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).