No 224, Avril 2018, éditeur: Fabien Merz

La cybersécurité dans les relations sino-américaines

Le cyberespace et le cyberespionnage représentent une source de tensions et de mésentente entre les États-Unis et la Chine. En 2015, les deux puissances ont pourtant réussi à trouver un accord sur la cybersécurité. L'objectif: stabiliser leur relation et réduire les risques de malentendu à propos d'activités menées dans le cyberespace.

Par Marie Baezner

La relation entre la Chine et les États-Unis s'inscrit dans la dynamique des rapports de concurrence entre grandes puissances. De fait, si les deux pays sont rivaux sur les plans militaire, politique et économique, leurs interactions évoluent au fil des ans. Le nouveau gouvernement américain a une approche politique plus étroite que ses prédécesseurs vis-à-vis de la Chine. De surcroît, l'administration du président Donald Trump ne semble pas avoir de stratégie globale pour traiter les questions liées à la Chine. La relation entre les deux pays reste régulièrement ponctuée de provocations dans le monde physique (revendications territoriales chinoises dans les mers de Chine orientale et méridionale menaçant les alliés et partenaires des États-Unis dans ces régions) comme dans le cyberespace (campagnes de cyberespionnage).

Un bâtiment à Shanghai qui hébergerait la cyber-unité «61398» de l'armée chinoise.
Carlos Barria / Reuters

Depuis vingt ans, les tensions entre les deux puissances s'intensifient sur plusieurs questions de cybersécurité: la Chine et les États-Unis ont mené des activités de cyberespionnage mutuel (voir la liste), la Chine n'est pas d'accord avec le modèle américain de gouvernance de l'internet et la Chine met à profit ses capacités militaires et cybernétiques croissantes pour créer des zones d'interdiction/de déni d'accès. Pour réduire ces tensions, les deux pays ont conclu en septembre 2015 un accord bilatéral contraignant sur la cybersécurité dans lequel ils s'engagent à ne pas perpétrer ni soutenir d'activités de cyberespionnage économique.

Campagnes de cyberespionnage

La première campagne de cyberespionnage des États-Unis attribuée à un acteur étatique chinois a été découverte en 2004. Elle visait le ministère américain de la Défense et des entreprises du secteur de la défense. À ce jour, au moins quatorze campagnes de cyberespionnage découvertes aux États-Unis ont été attribuées à des acteurs étatiques chinois. Ils ont ciblés des institutions publiques, l'armée, des entreprises des secteurs de l'informatique, des télécommunications et de l'énergie, des journalistes et des militants et volé des informations sensibles et des éléments soumis à la propriété intellectuelle. Selon un rapport de 2014, ces vols de propriété intellectuelle auraient représenté une perte de 250 milliards de dollars par an pour l'économie américaine. Il convient cependant de remettre cette somme en perspective car elle n'inclut pas les préjudices pour la réputation des entreprises, la perte d'avantages concurrentiels et les investissements réalisés dans la cyber-

Campagnes de cyberespionnage

2003 – 2006: Titan Rain – Espionnage de l'armée et d'institutions des États-Unis par la Chine.

2006 – 2010: Shady RAT – campagne de cyberespionnage chinois.

2007 – 2009: GhostNet – Espionnage d'ONG et de missions tibétaines par la Chine.

2008 – 2014: Hikit – Espionnage de journalistes, d'entreprises informatiques, d'instances universitaires et d'institutions gouvernementales par la Chine.

2008 – 2011: Byzantine Hades – Espionnage d'institutions des États-Unis par la Chine.

2009 – 2011: Night Dragons – Espionnage d'infrastructures critiques des États-Unis par la Chine.

2009 – 2010: Opération Aurora – Espionnage de Google, Adobe et d'autres entreprises informatiques par la Chine.

2009 – (probablement toujours en cours): Fourth Party Collection de la NSA – Espionnage par les États-Unis de pirates chinois ciblant le ministère américain de la Défense.

2010 – 2014: Opération Shotgiant – Espionnage de Huawei par les États-Unis.

2011 – 2013: Opération Beebus – Espionnage de fournisseurs du ministère américain de la Défense par la Chine.

2013 – 2015: Opération Iron Tiger – Espionnage par la Chine d'entreprises américaines et asiatiques des secteurs de l'informatique, des télécommunications et de l'énergie.

2014 – 2015: Campagne d'espionnage du Bureau de la gestion du personnel des États-Unis (OPM) par la Chine.

L'accord de 2015

1. Répondre aux demandes d'information et d'assistance concernant des cyberactivités malveillantes.
2. Enquêter sur les actes de cybercriminalité émanant des territoires respectifs des signataires.
3. Se tenir mutuellement informés de l'avancement de ces enquêtes.
4. Ne pas se livrer au cyberespionnage à des fins économiques ou au vol de propriété intellectuelle contre l'autre pays, ni soutenir de telles activités.
5. Déployer des efforts pour établir et promouvoir des normes internationales de comportement des États dans le cyberespace.
6. Créer un mécanisme conjoint de dialogue de haut niveau sur la lutte contre la cybercriminalité et les questions associées.
7. Instaurer une ligne directe pour discuter des aspects liés aux cyberactivités.

sécurité pour arrêter les intrusions. Par ailleurs, il est possible que le nombre d'entreprises touchées soit plus élevé, car beaucoup ne signale pas les intrusions par peur d'entacher leur réputation.

En 2013, Edward Snowden a mis au jour le programme américain de surveillance massive d'internet et les campagnes de cyberespionnage menées par les États-Unis contre la Chine. Il a révélé que les États-Unis avaient espionné des entreprises informatiques et des banques chinoises, ainsi que des dirigeants du Parti communiste. Du fait du manque de données, il est toutefois difficile d'évaluer les pertes économiques résultant du cyberespionnage américain en Chine et de déterminer si les États-Unis poursuivent de telles activités.

Le désaccord entre les deux puissances sur le cyberespionnage portait essentiellement sur la nature des campagnes menées. Les États-Unis effectuent la distinction entre le cyberespionnage au service de la sécurité nationale et le cyberespionnage à des fins économiques. Si le premier est toléré au niveau international, le deuxième ne l'est pas. On considère en effet que le renseignement visant à assurer la sécurité nationale fait partie intégrante de la responsabilité d'un État de protéger sa population et son territoire contre les menaces étrangères – ce qui n'est pas le cas du renseignement économique. Les autorités américaines ont déclaré que leurs campagnes de cyberespionnage étaient uniquement destinées à la sécurité nationale, et non à visée économique. Le gouvernement chinois a, quant à lui, nié toute activité de cyberespionnage. Ce désaccord a renforcé la méfiance entre les deux puissances, ainsi que le risque d'interpréter à tort des cyberactivités comme des actes de guerre.

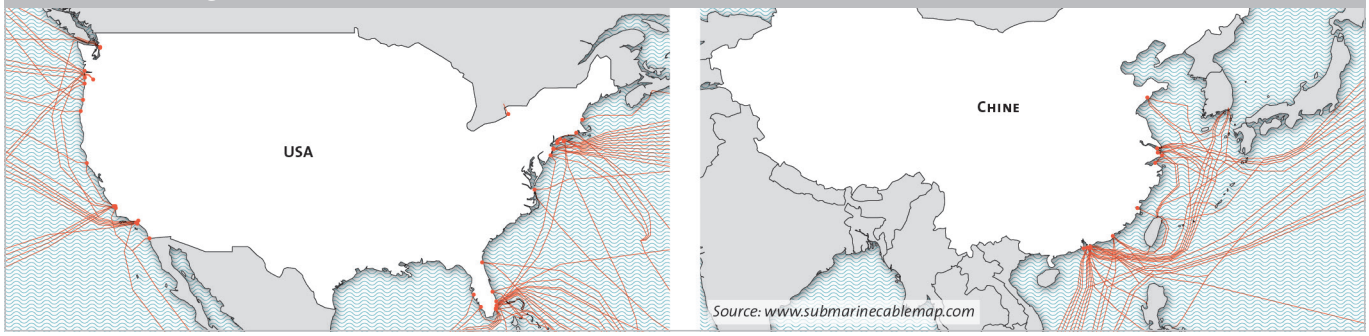
Des groupes affiliés à l'Armée populaire de libération (APL) ont mené un grand nombre de campagnes de cyberespionnage. Si le vol de propriété intellectuelle a permis à l'APL de développer des technologies sans avoir à investir dans la recherche, il semble que l'organisation ait eu du mal à transformer les informations volées en avantages concurrentiels. La première raison avancée serait due à la structure organisationnelle de l'APL. Alors qu'elle était submergée d'informations soumises à la propriété intellectuelle acquises lors des campagnes de cyberespionnage, l'APL ne parvenait pas à utiliser efficacement ces renseignements du fait de sa bureaucratie extrêmement compartimentée. L'APL a également eu plus de difficultés à imiter et reproduire parfaitement les nouvelles technologies qui sont devenues plus complexes au fil des ans.

L'accord de 2015

Les États-Unis ont tenté d'adopter une position plus dure à l'encontre des campagnes de cyberespionnage chinoises. Pour montrer qu'ils n'avaient pas l'intention de laisser les cyberattaques contre leurs entreprises impunies, ils ont inculpé en mai 2014 cinq membres de l'APL. Il s'agissait essentiellement d'un acte symbolique, dans la mesure où les cinq agents sont restés en Chine et n'ont donc jamais été emprisonnés. Après le piratage de leur Bureau de la gestion du personnel (OPM, *Office of Personnel Management*), les États-Unis ont également averti les autorités chinoises qu'ils envisageaient de prendre des sanctions économiques et des mesures diplomatiques. Cependant, les révélations d'Edward Snowden en 2013 ont entaché la crédibilité et la légitimité de leurs actions dans le cyberespace auprès de leurs alliés et de leurs concurrents. Mais si elles ont renforcé les tensions entre la Chine et les États-Unis, ces révélations ont surtout offert l'occasion de régler la question de la cybersécurité en dévoilant les pratiques des deux pays.

La solution pour réduire cette pression a pris la forme d'un accord bilatéral destiné à mettre en place des mesures de confiance dans le cyberespace. Dans cet accord conclu en 2015, les deux nations se sont engagées à ne pas perpétrer ni soutenir d'activités de cyberespionnage économique. L'accord prévoyait également des rencontres régulières entre les représentants des agences de sécurité des deux États pour échanger des informations sur la cybercriminalité, ainsi que la création d'une ligne directe pour communiquer sur les questions de cybersécurité (voir la liste de mesures). Cette entente a été vue comme une avancée en faveur de la coopération entre les États-Unis et la Chine sur les questions de cybersécurité – ceci dans l'espoir de réduire les risques de malentendu (interprétation d'une cyberattaque comme un acte de guerre) et d'escalade (transformation des tensions en guerre conventionnelle) dans le cyberespace. L'accord a été considéré comme une victoire pour les États-Unis, qui ont amené le gouvernement chinois à accepter la différence entre les activités de cyberespionnage à visée économique et celles au service de la sécurité nationale. Les autorités chinoises, qui demandaient depuis des années un ren-

Points d'atterrage des câbles sous-marins aux États-Unis et en Chine



forcement de la coopération sur la cybercriminalité, ont aussi accueilli favorablement cette initiative. En effet, des entreprises et des citoyens chinois étaient régulièrement pris pour cibles par des cybercriminels, et les autorités chinoises reprochaient aux pays occidentaux leur réticence à collaborer aux enquêtes.

Après l'accord de 2015

Dans un premier temps, les experts américains en cybersécurité ont noté une nette diminution du nombre de cyberattaques lancées par des acteurs étatiques chinois contre des cibles économiques américaines. En revanche, ils ont observé une hausse des attaques émanant d'autres pays. Selon eux, quatre hypothèses pourraient expliquer cette évolution. Premièrement, il se peut que des hackers chinois aient utilisé des proxys situés dans d'autres pays pour atteindre des cibles aux États-Unis. Deuxièmement, l'accord a peut-être poussé les hackers chinois à utiliser des techniques plus sophistiquées et plus difficiles à détecter dans le cyberespace. Troisièmement, il est possible que les hackers chinois aient redirigé leurs cyberattaques vers des cibles plus faciles en dehors des États-Unis. Enfin, peu après la signature de l'accord, les autorités chinoises ont mené une vaste campagne anticorruption au sein de leur administration et de l'APL. Il se peut que cette campagne ait découragé certains employés à continuer de mener des cyberattaques pour compléter leur salaire.

Toutefois, l'objectif de l'accord n'était pas de mettre un terme à tout cyberespionnage, mais seulement aux campagnes à motivation économique. Les activités traditionnelles de cyberespionnage au service de la sécurité nationale ont continué. Des groupes de hackers chinois liés au gouvernement ont été repérés alors qu'ils ciblaient des entreprises américaines de technologies à double usage travaillant avec le gouvernement des États-Unis et des entreprises du secteur maritime menant des activités en rapport avec la mer de Chine méridionale. L'administration Obama était au courant que des hackers Chinois testaient les « lignes rouges » de l'accord de 2015. Les hackers visaient des entreprises qui auraient aussi pu être considérées comme des cibles d'intérêt pour la sécurité nationale. En août 2017, le Bureau du représentant américain au commerce lança une enquête sur ces cas de cyberespionnage.

Même s'il semble avoir réduit le volume de cyberattaques en provenance de la Chine pendant les premières années, l'accord de 2015 présente certaines limites. Sa mise en œuvre est difficile à évaluer et le nombre de cyberattaques est compliqué à estimer précisément. En effet, toutes les victimes ne se signalent pas et il faut souvent du temps pour percer à jour les campagnes de cyberespionnage. De surcroît, ni le gouvernement américain, ni les autorités chinoises ne peuvent exercer un contrôle total sur chaque individu présent sur leur territoire. Aucune des deux parties ne serait en mesure d'empêcher des citoyens de mener une cyberattaque qui pourrait être interprétée par l'autre partie comme un acte exécuté ou soutenu par les autorités de l'État. En outre, l'accord de 2015 sur la cybersécurité ne prévoit pas de mesures coercitives. En effet, aucune sanction n'est prévue dans le cas où une des parties vient à mener ou soutenir des activités de cyberespionnage économique contre l'autre. Enfin, il est difficile de distinguer le cyberespionnage économique du cyberespionnage au service de la sécurité nationale. Un pays peut déclarer avoir réalisé une campagne de cyberespionnage pour des raisons de sécurité nationale contre une entreprise, mais ce ne sera pas facile à justifier. C'est particulièrement vrai pour les États-Unis, car les entreprises chinoises appartiennent souvent à l'État, ce qui complique la distinction entre les deux types de cyberespionnage.

Au niveau international, l'accord de 2015 sur la cybersécurité a d'abord été perçu comme un signe positif. Il a montré que ces questions pouvaient avoir des solutions diplomatiques. Par ailleurs, il aurait pu constituer un premier pas vers l'internationalisation de normes sur la cybersécurité, si un nombre suffisant d'États avait décidé de conclure des pactes similaires. Depuis 2015, le Royaume-Uni et l'Australie ont signé des accords comparables avec la Chine.

En octobre 2017, les États-Unis et la Chine ont annoncé ensemble leur volonté de continuer à respecter leur accord de 2015. Cependant, en Mars 2018, le Bureau du représentant américain au commerce a publié son rapport d'enquête sur les campagnes de cyberespionnage chinois depuis 2015. Le rapport démontre que les hackers chinois n'ont pas respecté l'accord de 2015 en menant des opérations de cyberespionnage économique sur des firmes américaines. L'annonce de la publication du rapport a fait suite à la déclaration du président Trump sur l'imposition de taxes à l'importation de produits chinois. Néanmoins, il n'est pas encore clair si la présidence américaine prendra d'autres mesures à l'encontre de la Chine. Le rapport est la première déclaration officielle américaine sur l'échec de l'accord de 2015. La publication de ce rapport risque aussi de décourager d'autres pays de signer un accord sur la cybersécurité avec la Chine.

La gouvernance de l'internet

Deux autres questions restent sources de tensions. La première concerne la gouvernance internationale de l'internet. Développeurs historiques de la toile, les États-

Unis ont imposé leur approche de gouvernance à la communauté internationale. Internet est actuellement géré par l'ICANN *(Internet Corporation for Assigned Names and Numbers),* une organisation à but non lucratif basée à Los Angeles. L'ICANN est dirigée par des représentants des principales parties prenantes (techniciens et entreprises informatiques) et des utilisateurs d'internet. Cette structure ascendante laisse peu de place à la contribution des États. Parmi ses fonctions, l'ICANN règlemente les aspects techniques de la structure d'internet comme l'attribution des adresses web, la gestion des serveurs racines et le développement des protocoles internet. En octobre 2016, le ministère américain du Commerce n'a pas prolongé le contrat qui régissait sa supervision des activités de l'ICANN.

Cette transition n'a rien changé au fonctionnement d'internet, mais elle a permis à l'ICANN d'être réellement indépendante dans ses processus de décision. La Chine, la Russie et d'autres pays critiquent toutefois cette approche de gouvernance multipartite et ascendante, affirmant qu'elle continue de servir les renseignements et les intérêts des États-Unis. Ils préféreraient un modèle de gouvernance qui donne plus de poids aux États, comme c'est le cas au sein de l'Union Internationale des Télécommunications, par exemple. Ces pays craignent que les États-Unis interfèrent dans leur gestion nationale d'internet. Depuis 1996, le gouvernement chinois contrôle strictement le contenu d'internet sur son territoire par le biais de sa «Grande Muraille numérique». Cet outil fonctionne comme un filtre qui empêche les personnes se trouvant en Chine d'accéder à certains sites web. En effet, le gouvernement chinois a peur qu'un accès illimité aux informations étrangères déstabilise l'ordre social et politique du pays. Les autorités chinoises accusent régulièrement les États-Unis de tenter d'influencer et d'occidentaliser sa population à travers internet. Le gouvernement chinois utilise ainsi depuis mars 2015 un «Grand canon», cyber outil offensif qui permet de censurer certains sites web en redirigeant le trafic internet vers un site internet particulier et en provoquant son effondrement par déni de service distribué (DDoS). Ce type d'attaque consiste à saturer un site web de visites. Or, l'accord de 2015 ne couvre pas la question de la gouvernance de l'internet, qui ne peut être traitée dans le cadre d'un accord bilatéral, mais plutôt d'une initiative internationale.

Zones A2/AD

Un deuxième point de désaccord réside dans la mise en place par la Chine de zones d'interdiction/de déni d'accès (A2/AD, *Anti-Access/Area Denial*) dans les mers de Chine orientale et méridionale. Les zones A2/AD sont une approche de défense asymétrique consistant à utiliser tous les domaines militaires pour empêcher ou dissuader un adversaire d'entrer dans une zone. La Chine a conscience qu'elle ne peut pas rivaliser avec les États-Unis dans une guerre conventionnelle complète. Pour assurer sa liberté de mouvement en mer, elle a donc mis en place ces zones destinées à limiter la projection de la force américaine dans ces régions. Afin de sécuriser ces zones, la Chine a non seulement modernisé son arsenal militaire, mais aussi amélioré ses cybercapacités en vue de contrôler l'espace d'informations en cas de conflit. L'objectif est d'altérer l'aptitude d'un adversaire à communiquer avec ses troupes et à les contrôler en coupant la localisation GPS et/ou les communications. La Chine a déjà montré qu'elle était capable de perturber le fonctionnement des satellites par des moyens conventionnels et cybernétiques. Elle a détruit l'un de ses anciens satellites en 2007 et piraté un satellite météorologique américain en 2014.

Comme on pouvait l'attendre, les États-Unis, qui ont des alliés et des partenaires dans la région, n'ont pas vu d'un bon œil l'instauration de zones A2/AD dans les mers de Chine orientale et méridionale. En réponse à cette initiative, ils ont créé le *Joint Operational Access Concept et l'AirSea Battle Operational Concept*. Ces deux concepts prévoient le déploiement d'un grand nombre de sous-marins équipés de missiles à longue portée en coordination avec des cyberopérations pour détruire les centres de commandement et de contrôle et contrer les systèmes de missiles chinois.

En théorie, le dispositif A2/AD pourrait aussi être appliqué au cyberespace. Le concept, également appelé cyberblocus, consiste à refuser l'accès à internet ou à perturber le flux d'informations d'un adversaire. L'un des moyens d'y parvenir serait de lancer des cyberattaques sur les points d'échange internet (interconnexions entre les réseaux internet) pour les rendre inopérants. Un autre serait d'altérer les infrastructures internet physiques (câbles, serveurs, points d'échange, etc.).

En cas d'escalade entre la Chine et les États-Unis, l'un des pays pourrait tenter d'interdire à l'autre d'accéder à internet en ralentissant ou en interrompant le flux d'informations vers et depuis les centres de commandement et de contrôle militaires. Pour ce faire, il pourrait agir sur les câbles sous-marins ou terrestres, ou sur les satellites de communication. Cela étant, il ne sera pas facile pour les États-Unis de déconnecter la Chine d'internet. La Chine comptant plus d'une dizaine de stations d'atterrage (stations où les câbles sous-marins sont connectés au réseau terrestre), les États-Unis devraient toutes les couper simultanément pour être efficaces (voir carte). La Chine aurait tout autant de mal à intervenir sur les stations d'atterrage américaines. Si les pays n'agissent que sur un petit nombre de câbles, l'accès à internet pourrait être ralenti, mais l'impact serait vraisemblablement insignifiant. Les pays pourraient aussi attaquer les satellites de communication, mais cela ne suffirait pas non plus à couper l'accès d'un adversaire à internet.

Le développement de telles zones et l'intégration du cyberespace comme domaine militaire témoignent ainsi d'un changement de discours: on s'éloigne de l'idée d'un «cyber Pearl Harbor», c'est-à-dire une cyberattaque très dévastatrice, pour s'orienter vers une approche plus pratique et doctrinale de la cybersécurité.

Marie Baezner est chercheuse au sein de l'équipe Cyberdéfense du Center for Security Studies (CSS), intégré à l'ETH de Zurich. Elle est coauteure de plusieurs «CSS Cyber Defense Hot Spot Analyses» sur les cyberincidents et les cyberaspects des conflits actuels.

Les analyses de politique de sécurité du CSS sont publiées par le Center for Security Studies (CSS) de l'ETH Zurich. Deux analyses paraissent chaque mois en allemand, français et anglais. Le CSS est un centre de compétence en matière de politique de sécurité suisse et internationale.

Editeurs: Christian Nünlist, Matthias Bieri, Fabien Merz, Benno Zogg
Traduction: Consultra; Relecture: Fabien Merz
Layout et graphiques: Miriam Dahinden-Ganzoni
ISSN: 2296-0228; DOI: 10.3929/ethz-b-000254542

Feedback et commentaires: analysen@sipo.gess.ethz.ch
Téléchargement et abonnement: www.css.ethz.ch/cssanalysen