Cybersécurité : risques et enjeux économiques

Nicolas ARPAGIAN*

Un monde sans frontières, où l'identité de chacun est modifiable à l'envie, où les coûts sont marginaux, où la zone d'intervention est naturellement planétaire et où l'hyperréactivité est la norme. Autant de caractéristiques qui font du cyberespace un territoire d'épanouissement pour l'industrie financière. Qui a depuis longtemps rompu avec les séances de cotation à la corbeille de la Bourse pour adopter sans retenue dès la fin du XX^e^ siècle la dématérialisation des échanges numériques. Les flux financiers n'ont jamais été aussi productifs et fluides : la nanoseconde devient l'unité de temps de déclenchement des ordres de Bourse. Les écrans sont les seuls témoins des transactions et les fortunes ne se matérialisent plus dans des livres de comptes, mais bien dans les seuls serveurs informatiques. Il devient nettement moins risqué, et certainement plus rentable au regard de la peine encourue, d'opter pour un détournement de fonds *via* une cyberattaque que de persister à vouloir s'en prendre physiquement aux coffres d'une agence bancaire. La rapidité des transferts de fonds et la capacité à déplacer ceux-ci en un clic d'un pays à un autre, et donc d'un régime juridique à un autre, pénalisent l'enquêteur d'un État démocratique. Il sera dépendant de la qualité de la coopération interétatique pour obtenir des informations sur la nature et l'origine de ces virements. Et si de tels franchissements de frontières se multiplient, l'ampleur de la procédure à déployer pour tenter de pister ce qu'il advient des sommes en question peut s'avérer dissuasive. De quoi rendre vaines les tentatives d'identification des flux financiers. Soit *de facto*, pour les esprits malintentionnés, un encouragement supplémentaire à basculer vers la cybercriminalité.

* Directeur scientifique du cycle « Sécurité numérique », Institut national des hautes études de la sécurité et de la justice (INHESJ) ; maître de conférences, École nationale supérieure de la police (ENSP) ; directeur de la stratégie et des affaires publiques, Orange Cyberdefense ; rédacteur en chef, *Prospective stratégique*. L'auteur s'exprime ici à titre personnel.

UNE EXPOSITION CROISSANTE AU RISQUE NUMÉRIQUE

La numérisation de nos existences est en marche. Qu'il s'agisse de nos vies personnelles où les smartphones sont devenus nos béquilles mentales, à qui nous confions les coordonnées de nos relations, les multiples mots de passe de nos réseaux sociaux et comptes bancaires ainsi que les photos et les messages qui jalonnent notre quotidien. Avec une situation paradoxale : ces téléphones intelligents rassemblent de plus en plus de données personnelles, voire intimes, mais leur sécurisation laisse encore largement à désirer. Alors que les antivirus et autres pare-feu équipent désormais les ordinateurs même domestiques, ces smartphones sont largement utilisés sans protection particulière. On demande donc à l'utilisateur/trice quels que soient son âge, sa formation ou son intérêt pour le sujet de prendre en charge la sécurisation de son équipement et de sa connexion. Chaque titulaire d'un accès à Internet a ainsi une « obligation de surveillance » dudit accès (article L-336-3 du Code de la propriété intellectuelle). Et l'article L-335-7-1 du Code de la propriété intellectuelle prévoit qu'un titulaire d'un abonnement à Internet peut voir sa responsabilité pénale engagée au titre de la contravention de négligence caractérisée. Cette exigence de sécurisation rompt avec la règle ancienne qui voulait que les services de l'État, qu'il s'agisse de l'autorisation de circuler d'un véhicule ou de la mise sur le marché d'un médicament, évaluent seuls les aspects de sécurité. Ne mettant à la disposition des consommateurs que des biens ou des services dont la dangerosité à l'usage avait été évaluée et encadrée. Dans le domaine du numérique, le consommateur final se trouve chargé de cette tâche. Quitte à voir par la suite sa responsabilité juridique et financière mise en cause.

Le canal numérique devient le moyen naturel de commercer, de se renseigner, de consommer et parfois de convoler. Autant d'occasions démultipliées de susciter la créativité des pirates. Tout ce que les délinquants et les criminels faisaient de mal dans le monde physique depuis des lustres trouve des déclinaisons par voie informatique : usurpation d'identité, détournement de fonds, chantage/extorsion, vol d'informations, vol de ressources, escroquerie, etc. La capacité de démarcher rapidement un grand nombre de futures victimes et le fait de pouvoir rapatrier sans délai et à coût réduit le fruit de son vol, le tout dans une relative impunité judiciaire, expliquent l'essor de la cybercriminalité. Celle-ci est encore recensée de manière très partielle par les services officiels, comme l'Observatoire national de la délinquance et des réponses pénales (ONDRP)[1].

Soucieuses de leur productivité, les entreprises incitent leurs collaborateurs à travailler lors de leurs déplacements et, le cas échéant, à leur domicile. Cette mobilité démultiplie les modes de connexion au système d'information central. Wifi publics, recours à des ordinateurs en libre-service ou à des équipements personnels pour se brancher sur l'informatique de la société... On est loin de la gestion d'un parc de machines entièrement maîtrisé par une Direction des

systèmes d'information omnisciente. Le phénomène touche les entreprises de toutes tailles et de tous secteurs, et gagne de plus en plus les administrations.

Si des solutions techniques protègent l'accès aux systèmes d'information et assurent une réelle confidentialité des échanges, les pirates optent désormais pour une tactique plus sournoise. En effet, faute de pouvoir/savoir casser la serrure, ils se renseignent pour savoir où vous cachez vos clés. C'est toute l'utilité de l'ingénierie sociale : l'élaboration d'un scénario fondé sur une approche très personnalisée de celui/celle qui détient l'information ciblée. Une consultation assidue des réseaux sociaux fournit à peu de frais tous les éléments de contexte permettant d'aborder de manière crédible un cadre dirigeant. En ayant identifié ses *hobbies*, ses expériences professionnelles passées ainsi que ses relations en affaires, le pirate dispose d'une matière éditoriale complète et à jour pour finaliser un discours d'approche très efficace. La cible croira à une sollicitation fortuite tandis qu'il s'agira d'un moyen d'entrer dans son cercle de connaissances. Une telle cartographie permet si besoin de préparer une rencontre dans la vie bien réelle. Le piratage en 2012 de l'intranet de la présidence de la République française a débuté par un message opportunément envoyé sur Facebook à un collaborateur du chef de l'État. En cliquant sur un lien contenu dans ledit message, il a infecté l'ordinateur qui lui servait à accéder à son compte de messagerie professionnelle. Ce travail préalable de *social engineering* a donc été pertinent pour mener à bien cette mission d'espionnage.

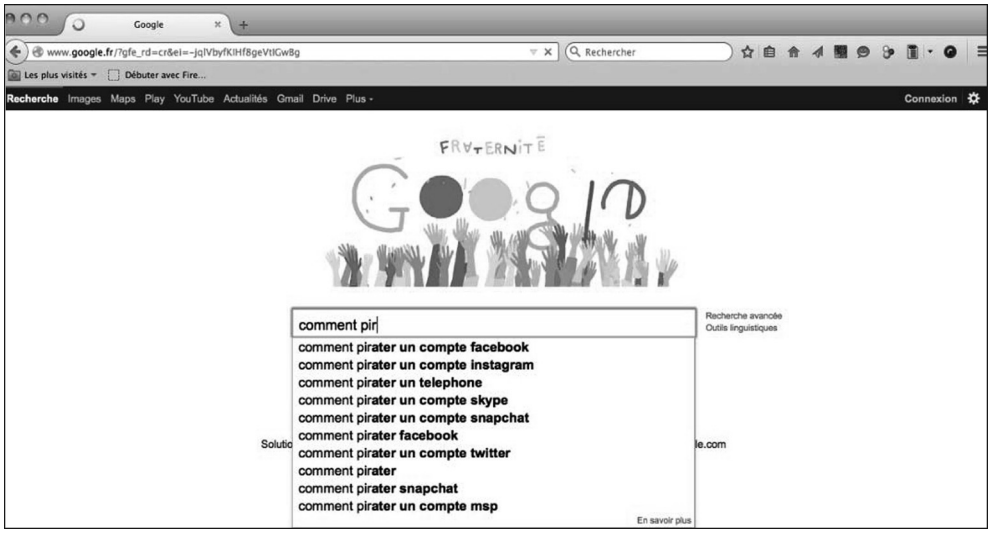
La généralisation de la numérisation de nos activités (dossiers de santé, impôts, comptes bancaires, correspondances professionnelles et personnelles, réseaux sociaux, smartphones géolocalisés, objets connectés, etc.) ouvre autant de brèches possibles pour atteindre le but poursuivi : vol d'identités, d'argent ou d'informations confidentielles. Sans oublier des opérations spécifiquement numériques comme le déni de service (paralysie d'un site internet sous le coup d'un très grand nombre de connexions frauduleuses simultanées) ou le chantage au chiffrement (les données chiffrées par les pirates sont rendues de nouveau accessibles en échange d'une rançon). De telles pratiques peuvent atteindre indifféremment des personnes ou des institutions soigneusement identifiées au préalable comme n'importe quelle entité dès lors qu'elle est connectée au réseau. Ce qui fait de tout utilisateur du Net une victime potentielle d'une cyberattaque.

UN ARSENAL DE CYBERATTAQUANT QUI SE DÉMOCRATISE

Si l'on considère que l'internaute est par essence exposé au risque numérique, il est tout aussi important d'indiquer qu'il est également en première ligne en ce qui concerne l'attaque. En effet, la modicité des prix des outils basiques de piratage et

leur simplicité d'utilisation ont déjà fait leur succès auprès du grand public. Les conjoints jaloux, les employeurs suspicieux et les parents inquiets ont trouvé facilement *via* les moteurs de recherche les applications indétectables leur permettant de récupérer le détail des déplacements, la liste des appels, l'intégralité des SMS ainsi que l'historique des sites internet visités par leur cible. Ces captations de grande ampleur qui autrefois étaient la spécialité des services de renseignement sont devenues des pratiques domestiques. La jurisprudence concernant des collégiens ou des étudiants conduisant des cyberattaques à l'encontre de leur établissement en vue de modifier leurs notes s'étoffe tous les jours. Et nombre de conflits intrafamiliaux comportent désormais leur volet numérique, notamment avec des atteintes à la réputation. La publication non autorisée de photographies intimes, vraies ou maquillées, est ainsi devenue une riposte presque habituelle à des contentieux sentimentaux. L'arme numérique fait partie de l'arsenal des particuliers. Il suffit de taper les premières lettres « comment pir » sur un moteur de recherche pour voir la facilité d'accès à des offres de piratage clés en main (cf. illustration). Cet affichage suggéré aussi précisément par le moteur témoigne de deux phénomènes : ces requêtes sont formulées par un très grand nombre d'internautes et le marché répond à cette demande par une offre diversifiée et abondante.

Illustration
Propositions spontanées de réponses sur le moteur de recherche www.google.fr avec la seule requête : « comment pir »
(consultation en décembre 2015)



Des outils plus perfectionnés et encore plus discrets sont évidemment déjà maîtrisés par les bons connaisseurs de la pénétration informatique, qui commer-

cialisent leur savoir-faire à des organisations visant des objectifs professionnels ou gouvernementaux. Edouard Snowden a révélé en outre dès 2013 comment les grandes plates-formes internet (Google, Apple, Facebook, Amazon, Microsoft, Twitter, etc.) collaboraient étroitement avec les autorités états-uniennes en fournissant à celles-ci les informations demandées. Une démarche qui épargne à Washington les opérations techniques d'espionnage puisque ses services peuvent ainsi se fournir directement chez ces grands équipementiers du Net. Mettant ainsi au service de la stratégie états-unienne l'ensemble des renseignements économiques, diplomatiques, personnels, connectés *via* ces sociétés qui collectent, drainent, croisent et stockent des milliards d'informations par jour.

QUAND LES ENTREPRISES DE RENOM OPTENT POUR L'ARME NUMÉRIQUE

La concurrence économique porte largement sur la capacité de l'un des compétiteurs à acquérir de l'information avant les autres. Cette aptitude à connaître ce que prévoit le rival, à identifier ses spécificités cachées et à réduire ainsi la part d'incertitude intéresse tous les dirigeants d'entreprise. Surtout si on les persuade qu'ils pourront acquérir cette information stratégique à un coût raisonnable, dans un délai rapide et sans risque réel d'être identifiés. C'est la raison pour laquelle il ne faut pas considérer les cyberattaques ou les recours offensifs aux technologies de l'information dans le monde de l'entreprise comme relevant des seules organisations mafieuses. On constate au contraire que de très grandes sociétés, en principe honorablement connues et signataires de nombre de chartes humanistes (pour le respect des droits des enfants, de la parité homme/femme, du recyclage des déchets et autres promesses de contribuer à un monde meilleur), sont prêtes à financer des campagnes d'attaques sur la Toile.

Qu'il s'agisse de voler de l'information ou d'organiser une campagne de dénigrement contre un concurrent. En octobre 2013, Samsung, le n° 1 mondial des téléphones portables, a été condamné par un tribunal de Taïwan pour avoir payé des blogueurs et des étudiants afin de dénigrer les produits de son concurrent HTC[2]. En juin 2014, Microsoft a été pris la main dans le sac à rémunérer des blogueurs influents pour publier des articles favorables à la nouvelle version de son navigateur Internet Explorer[3].

En septembre 2013, dans une enquête[4] publiée en deux volets dans le *Journal du Net*[5], j'ai expliqué comment une dizaine de grandes entreprises ou associations professionnelles avaient bénéficié de la publication de textes en leur faveur dans les colonnes de grands médias français : *Les Échos*, *L'Obs*, *Mediapart*, *Le Figaro*, le *Journal du Net*, etc. En usurpant des identités, en volant les photos de vraies personnes, en invoquant des noms d'employeurs prestigieux, de faux analystes ou

experts ont pris la plume pour vanter les mérites ou critiquer vertement des sociétés commerciales ou des personnalités. Misant sur le crédit des supports de presse utilisés pour donner de la consistance et du poids à leurs prises de positions, tant vis-à-vis des internautes que des moteurs de recherche. Pour que ces articles soient le mieux référencés possibles et donc participent à la mise en avant de leurs intérêts. Et quelquefois, ce procédé est utilisé pour des opérations financières. Ainsi, le 5 janvier 2015, j'ai démontré dans le *Journal du Net*[6] comment l'offre publique d'achat (OPA) sur la société Club Méditerranée d'un montant de 1 Md€ comportait un volet d'influence visant à dévaloriser l'un des deux candidats au rachat, l'italien Bonomi. En totale violation du Règlement général de l'Autorité des marchés financiers (AMF) et du Code pénal, des articles publiés dans les pages de *Mediapart*, du quotidien *Les Échos* ou du *Journal du Net* tentaient de saper l'image de l'investisseur italien afin de décrédibiliser son offre. L'investigation technique a permis de remonter jusqu'à un cabinet de conseil. Les explications et les détails fournis par des personnes travaillant ou ayant travaillé au sein de cette officine ont complété la description de leur mode opératoire. C'est l'objet d'une enquête détaillée[7] publiée le 12 janvier 2015 dans le *Journal du Net* où l'on apprend que ces professionnels ne se contentent pas d'alimenter les médias en articles sans aucune fiabilité, mais qu'ils sont également des contributeurs très actifs de l'encyclopédie en ligne Wikipedia. Ce qui leur a permis d'accéder à un statut élevé dans la hiérarchie des rédacteurs/correcteurs de ce site très fréquenté. Ils monnaient à leurs clients leur aptitude à embellir les notices les concernant, voire à biaiser celles de leurs concurrents. Un réel pouvoir d'influence alors que nombre d'internautes considèrent Wikipedia comme leur première source d'information.

UNE RÉPONSE POLICIÈRE ET JUDICIAIRE DISPARATE

Le réseau des réseaux est international par nature. Mais la réponse policière et judiciaire reste encore largement nationale. Le seul texte de dimension planétaire relatif à la cybercriminalité est la Convention de Budapest du Conseil de l'Europe du 23 novembre 2001[8]. Les grands États ont longtemps tardé à l'intégrer dans leur droit national, ils sont encore nombreux à ne pas le prendre en compte. Même l'Union européenne, cet ensemble politique, économique et juridique particulièrement intégré, aura attendu le 12 août 2013 pour que le Parlement européen et le Conseil de l'Union européenne adoptent la directive 2013/40/UE[9] relative aux attaques contre les systèmes d'information qui vise à combattre la cybercriminalité, la date limite de transposition étant donc le 4 septembre 2015. C'est seulement en 2013 qu'Europol s'est doté d'un centre européen de coordination en matière de cybercriminalité : The European Cybercrime Center (EC3)[10]. Là encore, on parle d'échanges et de coopération entre les États membres, ce qui

suppose des tractations mêmes informelles. On est encore loin d'un modèle intégré de réponse qui permettrait de gagner en réactivité. Les gouvernements restent encore très attachés à piloter eux-mêmes leurs politiques en matière de cybersécurité et de lutte contre la criminalité numérique.

CONCLUSION PROVISOIRE

Il serait déraisonnable de croire que l'on pourrait conclure de manière définitive sur les questions de cybersécurité. Ce qui explique l'adjonction du qualificatif « provisoire » à l'intitulé de cette conclusion. En effet, des facteurs multiples viendront affecter la manière dont cette sécurité numérique évoluera. Car nous nous situons à la croisée de multiples chemins. Principalement trois segments majeurs.

À commencer par le chantier de la gouvernance du Net encore largement piloté par les États-Unis, celle-ci est de plus en plus discutée par des poids lourds comme la Chine et la Russie. Dans ce débat, l'Europe est pour le moins timide et ne valorise pas comme elle le pourrait et devrait le poids économique de sa population. Le risque étant un *statu quo*, faute de pouvoir proposer une solution alternative satisfaisante au modèle existant.

Ensuite vient la question de l'influence et de l'action normative des géants du Net comme Facebook, Google, Apple, etc. dont les conditions générales d'utilisation prétendent devenir le véritable *corpus* juridique de la vie numérique. Faute de dispositifs juridiques effectivement opérationnels, comme, par exemple, la définition d'une identité numérique d'origine étatique pour chacun, les profils créés chez chacune de ces plates-formes ont quasiment valeur de pièce d'identité. Un privilège qui jusqu'à présent relevait des seuls États et auxquels elles pourraient un jour prétendre se substituer. Ces multinationales occupent peu à peu tous les champs de l'activité humaine : le commerce, la santé, la banque, la gestion des correspondances, la cartographie, l'automobile, l'équipement ménager, les relations sociales, etc. Et façonnent à leur goût nos activités en prenant soin d'en autoriser certaines, d'en bannir d'autres, tandis qu'elles enregistrent le détail de tous nos actes. L'interconnexion de ces éléments donne corps au panoptique et à la société de surveillance généralisée[11].

Cet état de fait, qui est quasiment atteint aujourd'hui, peut être le déclencheur du troisième segment d'évolution : celui de la prise de conscience des utilisateurs. Qui pensent encore être les sujets de cette société numérique en construction, alors qu'ils n'en sont essentiellement que les objets. Offrant le détail de leurs vies (personnelle, professionnelle, affective, etc.) en pâture à ces services gratuits qui fondent leur prospérité sur la mise en fiches et la commercialisation de chaque épisode ou envie de nos existences. Au point d'en prendre le contrôle avec une

intensité que n'ont jamais atteint les régimes politiques les plus autoritaires. Si une prise de conscience survenait au sein de l'opinion publique, elle pourrait remettre en question cette évolution. Car rappelons-le, l'entreprise reste un corps social mortel. Qui peut se déliter et disparaître dès lors que ses clients désertent. Le consommateur-internaute vote avec sa souris sur son ordinateur ou son doigt sur son smartphone. Ce sont les bulletins de vote modernes pour décider de l'avenir de son destin personnel. En choisissant tel ou tel prestataire, on le renforce dans ses pratiques, tandis qu'en délaissant tel autre, on le fragilise et l'oblige à adapter son offre en fonction des intérêts et des exigences de ses clients. Cette prise en compte de la valeur de notre engagement lors de notre consommation numérique constitue les prémices d'une reconquête d'une part individuelle de souveraineté. L'un des derniers moyens de ne pas subir, mais de recouvrer sa place de citoyen éclairé. Il ne reste plus beaucoup de temps pour y parvenir. Nos atermoiements agissent en notre défaveur, tandis que se dessine le périmètre restreint de notre liberté individuelle. De l'utilité de relire sans tarder le roman *1984* du génial Georges Orwell et *La Peau de Chagrin* publié en 1831 par Honoré de Balzac dans *La comédie humaine*. On ne pourra pas dire que nous n'étions pas prévenus.

Notes

1. Voir le site : www.inhesj.fr/fr/page/ondrp/presentation.

2. Voir le site : www.theguardian.com/technology/2013/oct/24/samsung-fined-taiwan-campaign-against-smartphone-htc.

3. Voir le site : http://uncrunched.com/2014/06/17/microsoft-paying-bloggers-to-write-about-internet-explorer/.

4. Premier volet de l'enquête de Nicolas Arpagian publié dans le *Journal du Net* (9 septembre 2013) : « Le Plus, l'Express et le Journal du Net victimes d'une intox à grande échelle » : www.journaldunet.com/ebusiness/crm-marketing/les-pros-de-la-e-reputation-infiltrent-les-medias-web.shtml.

5. Second volet de l'enquête de Nicolas Arpagian « Opération d'intox sur Internet : Numericable, Vivarte et neuf autres marques impliquées » parue le 16 septembre 2013 dans le *Journal du Net* : www.journaldunet.com/ebusiness/crm-marketing/faux-chroniqueurs-sites-medias-influence-e-reputation.shtml.

6. Voir le site : www.journaldunet.com/ebusiness/le-net/opa-club-med-intox-internet.shtml.

7. Voir le site : www.journaldunet.com/ebusiness/le-net/istrat-manipulateur-sites-media-wikipedia.shtml.

8. Présentation sur le site du Conseil de l'Europe : www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185.

9. Dont le texte est accessible sur le site : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32013L0040.

10. Son site officiel : www.europol.europa.eu/ec3.

11. Lire à ce propos : *Liberté, Egalité... Sécurité* de Nicolas Arpagian, Dalloz, 2007.