de l'armée de l'Air, interarmées ou multinationaux (OTAN, UE). De 2015 à 2017, il a commandé les écoles des sous-officiers et des militaires du rang de l'armée de l'Air, ainsi que la base aérienne 721 de Rochefort et

la base de défense Rochefort-Cognac. Il devient ensuite, entre 2017 et 2019, l'officier général adjoint à l'officier général « commandant de la cyberdéfense ». Par décret du Président de la République en date du 17 juillet 2019, le général de division aérienne Tisseyre est nommé officier général « commandant de la cyberdéfense » de l'état-major des armées à compter du 1er septembre 2019. Il est promu général de division aérienne à la même date. Ses fonctions opérationnelles s'articulent autour de quatre axes majeurs : la conduite de la défense des systèmes d'information du ministère des Armées ; la protection des systèmes d'information de la responsabilité du chef d'état-major des armées ; la conception, la planification et la conduite des opérations militaires dans le cyberespace. Au-delà de ces responsabilités opérationnelles, il assure la cohérence du modèle de cyberdéfense du ministère des Armées et sa coordination générale, en particulier dans les domaines des ressources humaines et capacitaires ainsi que des relations internationales. Le général Tisseyre est officier de l'ordre national de la Légion d'honneur, officier de l'ordre national du Mérite et titulaire de la médaille de l'Aéronautique.

→ ***Retour sur la genèse de la cyberdéfense militaire***

Yves VERHOEVEN est ancien élève de l'Ecole normale supérieure. Docteur en informatique, il est ingénieur en chef des Mines. Après un début de carrière en 2005 au sein du ministère des affaires étrangères, il a rejoint le secrétariat général de la défense nationale en 2007, puis l'Agence nationale de la sécurité des systèmes d'information en 2009. Entre recherche, gestion de projet, responsable de la sécurité des systèmes d'information, officier de programme, responsable des relations internationales et conseiller numérique du directeur général, Yves Verhoeven a couvert un large éventail d'activités en lien avec la sécurité du numérique et la cyberdéfense. Il exerce la fonction de sous-directeur depuis janvier 2016, d'abord des Relations extérieures et de la coordination, puis de la Stratégie.

→ ***Protection des infrastructures critiques : 5 ans après la loi***