Les multiples impacts stratégiques et déstabilisateurs du phénomène cyber

▶ *Entretien avec…*
Jean-Louis Gergorin *

*** Jean-Louis Gergorin,**
ancien directeur du Centre d'analyse et de prévision du Quai d'Orsay, est consultant industriel et donne un cours sur le nouveau bouleversement stratégique à Sciences Po Paris. Il mène une réflexion sur le phénomène cyber et son impact stratégique[1].

***Questions internationales** – Cybermenaces, cybertensions, cybersabotage, cyberespionnage, cyberguerres…, que recoupent exactement ces termes ?*

Jean-Louis Gergorin – Dans le cyberespace, il existe une gradation des interventions malveillantes.

Tout d'abord, en bas de l'échelle si je puis dire, on trouve des **hackers** et techniciens doués qui arrivent à pénétrer facilement, et exclusivement à des fins ludiques, des systèmes d'information. Les premiers hackers arrêtés par le FBI dans les années 1980 étaient des gamins surdoués, âgés de 15 à 18 ans, dont certains, par jeu, sont parvenus à entrer dans le système informatique du Pentagone ou dans celui de la NASA. Souvent, les hackers commencent leur activité par simple jeu puis sont ensuite recrutés par les États, les organisations criminelles ou les grandes firmes.

Deuxième niveau, **la cybercriminalité**. Devenue un business gigantesque et en croissance exponentielle, elle consiste pour un hacker à falsifier une identité, à voler des mots de passe, des empreintes électroniques, afin de pénétrer dans un système d'information. Dans cette catégorie, on trouve principalement les fraudes aux cartes de crédit et le hacking proprement dit. Le groupe Target, numéro trois de la grande distribution aux États-Unis, a ainsi été victime au cours de la période de Noël 2014 de hackers qui ont pillé les données confidentielles d'environ 40 millions de clients détenteurs de cartes de paiement. Le préjudice financier s'est alors doublé d'une atteinte à la réputation de l'entreprise. Des sociétés comme Apple ou Microsoft, qui conservent les coordonnées bancaires de centaines de millions de clients, sont particulièrement exposées.

À Londres, la plupart des grandes banques de la City ont fait l'objet de piratage de leur système d'information. Les pirates, une fois qu'ils ont pris le contrôle des systèmes d'information ou des données des clients, exigent le paiement d'une rançon dans la plus grande discrétion, généralement dans un paradis fiscal. Par crainte de perdre leur réputation et leurs clients, les banques se sont pliées la plupart du temps à ces extorsions et ces chantages.

Le crime organisé est derrière l'ensemble de ces activités de cybercriminalité, les réseaux étant souvent originaires d'Europe de l'Est, de Russie ou d'Asie. Certes, les banques et les

[1] Le texte qui suit est la retranscription d'une interview accordée par Jean-Louis Gergorin à la rédaction de *Questions internationales* le 3 mars 2017.

sociétés sont de mieux en mieux protégées mais les maîtres chanteurs sont de plus en plus inventifs et rapides.

Troisième catégorie, **le cyberespionnage**. Celui-ci peut avoir des visées économiques ou politiques, la frontière étant d'ailleurs très étroite entre les deux, puisque voler une information économique peut rapidement avoir des répercussions politiques. L'informatisation qui accompagne et nourrit la mondialisation depuis vingt ou trente ans est certes un eldorado économique, mais elle représente aussi un champ immense de vulnérabilité. Plus une entreprise est numérique et connectée, plus elle est vulnérable. Les occasions de cyberespionnage se sont donc multipliées ces dernières décennies.

Le cyberespionnage économique a rapidement attiré des entrepreneurs de tous horizons. Contrairement à une idée reçue, ce type d'activité ne vise pas uniquement des firmes internationales. Le grand spécialiste de cryptologie Guillaume Poupard, directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), a récemment souligné que l'essentiel du cyberespionnage en France était le fait d'entreprises en concurrence. Il en est de même aux États-Unis où certaines officines sont spécialisées dans ce type d'activités.

Dans le cyber, il n'existe pas de protection absolue et l'épée a toujours un coup d'avance sur le bouclier. Avec le développement du stockage des informations dans le *cloud* (nuage), un élément supplémentaire de vulnérabilité s'est en outre ajouté.

Dernier niveau dans notre typologie, **la cyberguerre** qui inclut les actions de cybersabotage. Sous ce vocable, on trouve les actions malveillantes destinées à paralyser les systèmes d'information civils et militaires ou les points névralgiques d'un État, comme ses infrastructures énergétiques ou de transport, en rendant inopérants ses liaisons et ses réseaux informatiques.

QI – Revenons au cyberespionnage. Pouvez-vous nous en donner quelques exemples et nous indiquer les liens économiques et politiques qui existent entre ces actions ?

J.-L. G. – Certains États, parmi lesquels ceux qui étaient le plus en retard d'un point de vue technologique comme la Chine, ont vite compris l'opportunité que représentait le cyberespionnage. Finies les Mata Hari chargées de séduire un ingénieur endetté pour lui extorquer des informations confidentielles ! Désormais, l'accès aux informations est beaucoup plus simple : il suffit juste de s'introduire à distance dans les systèmes d'information d'une entreprise ou de subtiliser des informations au moment de leur transfert par Internet.

En la matière, l'approche stratégique chinoise a été influencée par la doctrine d'Andrew W. Marshall, directeur de l'Office of Net Assessment au sein du département de la Défense des États-Unis entre 1973 et 2015. Selon Marshall, chaque puissance doit réaliser un bilan de ses forces et de ses faiblesses afin de mieux orienter ses choix stratégiques. Au terme de cette évaluation, les Chinois ont conclu que, s'ils devaient concurrencer les États-Unis sur le terrain des missiles balistiques ou du nucléaire, ils allaient rapidement épuiser leurs forces – d'où leur doctrine nucléaire qui est celle de la simple suffisance, assez curieusement proche de la doctrine française. Ils ont alors décidé de tout miser sur des domaines dans lesquels ils estimaient pouvoir rapidement surclasser les Américains, en particulier l'espace, les armes antisatellites et le cyber.

Il n'y a strictement aucun doute sur le fait que le cyberespionnage a constitué l'un des facteurs décisifs du rattrapage industriel chinois. La quantité d'informations obtenues par les Chinois ces dix ou quinze dernières années grâce au cyberespionnage est sans commune mesure avec ce que les Soviétiques ont récolté durant toute la guerre froide par des méthodes traditionnelles. C'est notamment le cas pour ce qui concerne l'aéronautique militaire ou les transports : le TGV chinois ressemble par exemple à s'y méprendre au TGV de Siemens, entreprise avec laquelle il existait des coopérations.

Les Russes se sont aussi très tôt lancés dans les activités de cyberespionnage. Les résultats sont toutefois moins visibles. Leur problème

En 2016, la Japan Network Security Association a organisé la cinquième édition du *Security Contest* (« SECCON »), une compétition de cybersécurité qui permet à des hackers « éthiques » débutants ou confirmés d'être confrontés individuellement ou en équipe à des mises en situation réelles (comme mener ou réagir à des cyberattaques, sécuriser des postes ou des réseaux, mener des investigations, etc.).

© Toru Yamanaka / AFP

est qu'ils ne peuvent pas, comme les Chinois, s'appuyer sur des entreprises aussi nombreuses ayant un niveau technologique très élevé ou étant aussi bien intégrées à l'économie mondiale.

QI – À plus ou moins long terme, ces activités de cyberespionnage ne passent pas inaperçues. Les Américains, qui en ont été avec les Européens les principales victimes, n'ont-ils rien entrepris afin de les endiguer ?

J.-L. G. – Les Américains ont en effet obtenu récemment une certaine forme d'« *Arms control* » en matière de cyberespionnage. Afin d'endiguer la vague de cyberespionnage dont ils faisaient l'objet de manière croissante, ils ont réagi « à l'américaine », c'est-à-dire en faisant intervenir leur appareil judiciaire dont on sait à quel point il est puissant.

Après plusieurs dénonciations, des enquêtes judiciaires ont été lancées en juillet 2013. Les services de renseignement américains ont été sollicités pour apporter des preuves, ce qu'ils ont fait en accumulant les preuves de hacking chinois à l'encontre de grandes entreprises américaines. Ces dernières ont alors été incitées à porter plainte.

Le procureur fédéral de Pennsylvanie, qui s'est spécialisé dans les affaires de cyberespionnage, a mis en examen des responsables chinois, y compris cinq militaires dont les photos ont été rendues publiques. La technique relève de ce que les Américains appellent le *name and shame*, c'est-à-dire identifier et faire honte. En fait, les États-Unis ont menacé les Chinois au portefeuille en leur demandant des dommages et intérêts et en les menaçant de saisir l'Organisation mondiale du commerce.

Face à cette perspective, un accord a été conclu en septembre 2015 : les deux pays ont accepté de renoncer mutuellement à utiliser des moyens étatiques pour des opérations de cyberespionnage au profit de leurs entreprises. Cet accord, qui représente un beau succès pour l'administration Obama, est le seul engagement de ce type qui existe au monde. Il est vrai que le marché américain reste essentiel pour les entreprises chinoises qui ne peuvent s'en passer. Depuis lors, on a assisté à une diminution spectaculaire des intrusions chinoises d'origine étatique aux États-Unis.

Les Américains ont tenté de faire de même avec la Russie, mais l'affaire a tourné court depuis l'annexion de la Crimée en 2014, qui a entraîné un regain des tensions entre les deux pays.

Quant à l'Europe, aucun accord équivalent n'existe. Pour que l'Allemagne et la France puissent peser dans le rapport de force, il faudrait qu'elles disposent d'un ensemble judiciaire unifié leur permettant de faire face aux multiples actions de cyberespionnage dont elles sont victimes.

QI – L'Estonie en 2007, la Géorgie en 2008, l'Ukraine en 2014, l'Allemagne en 2015, la Suède ou les États-Unis en 2016, toutes les cyberattaques dont ont été victimes ces pays appartiennent-elles au registre de la cyberguerre ? Ne placent-elles pas la Russie au cœur du phénomène ?

J.-L. G. – Dans la plupart des affaires où son nom est apparu, et qui sont davantage des opérations de cybersabotage que de cyberguerre, la Russie n'a fait aucun effort pour dénier son implication. Au moment de l'affaire dite *Podesta* – la dissémination des emails internes de l'équipe de campagne d'Hillary Clinton lors de la dernière campagne présidentielle américaine –, Moscou s'est contenté de déclarer qu'aucun organe officiel russe n'avait participé à cette opération…

Contrairement aux Chinois qui sont très focalisés sur la sphère militaire et l'espionnage, les Russes s'appuient sur un concept global. Développé en janvier 2013 par le général Valeri Guerassimov, chef d'état-major général des forces armées de la Fédération de Russie, il prévoit que les actions de la Russie s'inscrivent dans le cadre global de la « guerre non linéaire ». Ce concept, qui correspond à celui de « guerre hybride » de l'OTAN, recouvre l'ensemble des moyens de guerre, et notamment de l'information *(information warfare)*, qu'ils soient cybers ou non, permettant de déstabiliser l'adversaire.

Il y a de cela quelques décennies, certains États cherchaient à déstabiliser leurs ennemis

en les intimidant avec des attentats. Désormais, ils utilisent des actions de cybersabotage qui constituent en fait le premier degré de la cyberguerre, puisqu'ils visent à la neutralisation des systèmes informatiques et/ou des infrastructures de l'adversaire. Les Russes ne cachent pas avoir acquis une grande maîtrise des moyens cybers. Apparaître plus redoutables qu'ils ne le sont réellement en utilisant des moyens cybers est l'un des éléments de leur posture stratégique.

QI – Les États-Unis utilisent-ils également le cyberespionnage et/ou le cybersabotage ?

J.-L. G. – De nos jours, il ne me semble pas que les Américains utilisent des moyens étatiques importants, je dis bien étatiques, pour dérober des secrets commerciaux. En revanche, la NSA (National Security Agency) est depuis longtemps très active pour mettre en évidence les mauvaises pratiques des entreprises concurrentes des entreprises américaines et les dénoncer. Afin d'« égaliser le terrain de compétition » *(level the playing field)* entre entreprises américaines et non américaines, un terrain sur lequel la corruption a longtemps faussé la compétition économique dans certains pays, les États-Unis ont utilisé massivement le cyberespionnage pour mettre au jour les opérations de corruption et dénoncer les corrompus comme les corrupteurs.

Si l'on revient un peu en arrière, les États-Unis ont mis du temps à se lancer dans l'espionnage électronique, le signal intelligence. Il a fallu la Seconde Guerre mondiale et l'affaire Enigma[2] pour qu'ils prennent conscience de l'importance de cette dimension. Au sortir de la guerre, ils ont alors créé trois institutions majeures de l'appareil de sécurité américain, le National Security Council, la CIA (Central Intelligence Agency) et la NSA, cette dernière étant à l'origine dédiée aux interceptions hertziennes. Puis, les activités d'espionnage ont pris une importance colossale et les États-Unis ont acquis un sentiment de toute-puissance au fur et à mesure que leur volonté de tout savoir allait croissant.

Tout s'est effondré en 2013 avec l'affaire Snowden, qui a révélé au monde les pratiques américaines de collecte d'information à des fins de déstabilisation politique. Le fait que des informations qui devaient rester confidentielles aient été rendues publiques a alors eu un effet dévastateur pour l'ensemble du système de renseignement américain.

Concernant le cybersabotage et les cyberattaques, les Américains n'ont pas manqué d'y avoir recours sous l'administration Obama – notamment avec l'usage intensif de drones –, en particulier dans leur guerre contre l'organisation État islamique. Ces modalités d'intervention caractérisent même le principe de l'« empreinte légère » *(light footprint)* mis en avant par le Pentagone pour réduire à la fois le coût et les effets contre-productifs des déploiements américains à l'étranger, tout en maintenant à l'abri du regard de l'opinion américaine – et du reste du monde – l'implication militaire du pays.

Au début de la guerre d'Irak en 2003, les États-Unis avaient déjà « cyberneutralisé » le système irakien de défense aérienne avant de lancer leur offensive contre le régime de Saddam Hussein. Près de dix ans plus tard, ils ont longuement hésité à déclencher une cyberguerre totale contre la Syrie de Bachar al-Assad, mais ils y ont renoncé par crainte de ne pouvoir en contenir les dommages collatéraux.

Que l'on se rappelle ce qui s'est passé naguère en ex-Yougoslavie et au Kosovo, il suffisait de bombarder des voies ferrées ou des ponts pour maîtriser l'ennemi. Dorénavant, on peut empêcher les trains de rouler sans avoir à bombarder les voies ferrées.

De fait, en matière de cyberguerre, il n'existe que quelques États dans le monde qui se sont dotés d'une capacité importante de mener des opérations offensives cybers pour déstabiliser des infrastructures adverses : la Chine, les États-Unis, la Russie de manière certaine, très probablement l'Iran et Israël, plus récemment la France, le Royaume-Uni et l'Allemagne.

[2] La machine Enigma a été créée en 1919 par l'ingénieur allemand Arthur Scherbius pour chiffrer et déchiffrer des messages. Dès le début des années 1930, une partie de ses codes furent cassés par des mathématiciens polonais puis secrètement transmis aux Britanniques après l'invasion de la Pologne par l'Allemagne nazie. Au cours de la Seconde Guerre mondiale, la marine allemande continua à utiliser des machines Enigma, dites « machines M », devenues plus complexes et dont les clés furent néanmoins découvertes par les services alliés.

Dès le début des années 2010, ces États, et notamment les États-Unis et la Chine, ont toutefois compris qu'il convenait de ne pas aller trop loin par intérêt mutuel. Il existe donc entre eux une sorte d'accord implicite pour ne pas « cybersaboter » les infrastructures des uns et des autres. Le cybersabotage pourrait en effet avoir des conséquences catastrophiques : la destruction d'un système informatique qui gère le réseau électrique des hôpitaux entraînant leur paralysie, ou l'anéantissement du système de navigation aérienne d'un État seraient susceptibles d'être considérés comme des actes de cyberguerre majeurs.

QI – L'attaque menée contre l'Iran et ses centrifugeuses d'enrichissement d'uranium en 2010 via le virus Stuxnet ne constitue-t-elle pas, à cet égard, un acte de cyberguerre ?

J.-L. G. – Le virus Stuxnet, qui aurait été introduit par une clé USB pour retarder la montée en puissance des centrales nucléaires iraniennes, avait pour objectif de paralyser des installations et donc de causer des dommages sur le territoire d'un autre État souverain. En cela, certains le considèrent comme un acte de cyberguerre.

Dans ce genre d'opération, le problème est que les conséquences d'une cyberattaque sont parfois inattendues. Dès lors qu'il est entré dans un système informatique, un virus se répand sans contrôle, à l'instar d'une bactérie dans un corps vivant. En l'espèce, Stuxnet a affecté des dizaines de milliers d'ordinateurs en Iran mais aussi en Allemagne, en France ou en Inde.

À l'époque, les Russes ont aidé les Iraniens à détecter le virus puis à en stopper la progression. Les Iraniens, qui sont très doués en matière cyber, ont riposté en s'en prenant à l'Arabie saoudite et, plus précisément, en paralysant pendant près de trois jours les ordinateurs de la compagnie nationale saoudienne d'hydrocarbures Aramco. Puis, ils ont tenté de perturber la gestion informatique de certains barrages de l'État de New York, sans toutefois y parvenir. Les Américains ont alors mis plusieurs semaines pour identifier l'origine iranienne de cette tentative de cybersabotage.

QI – La frontière entre la réalité et la science-fiction apparaît à cet égard bien mince ?

J.-L. G. – Vous ne croyez pas si bien dire. Je vous recommande d'ailleurs le remarquable livre *Ghost Fleet* de Peter W. Singer et August Cole, paru en 2015. Ce roman d'anticipation met en scène un conflit mondial opposant, dans les années 2020, la Chine et la Russie aux États-Unis. Les auteurs imaginent qu'un régime nationaliste chinois, parvenu au pouvoir après un coup d'État, fait monter les tensions dans le Pacifique, à tel point que les Américains décident d'instaurer un embargo contre la Chine.

Intervient alors un véritable « cyber Pearl Harbor » : grâce à une première attaque uniquement électronique, cybernétique et spatiale, les Chinois parviennent à neutraliser l'intégralité des systèmes satellitaires américains. Les sous-marins américains sont alors repérés et neutralisés, la flotte américaine est anéantie à partir de l'espace et une coalition sino-russe envahit avec succès Hawaï. Tandis que les Européens et les Japonais proclament leur neutralité, seuls les Australiens, les Canadiens et la Nouvelle-Zélande soutiennent les Américains.

Au-delà de l'anecdote, ce roman, qui a servi de support à de nombreux séminaires et sessions de formation des soldats américains, a aussi été abondamment commenté dans les réunions du National Security Council où, dans l'éventualité d'un conflit sino-américain, les scénarios en vogue semblent privilégier un affrontement cyber, spatial et faiblement conventionnel plutôt que nucléaire.

QI – Revenons à une réalité plus immédiate, quels vous semblent être les principaux défis à venir ?

J.-L. G. – Ce qui me semble certain, c'est que les moyens cybers démultiplient les opportunités et que la numérisation joue au profit du faible et au détriment du fort. Je m'explique : au départ, les Américains et avec eux l'ensemble des observateurs ont estimé que le cyber était l'affaire des grandes puissances. Or, il n'en est rien, bien au contraire. Les réseaux sociaux, les messageries cryptées et les smartphones sont en effet devenus les moyens de communication,

de renseignement et de commandement « du pauvre ».

De nos jours, la puissance de calcul d'un smartphone est supérieure à celle des ordinateurs qui ont mis au point la bombe H américaine en 1953. Les réseaux sociaux permettent des centaines de millions de communications par jour qui sont, en raison du cryptage, de plus en plus difficiles à intercepter ou à contrôler.

Inventée par deux Russes, l'application de messagerie cryptée Telegram fait par exemple de la sécurité des communications son principal argument de vente. Comptant désormais plus de 100 millions d'utilisateurs dans le monde, son usage est privilégié par les jihadistes de l'organisation État islamique pour échanger en toute impunité et pour propager leurs idées au plus grand nombre. Même l'opérateur ne peut intercepter les informations qui sont diffusées. Pour le moment, l'avantage est incontestablement à ceux qui cryptent plutôt qu'à ceux qui décryptent.

Le cyber a donc un fort pouvoir égalisateur entre les acteurs des relations internationales. Le hacking et l'utilisation des réseaux Internet comme vecteurs de propagande et de recrutement compliquent fortement la tâche des États en matière de sécurité intérieure comme extérieure. Sur le plan stratégique, ce défi va devenir essentiel dans les années à venir. La disparition probable du califat syro-irakien laissera certainement des poches de résistance sur le terrain. Dans le même temps, il y a fort à parier que les mouvements jihadistes éclatent en différents groupuscules dispersés dont la cohérence stratégico-opérationnelle sera assurée par des communications cybercryptées.

Dans sa lutte contre les réseaux terroristes, la nouvelle administration Trump veut rétablir les liens de collaboration directe avec la Silicon Valley, lesquels avaient été mis à mal au moment de l'affaire Snowden.

QI – Que pensez-vous des événements qui ont entouré la dernière campagne présidentielle américaine ?

J.-L. G. – Il convient tout d'abord de bien distinguer entre les cyberattaques à proprement parler et la diffusion d'informations fausses ou présentées de manière à nuire à la réputation d'un individu ou à celle d'une organisation. En l'espèce, la dernière campagne présidentielle américaine a donné lieu à des opérations d'utilisation de moyens cybers pour déstabiliser le camp démocrate et influencer le vote des électeurs plutôt qu'à des opérations de cybersabotage proprement dites, qui auraient consisté à essayer de fausser les résultats, notamment en hackant les machines à voter.

Le fait de révéler dans une campagne électorale des informations confidentielles sur l'un des candidats, en l'occurrence Hillary Clinton, n'a en soi rien de nouveau. Montrer que le Parti démocrate est aux mains de riches sponsors et de Wall Street, et que l'appareil du parti a cherché à éliminer le candidat Bernie Sanders durant les primaires aurait pu venir des révélations d'une secrétaire dans la presse et non du hacking de mails. Ce qui a été nouveau et, dans le cadre d'une élection aussi serrée, a suffi à provoquer des changements à la marge qui ont pu faire pencher la balance du côté de Donald Trump, fut la diffusion au compte-gouttes, sur Internet, d'informations confidentielles déstabilisant Hillary Clinton.

Certaines manipulations numériques ont aussi joué un rôle important dans l'issue du scrutin. La société Cambridge Analytica a ainsi travaillé avec l'équipe de campagne de Donald Trump pour cibler très précisément des internautes (psychométrie). Des algorithmes puissants auraient permis à cette société, selon ses responsables, de prédire, à partir d'un certain nombre de *likes* et de *dislikes*, la couleur de peau (certitude à 95 %), l'orientation sexuelle (à 88 %) ou les convictions politiques (à 85 %) des détenteurs de comptes Facebook.

La société a alors envoyé aux électeurs noirs ou aux ouvriers des *Swing States* les informations les plus défavorables à Hillary Clinton : par exemple, ses discours complaisants à l'égard du monde de la finance et de Wall Street ou des extraits d'un discours de 1994 dans lequel elle défendait la politique sécuritaire de son mari et évoquait – à propos des jeunes délinquants (en grande majorité afro-américains) – des « préda-

teurs qu'il fallait envoyer en prison ». Ce faisant, Cambridge Analytica, et derrière elle l'équipe de campagne républicaine, n'avait pas pour objectif que les électeurs noirs votent pour Donald Trump, mais qu'ils s'abstiennent. Le pari semble avoir réussi puisque le taux d'abstention chez les Noirs a été beaucoup plus fort dans les *Swing States* tels que le Michigan et le Wisconsin que lors des deux précédents scrutins présidentiels, cette abstention entraînant la victoire de justesse de Trump dans ces États...

QI – La difficulté de l'attribution des attaques dans le cyberespace ne constitue-t-elle pas le problème central ?

J.-L. G. – Cette question de l'attribution des attaques est en effet un grand problème. Non que l'on ignore qui se cache en général derrière les attaques, mais parce qu'il est extrêmement difficile de le prouver et, *a fortiori*, d'entamer des poursuites. En fait, ce qui peut paraître surprenant, est qu'il est assez facile de remonter à la source de la plupart des opérations cybers. Les autorités et organismes chargés de la détection de telles opérations disposent d'outils de traçabilité : il existe en effet chez les hackers des signatures et des méthodes reconnaissables – à l'instar de cambrioleurs qui utilisent toujours le même mode opératoire.

Les Américains ont ainsi rapidement identifié les auteurs de l'opération *Podesta* en 2015. De nombreuses attaques ont été attribuées aux groupes de hackers russes surnommés APT28 et APT29 qui seraient respectivement liés aux services de renseignement militaire (GRU) et intérieur (FSB) russes. Lors de la cyberattaque menée en avril 2015 contre la chaîne de télévision francophone TV5 Monde, qui donnait fréquemment la parole à l'opposition russe et qui a conduit à un black-out total de la chaîne pendant vingt-quatre heures, l'opération a ainsi pu être rapidement attribuée au groupe APT28, bien qu'elle ait été menée sous le faux drapeau du cyberjihad.

QI – Qu'en est-il de la France justement ? A-t-elle pris des mesures contre les menaces cybers ?

J.-L. G. – Dès le Livre blanc sur la défense et la sécurité nationale de 2008, les cybermenaces ont été clairement identifiées et hissées au rang de priorité nationale. S'en est suivie la mise en place d'une stratégie de défense active, comprenant le besoin de développer des « capacités offensives ». En 2009 a été créée une Agence nationale de la sécurité des systèmes d'information (ANSSI) qui assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, en particulier sur les réseaux de l'État français.

Cette mobilisation s'est renforcée dans les cinq dernières années, notamment sous l'impulsion du ministre de la Défense Jean-Yves Le Drian. Il a décidé en 2016 de créer un commandement interarmées de la lutte informatique, le commandement cyber des Armées. S'y ajoutent l'ANSSI, chargée auprès du Premier ministre de la protection des systèmes, et la direction technique de la Direction générale de la sécurité extérieure (DGSE), chargée du renseignement cyber et hertzien. Ces trois structures disposent de moyens croissants. Leurs maîtres mots sont désormais « riposte et neutralisation », selon les termes de Jean-Yves Le Drian. ■