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.

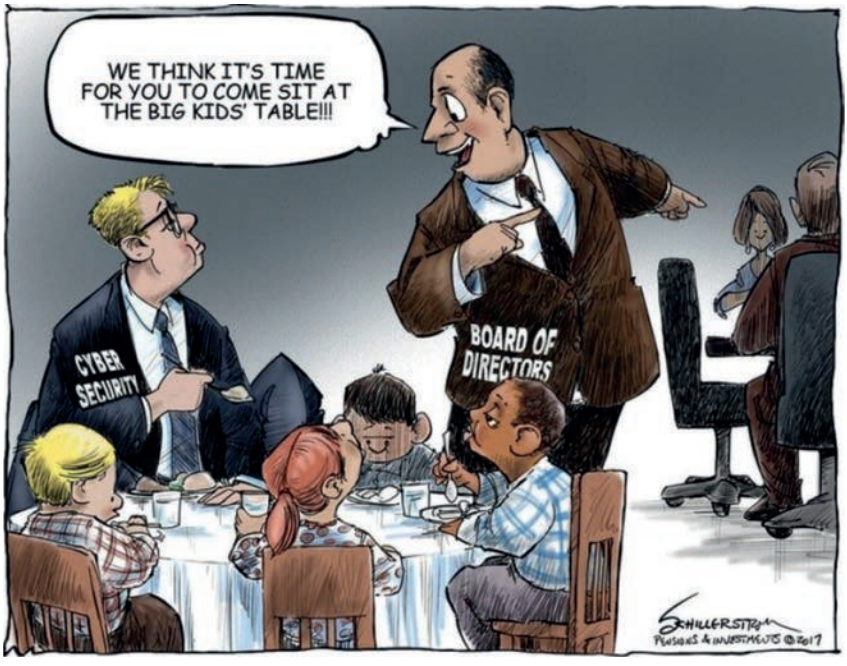

Illustration 1.

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.

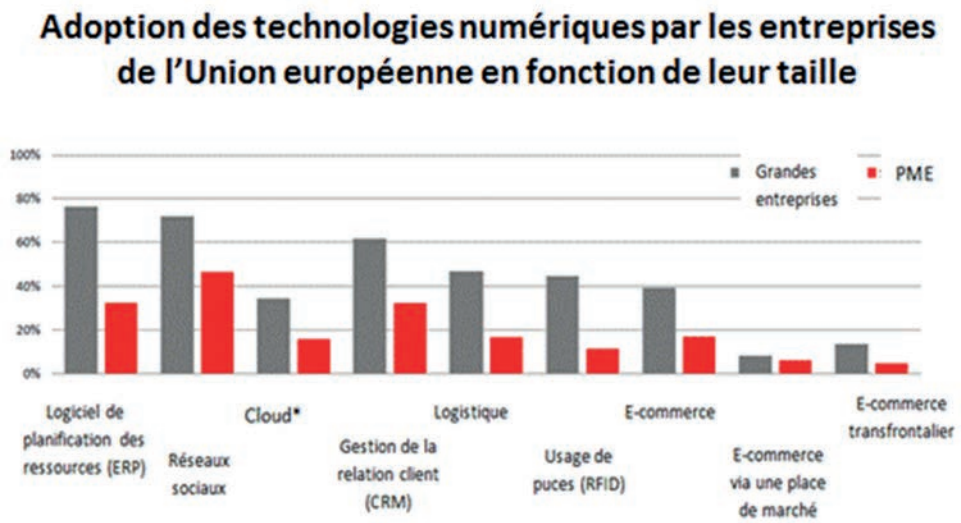

Illustration 2.

(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

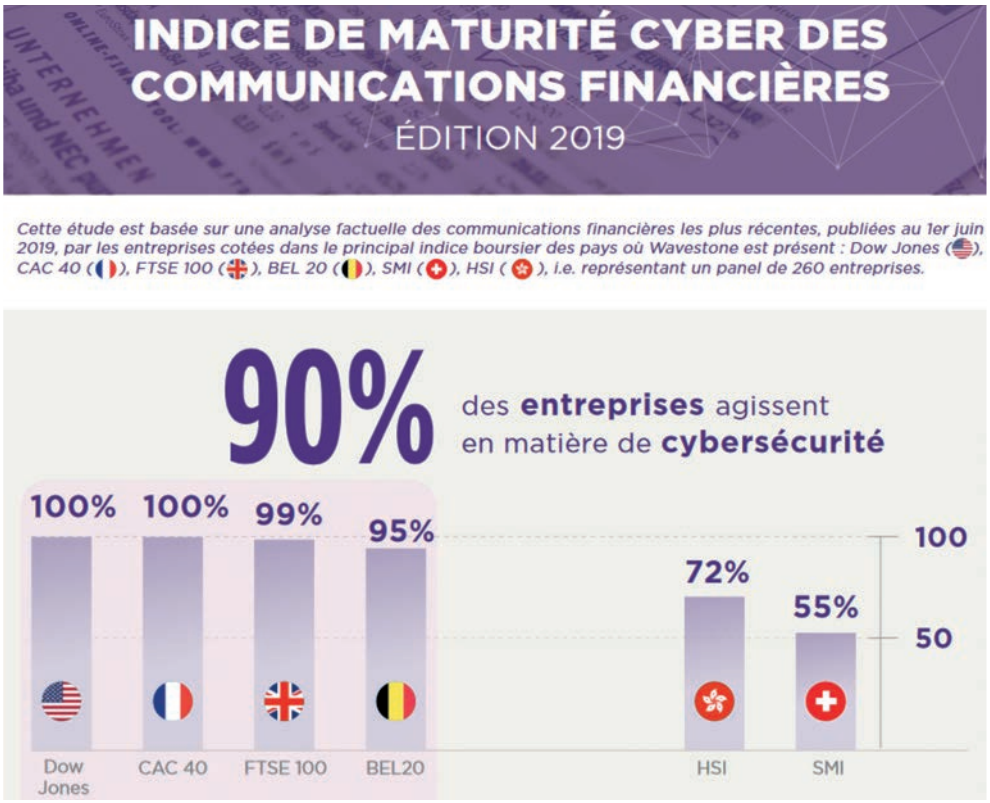

Illustration 3 : « Maturité cybersécurité dans les communications financières des grands indices boursiers », juillet 2019, Cabinet Wavestone.

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.

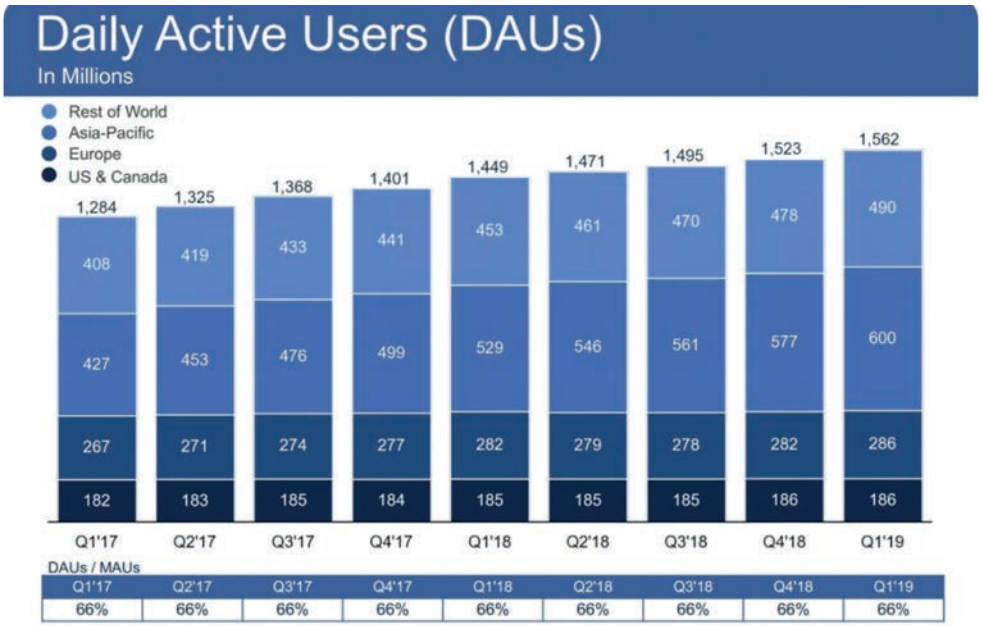

Illustration 4 : Nombre d'utilisateurs actifs de Facebook. Source : Facebook.

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.