La stratégie des « Trois guerres » de la Chine ou comment atténuer les retombées du cyberespionnage

Emilio Iasiello*

D'aucuns accusent la Chine d'avoir lancé, il y a quelque temps déjà, une campagne d'espionnage informatique à l'encontre d'une série de pays, dont les États-Unis. Le pays fait, à ce titre, l'objet de vives critiques. La mauvaise presse qui découle de ces activités alimente la perception selon laquelle la « montée en puissance » de la Chine à l'échelle mondiale repose sur la volonté de ses dirigeants de se faire une place parmi les grandes puissances mondiales en volant subrepticement la propriété intellectuelle de ses concurrents, et peut-être de pouvoir ainsi rivaliser avec les États-Unis sur le terrain militaire régional et mondial. Afin de combattre cette perception, le présent article pose le postulat que la Chine a mis à profit sa stratégie des « Trois guerres » – guerre de l'information à trois volets s'articulant autour de composantes médiatiques, juridiques et psychologiques afin d'influencer la communauté internationale, et les États-Unis en particulier – dans l'objectif d'empêcher l'élaboration et la mise en œuvre de toute contre-stratégie. Le résultat lui a, jusqu'à présent, été largement favorable, et a permis à la Chine d'atteindre les jalons énoncés dans ses plans nationaux de développement, tout en échappant aux sanctions diplomatiques et économiques de la part de la communauté internationale, y compris celles imposées par les États-Unis en matière de cyber-espionnage. Le présent article examine l'activité cybernétique de la Chine, les perceptions internationales de la menace cybernétique chinoise et la façon dont sa stratégie des « Trois guerres » s'applique aux cyber-opérations. Nous formulons, sur cette base, une série de conclusions.

*Fort de plus de 12 ans d'expérience en tant qu'analyste stratégique en renseignement cybernétique, Emilio Iasiello collabore avec divers organismes de renseignement civils et militaires du gouvernement américain, ainsi qu'avec le secteur privé. Il a donné plusieurs exposés sur la cyber-menace lors de congrès nationaux et internationaux et a publié de nombreux articles dans des revues évaluées par des pairs.

IASIELLO, Emilio, « China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities », *Journal of Strategic Security* 9, n° 2, 2016, pp. 45-69. DOI : http://dx.doi.org/10.5038/1944-0472.9.2.1489. Accessible à l'adresse : http://scholarcommons.usf.edu/jss/vol9/iss2/4

La cyberactivité chinoise

Le général Keith Alexander, ancien directeur de l'Agence nationale de sécurité (NSA) et commandant du sous-commandement interarmées de combat en charge de la sécurité de l'information (U.S. Cyber Command), estime les pertes encourues par les États-Unis en raison des activités de cyber-espionnage à quelque 338 milliards de dollars[1]. Si ces pertes ne sont certes pas toutes dues aux efforts chinois, il reste évident que la Chine, identifiée comme le principal acteur du cyber-espionnage à l'échelle mondiale, est soupçonnée d'être à l'origine d'une bonne partie de cette activité[2]. L'ampleur de ces activités de cyber-espionnage soulève la question suivante : en dépit des avantages découlant du vol d'informations sensibles et exclusives que dénonce la communauté internationale, quel est le plan stratégique de Pékin ?

La Chine a trois objectifs principaux en matière de sécurité nationale : assurer la survie du régime, défendre la souveraineté nationale et l'intégrité territoriale et s'élever au rang de puissance régionale et internationale[3]. La position de la Chine vis-à-vis des États-Unis traduit un prudent mélange de scepticisme, de volonté de collaborer et de rivalité. Les Chinois considèrent les États-Unis comme une puissance révisionniste cherchant à réduire leur influence politique et à nuire à leurs intérêts[4]. L'une des façons de contrer la suprématie américaine consiste, pour la Chine, à s'engager dans des opérations cybernétiques dans le but de soutirer des informations de nature « diplomatique, économique et industrielle qui soutienne les programmes de défense des États-Unis[5] ». Dans ce contexte, on peut considérer que les opérations cybernétiques visent davantage à renforcer le noyau dur de la Chine qu'à réduire le pouvoir américain. Se concentrant uniquement sur les États-Unis, les cyber-espions chinois ont notamment ciblé les industries suivantes au cours des deux dernières années : l'espace[6], les infrastructures[7], l'énergie[8], l'énergie nucléaire[9], les entreprises technologiques[10], l'énergie propre[11], la biotechnologie[12] et les soins de santé[13].

Le 12e Plan quinquennal de la Chine reflète les objectifs globaux du gouvernement afin de promouvoir la croissance économique. Il s'agit d'un outil d'une importance cruciale qui permet de tracer, par cycles de cinq ans, les progrès du pays au moyen de lignes directrices, de cadres stratégiques et d'objectifs pour les décideurs à tous les niveaux de gouvernement[14]. Dans son Plan quinquennal actuel, qui couvre la période 2011-2015, la Chine a identifié sept secteurs prioritaires à développer, dans lesquels les États-Unis ont, en général, été un innovateur et un chef de file. Ces « industries stratégiques émergentes » sont censées devenir l'épine dorsale de l'économie chinoise dans les décennies à venir[15]. Ces industries sont :

- Nouvelles énergies (nucléaire, éolienne, solaire)
- Conservation de l'énergie et protection de l'environnement (objectifs de réduction de la consommation d'énergie)
- Biotechnologie (médicaments et dispositifs médicaux)

- Nouveaux matériaux (terres rares et semi-conducteurs haut de gamme)
- Nouvelles technologies de l'information (réseaux à large bande, infrastructure de sécurité Internet, convergence des réseaux)
- Fabrication d'équipements haut de gamme (équipements aérospatiaux et de télécommunications)
- Véhicules à énergie propre[16]

Une corrélation peut être facilement établie entre les types d'industries ciblées aux États-Unis au cours des deux dernières années et les industries émergentes stratégiques mises en avant par la Chine. De plus, la Chine voit la cybernétique comme un outil idéal pour atteindre ces objectifs en raison du caractère peu coûteux de la technique et de la facilité qu'elle offre en permettant d'atteindre plusieurs cibles potentielles de renseignement à la fois. En février 2007, la revue *China National Defense News* a défini la cyber-guerre comme « l'utilisation de la technologie et des méthodes en réseau à des fins de collecte d'informations dans les domaines politique, économique, technologique et militaire[17] ». Le principal avantage est que la cyber-guerre est directement liée à l'« avantage de l'information » et non à l'avantage militaire, ce qui suggère que les cyber-activités en temps de paix visent davantage à soutenir le développement de la Chine dans des domaines stratégiques et moins à établir une supériorité militaire à travers la reconnaissance d'un futur champ de bataille.

La perception de la menace cybernétique chinoise

Si certains experts estiment que les États-Unis, ainsi que la Chine et la Russie, sont engagés dans une course aux armements cybernétique[18], la Chine n'a pas encore été impliquée dans un incident portant sur la destruction de systèmes d'information ou des informations qui s'y trouvent, ni suspectée de l'avoir été. De nombreux ouvrages militaires stratégiques chinois préconisent l'utilisation de la guerre de l'information comme arme préventive avant le début des engagements militaires[19]. Toutefois, si la Chine est bel et bien à l'origine du volume des activités de cyber-espionnage qui lui sont attribuées, elle préfère tirer parti des intrusions informatiques comme moyen de collecte d'informations et d'avantages commerciaux en temps de paix plutôt que comme arme de dissuasion.

Actuellement, plusieurs pays, dont l'Allemagne, l'Australie, le Canada, l'Allemagne, l'Inde, Taiwan et le Royaume-Uni, ont publiquement accusé la Chine d'intrusion sur les réseaux de leurs secteurs public et privé[20]. De façon plus spécifique, les États-Unis sont depuis une douzaine d'années la cible principale des cyber-opérations orchestrées ou dirigées par la Chine. Alors que le gouvernement américain a maintenu une position réservée pendant la plus grande partie de cette période, en 2012, il s'est prononcé plus ouvertement sur le volume des activités de cyber-espionnage visant ses secteurs public et privé. En octobre 2011, Mike Rogers, membre du Congrès des

États-Unis et du Comité permanent de la Chambre des représentants sur le renseignement, a accusé publiquement la Chine d'avoir volé des informations sensibles :

> L'espionnage économique de la Chine a atteint un niveau intolérable et je crois que les États-Unis et nos alliés en Europe et en Asie ont le devoir de faire obstacle à Pékin et d'exiger que le pays mette un terme à cette piraterie[21].

En 2013, la société de sécurité Mandiant a publié un rapport détaillé identifiant une unité militaire chinoise impliquée dans le cyber-espionnage[22]. Jamais auparavant les preuves et analyses techniques établissant un lien entre ce type d'activités et une entité gouvernementale n'avaient été rendues publiques. Le rapport Mandiant a été un tournant décisif pour les hauts responsables du gouvernement américain, et plusieurs d'entre eux, dont le président Obama, ont évoqué publiquement la question de l'espionnage informatique chinois. Peu après la publication du rapport, en mars 2013, le conseiller à la sécurité nationale des États-Unis, Thomas Donilon, a déclaré :

> ... les entreprises expriment leur plus grande préoccupation à l'égard du vol ciblé et organisé d'informations commerciales confidentielles et de renseignements propriétaires exclusifs opéré par l'intermédiaire d'intrusions cybernétiques provenant de la Chine[23].

Au cours du même mois, le président Obama a interpellé directement le président chinois Xi Jinping au sujet de la cyber-sécurité et des futures opportunités de collaboration[24]. Cet entretien s'est suivi d'un sommet en juin au cours duquel les deux dirigeants ont discuté plus longuement de la cyber-sécurité[25]. Cependant, aucun progrès n'a été réalisé en mai 2014 lorsque le département de la Justice des États-Unis a accusé cinq officiers militaires chinois de cyber-espionnage. Ce fut la première fois que le gouvernement américain accusait publiquement des membres d'un gouvernement étranger de crimes contre des entreprises américaines[26]. D'autres rapports portant le groupe Axiom, un autre groupe chinois soupçonné d'espionnage dont les pratiques étaient réputées plus élaborées que celles décrites dans le rapport Mandiant, dressent un portrait peu reluisant de la Chine en tant que cyber-espion coupable de vols incessants d'informations sensibles[27]. Compte tenu du grand nombre de cyber-incidents indiquant un certain degré d'implication du gouvernement chinois, Pékin tente de maintenir son image de « montée en puissance pacifique » au milieu de la bronca grandissante de la communauté internationale, les États-Unis en tête, qui menacent d'imposer des cyber-sanctions contre les auteurs d'activités d'espionnage commercial.

La stratégie des « Trois guerres »

Il semble contre-productif pour un pays si soucieux de son « image » de s'engager dans des activités aussi flagrantes, aussi agressives et aussi nuisibles à sa réputation. Le *guanxi* et le *mianzi* sont deux concepts essentiels de la culture chinoise. Le premier, le *guanxi*, a été défini comme le partage des faveurs entre les individus, les

connexions et les relations et la capacité à exercer une influence. Le second, le *mianzi*, signifie la « face », comme dans les expressions sauver la face, perdre la face, voire montrer son (vrai) visage[28]. Alors, pourquoi donc un pays imprégné de cet état d'esprit risquerait-il volontairement d'écorner son image, surtout à un moment où le pays est considéré comme une puissance économique mondiale en pleine expansion ? La mise en œuvre d'opérations non cinétiques, non violentes, mais néanmoins offensives est la meilleure solution, en temps de paix, pour la stratégie chinoise d'influencer les processus cognitifs des dirigeants et de la population d'un pays, ou ce que Sun Tzu décrit comme « maîtriser l'ennemi sans se battre[29] ». En 2003, le Comité central du Parti communiste chinois et la Commission militaire centrale ont approuvé le concept des « Trois guerres », un outil de guerre d'information non militaire destiné à être utilisé par l'Armée populaire de libération avant et pendant les hostilités[30]. À elles trois, ces guerres permettent à la Chine d'entrer dans n'importe quel conflit, que ce soit en temps de paix ou de guerre, en bénéficiant d'un avantage politique qui pourra utilisé pour influencer l'opinion publique ou internationale[31]. Ces trois guerres sont :

- *Guerre psychologique* — La guerre psychologique affaiblit la capacité d'un ennemi à mener des opérations de combat par l'intermédiaire d'opérations visant à dissuader, déstabiliser et démoraliser le personnel militaire ennemi et à soutenir les populations civiles[32].
- *Guerre de l'opinion publique/médiatique* — Influence l'opinion publique nationale et internationale pour obtenir le soutien des actions militaires de la Chine et dissuader un adversaire de mener des actions contraires aux intérêts de la Chine[33].
- *Guerre juridique* — Utilise le droit international et national pour revendiquer une position de supériorité juridique ou faire valoir les intérêts chinois. Elle peut être utilisée pour entraver la liberté opérationnelle d'un adversaire et agencer l'espace opérationnel. La guerre juridique a également pour but d'obtenir le soutien de la communauté internationale et de gérer les répercussions politiques possibles des actions militaires de la Chine[34].

La guerre médiatique intègre le mécanisme des messages à transmettre, tandis que la guerre juridique justifie la raison des actions menées. La guerre psychologique apporte les nuances nécessaires en tirant parti de la capacité de diffusion des médias et des mécanismes juridiques plus formels pour démontrer le bien-fondé des activités auprès des publics nationaux et internationaux. Étant donné que chacun de ces types de guerre repose sur le ciblage et l'influence d'un public cible spécifique, il est facile de comprendre pourquoi les analyses chinoises associent presque toujours ces trois types de « combat »[35].

Guerre de l'opinion publique/médiatique

La guerre de l'opinion publique renvoie à l'utilisation de divers canaux d'information, y compris Internet, la télévision, la radio, les journaux, les journaux, les films et d'autres formes de médias, conformément à un plan d'ensemble et à des objectifs définis. Elle vise à transmettre des informations minutieusement sélectionnées à un public cible[36]. Les objectifs sont de préserver le moral des troupes, d'obtenir l'appui du public de la population nationale et à l'étranger, d'affaiblir la volonté de l'ennemi de combattre et de modifier son appréciation de la situation. La guerre défensive de l'opinion publique est utilisée pour neutraliser les effets possibles sur la population chinoise[37]. Compte tenu des nombreuses allégations de piratage informatique portées contre la Chine, la guerre défensive de l'opinion publique est un contrepoids naturel. Selon Cheng, quatre thèmes sont inhérents aux écrits chinois sur l'opinion publique[38] :

- *Suivre une orientation descendante (top-down)* — La haute direction dictera les mesures à prendre en fonction des objectifs stratégiques.
- *Mettre l'accent sur la préemption* — Les analyses chinoises de la guerre de l'opinion publique soulignent que « le premier à se faire entendre s'empare du peuple, le premier à s'engager assoie sa domination (*xian sheng duoren, xianru weizhu*).
- *Souplesse et réactivité face à l'évolution des conditions* — Utilisation de différentes activités de propagande selon le public visé. « Il convient de faire la distinction entre les éléments les plus têtus et le reste de la population de façon générale ».
- *Exploiter toutes les ressources disponibles* — Les ressources civiles et commerciales telles que les agences de presse, les installations de radiodiffusion, les utilisateurs d'Internet, etc. sont considérées comme une ressource inestimable pour faire passer le message de la Chine auprès des publics nationaux et internationaux.

Les premières critiques à l'égard des intrusions soutenues par Pékin ont fait surface dans l'opinion publique dès 2005, lorsqu'il a été révélé que des intrusions présumées du gouvernement chinois, appelées « *Titan Rain* », visaient depuis 2003 des acteurs des secteurs public et privé américains[39]. Depuis lors, de nombreux gouvernements étrangers se sont exprimés publiquement pour dénoncer les activités intrusives du gouvernement chinois ou de ses agents[40]. De plus, les entités du gouvernement américain soupçonnent depuis longtemps les sociétés de télécommunications chinoises Huawei et ZTE d'être des instruments de l'état, et des intermédiaires utilisés par le gouvernement chinois pour collecter des renseignements[41]. Ce débat s'est invité dans les plus hautes sphères de l'état, comme en 2013 lors des rencontres entre le président chinois Xi Jinping et le président américain Barack Obama[42]. En 2014, le secrétaire d'état à la Défense Charles Hagel a révélé à la Chine la structure et les capacités des cyber-forces américaines dans un effort de transparence militaire[43].

Applications au cyberespace de la guerre de l'opinion publique et médiatique de la Chine

La réponse chinoise a évolué au cours de cette période, où elle a été présentée comme une présence cybernétique ennemie. La Chine a généralement réagi à ces accusations en adoptant une attitude défensive, niant les allégations et demandant des compléments d'informations dans le but d'aider à retrouver les auteurs. Ainsi, des déclarations officielles de haut niveau émanant du ministère chinois de la Défense[44], du ministère des Affaires étrangères[45] et de son Premier ministre[46] se sont inscrites dans la ligne de conduite du parti, soutenant que la Chine n'est pas derrière les attaques, que le pays était une victime et non l'auteur de ces activités cybercriminelles, et que les lois chinoises considèrent, sans restriction, le piratage informatique comme un acte comme illégal condamnable[47].

La Chine a toutefois adopté une position plus affirmée lorsque l'ancien entrepreneur de la NSA, Edward Snowden, a publié des documents présumés hautement confidentiels exposant les activités de surveillance des États-Unis à l'échelle mondiale. Au lieu d'essayer de détourner les accusations, la Chine pointe maintenant le gouvernement américain du doigt. Pékin a même exigé des explications aux États-Unis sur de possibles activités d'espionnage de la compagnie chinoise Huawei par la NSA[48]. Un comble compte tenu des soupçons du gouvernement américain à l'égard des activités d'espionnage commises par la société Huawei au nom du gouvernement chinois. Notons toutefois que la véracité des allégations américaines n'a pas été démontrée par l'enquête diligentée pour le compte des États-Unis par Mike Rogers, membre du Congrès et du Comité permanent de la Chambre des représentants sur le renseignement[49]. En dépit de la persistance des sceptiques, la Maison-Blanche a procédé à sa propre enquête de sécurité de Huawei en octobre 2012 et n'a trouvé aucune preuve démontrant que Huawei espionnait les États-Unis au nom du gouvernement chinois[50]. En mars 2014, l'équipe nationale chinoise d'intervention d'urgence informatique a identifié les États-Unis comme la principale source d'intrusion contre ses ordinateurs[51].

Les efforts déployés par les États-Unis pour gérer leur image publique n'ont pas été à la hauteur des attentes, les alliés et les adversaires ayant exprimé leur indignation face au scandale dévoilé par Snowden[52]. La nuance subtile sur laquelle le gouvernement américain fonde sa défense, à savoir que le pays mène ces activités pour assurer la sécurité nationale et non pour procurer un avantage concurrentiel aux sociétés américaines, semble éculée, surtout après avoir été pris la main dans le sac cybernétique. Plusieurs accusations ont été portées à la suite de fuites de documents indiquant que la NSA espionnait des entités de sécurité non nationales, dont la plus grande compagnie pétrolière brésilienne[53], le commissaire de l'Union européenne en charge d'une enquête sur les sociétés Google, Microsoft et Intel[54], le Fonds monétaire international

et la Banque mondiale[55]. Même sur le sol américain, les groupes d'intérêts publics et spéciaux qui défendent les libertés civiles ont condamné les activités de la NSA[56].

Alors que les États-Unis semblaient avoir l'avantage et le soutien de la communauté internationale à l'égard des soupçons d'espionnage cybernétique de la Chine, le pays a réussi à redorer son blason. Elle continue de se présenter comme une cyber-victime et un partenaire coopératif en matière de cyber-sécurité. En 2014, la Chine a exprimé son souhait d'une coopération cybernétique avec les États-Unis[57] et, depuis avril 2014, le Pentagone a engagé des échanges militaires avec la Chine dans un esprit de transparence militaire[58].

Malgré les allégations persistantes de malveillances cybernétiques à son égard, la Chine est donc parvenue à améliorer son image, au détriment des cyber-activités secrètes américaines. Peut-être en réaction à se revirement, le département de la Justice des États-Unis a inculpé pour cyber-espionnage en mai 2014 cinq pirates informatiques militaires chinois[59]. Bien que cette décision historique visât à démontrer l'implication directe du gouvernement chinois dans le cyber-espionnage, elle n'a pas davantage incriminé la Chine aux yeux du grand public. Après tout, de nombreuses organisations publiques et privées partent généralement du principe que le gouvernement chinois s'approprie des propriétés intellectuelles et collecte des informations sensibles. À l'inverse, la sortie massive de documents hautement sensibles révélant le rôle du gouvernement américain dans des activités similaires (contre les gouvernements alliés et ennemis) a été perçue comme une injustice bien plus grande et comme un comportement indigne de la part d'un gouvernement prônant les droits de l'homme et les libertés individuelles.

Guerre juridique

La guerre juridique est l'un des instruments clés de la guerre psychologique et de la guerre de l'opinion publique[60]. Souvent, elle est utilisée conjointement à l'un ou aux deux autres types de guerre : elle est plus efficace en association avec une autre. De cette façon, la guerre juridique fournit la base qui renforce la guerre de l'opinion publique et la guerre psychologique[61]. Par définition, la guerre juridique est destinée à justifier une ligne de conduite. Deux influences alimentent la guerre juridique menée par la Chine :

- *Position de la Chine sur le rôle et la primauté du droit* — Des considérations historiques et culturelles éclairent la perception du gouvernement chinois en matière de guerre juridique. Le confucianisme et les influences légalistes faisaient partie intégrante de la Chine impérialiste, mais au fur et à mesure du mandat de Mao et de l'évolution du gouvernement, les perspectives marxistes ont préconisé que « la loi devrait servir d'instrument idéologique à la poli-

tique[62] ». Aujourd'hui, l'accent est mis sur le droit commercial et le droit des contrats, tandis que le droit pénal reste en retrait[63].

- *Perception de la Chine de la guerre juridique en Occident* — La Chine tient compte de cette importance aux yeux des Occidentaux lorsqu'elle justifie ses actions par le droit. Lors de la première guerre du Golfe, les États-Unis ont obtenu l'autorisation de l'ONU de recourir à des sanctions et à la force en Irak, tandis qu'au Kosovo, ils ont soutenu que leurs actions étaient « conformes à la loi » parce qu'elles étaient prises sous les auspices de l'OTAN[64]. Cette capacité à utiliser la primauté du droit ou ses perceptions juridiques pour justifier ses actions est un puissant outil de la pensée chinoise.

Applications au cyberespace de la guerre juridique de la Chine

En tant que mode d'influence, la guerre juridique est généralement utilisée avant le déclenchement d'un conflit physique, et ne survient que dans le contexte d'une guerre réelle. Toutefois, depuis que les projecteurs internationaux se sont tournés vers les activités de cyber-espionnage et que la Chine a été accusée d'être l'auteur de vols de propriété intellectuelle, il semble que les Chinois se servent peut-être des principes de la guerre juridique pour défendre leurs intérêts stratégiques. Les événements suivants se sont produits après que plusieurs gouvernements ont publiquement blâmé la Chine pour avoir piraté leurs réseaux et volé des données :

- *2014 — Les États-Unis projettent d'abandonner le contrôle de l'Internet* — En décembre 2012, la Chine et la Russie ont obtenu un soutien international pour que tous les états jouissent de droits égaux sur la gouvernance de l'Internet. L'accord a revu les règles de télécommunications de l'ONU, dont la création remontait à 24 ans[65]. S'il n'est pas contraignant, 89 pays l'ont signé, 55 se réservant le droit de le signer à une date ultérieure[66], ce qui témoigne d'un large soutien. Cette initiative a poursuivi les mesures nécessaires pour que l'Union internationale des télécommunications (UIT) joue un rôle actif dans le modèle multipartite de l'Internet[67]. Ces efforts, conjugués à la fuite de documents sensibles concernant la prétendue surveillance mondiale de la National Security Agency, ont exercé une pression considérable sur les États-Unis pour qu'ils renoncent à soutenir l'Internet Corporation for Assigned Names and Numbers (ICANN) et son influence sur le contrôle du trafic Internet[68]. L'obtention d'un soutien international et l'utilisation de l'UIT en tant qu'organe autorisé ont conféré à ces efforts une évidente légitimité. En janvier 2016, les responsables américains ont réitéré leur volonté de renoncer au contrôle fédéral sur la gouvernance d'Internet d'ici septembre[69].
- *2011/2015 — Lettres de la Chine et de la Russie aux Nations Unies* — Comme il n'existe pas de lois internationales officielles ni même de définitions communes

régissant les activités cybernétiques, la Chine a été un fervent défenseur de la mise sur pied de bonnes pratiques pour les états nations. En 2011, la Chine s'est associée à la Russie, au Tadjikistan et à l'Ouzbékistan pour présenter un code de bonne conduite international sur la sécurité de l'information à l'ONU[70], qui a été mis à jour en janvier 2015[71]. En substance, le cœur des deux propositions mettait l'accent sur l'identification des droits et des responsabilités des états dans l'espace de l'information, ainsi que sur la promotion de comportements constructifs et responsables dans le but de renforcer leur coopération en matière de lutte contre les menaces et de défis communs à relever. Bien qu'au moment de la rédaction du présent article, la proposition soit toujours en cours d'examen par les états membres, la Chine a joué un rôle de premier plan à l'échelle internationale en essayant d'établir des normes de bonne conduite pour les états nations en faisant appel à un organisme international pour légitimer ses efforts.

- *2009 — Mise à jour de la législation chinoise sur la cybercriminalité* — La Chine soutient publiquement que le piratage informatique est contraire aux lois chinoises[72]. En 2009, la Chine a étendu les peines infligées aux personnes reconnues coupables d'activités cybercriminelles[73]. Lorsqu'elle est accusée de parrainage de piratage, la Chine est prompte à invoquer ses propres lois pour justifier légalement pourquoi elle ne se livre pas à cette activité[74].

La Chine fait appel à des organisations internationales comme l'ONU, dont l'autorisation est étayée par des arguments juridiques, pour légitimer ses efforts. Cette approche sert deux objectifs stratégiques majeurs : 1) Elle tempère l'image négative de la Chine en tant qu'état pirate en démontrant qu'elle cherche à travailler collectivement et dans le cadre des règles définies par les organisations internationales établies, et 2) elle aide la Chine à mettre en œuvre des moyens asymétriques non cinétiques pour poursuivre ses objectifs politiques et économiques, en évitant le besoin d'utiliser la force ou l'influence militaire, réduisant ainsi le risque d'escalade potentielle sur une question donnée.

La guerre psychologique de la Chine

La guerre psychologique est profondément enracinée dans la stratégie chinoise. Par exemple, « les positions chinoises affirment qu'en temps de paix, les opérations psychologiques cherchent à révéler et à exploiter les divisions de l'establishment politique ou de l'alliance interne de l'ennemi et à remettre en cause les valeurs de l'ennemi[75] ». Elle vise un degré de précision élevé dans le ciblage des points critiques afin d'obtenir des effets non linéaires.

Applications au cyberespace de la guerre psychologique de la Chine

Selon les spécialistes chinois, la guerre psychologique fait partie intégrante de la guerre de l'information[76]. Toutefois, il est plus difficile de définir la guerre de l'information dans un contexte chinois, car il n'existe pas de doctrine publiée sur la guerre de l'information et nous ne disposons que d'écrits chinois pour comprendre cette discipline complexe. Les premiers écrits sur le sujet ont été largement empruntés aux doctrines en vigueur aux États-Unis, en Russie, en France et en Allemagne[77]. Au fil du temps, la pensée chinoise en matière de guerre de l'information s'est développée, notamment à l'égard du concept de « domination de l'information », qui, selon James Mulvenon, cyber-expert chinois, est le principal objectif de la stratégie chinoise de guerre de l'information[78]. La domination de l'information a deux objectifs principaux : l'infrastructure de l'information physique et les données qui l'ont traversée et, de façon peut-être encore plus importante, les agents humains qui interagissent avec ces données, en particulier ceux qui prennent des décisions[79].

Selon les écrits chinois, il y a cinq grandes tâches associées à la guerre psychologique[80]. Compte tenu de la participation de la Chine à l'activité d'intrusion mondiale, ces composantes peuvent être appliquées à l'environnement actuel de la manière suivante :

1. *Souligner la légitimité de son propre camp* — La Chine est très soucieuse de son image publique, ce qui incite à s'interroger sur son ambivalence envers la publicité négative entourant ses activités de piratage. Toutes les tentatives visant « à blâmer et à faire honte » à la Chine se sont soldées par un échec retentissant, qui peut être attribué au fait que la Chine a établi et maintenu la même position officielle, quel que soit le gouvernement qui la pointe du doigt. Elle pare généralement ce type d'argument en réfutant systématiquement les allégations de piratage et en soulignant immédiatement qu'elle est elle-même victime du piratage[81]. Par ailleurs, comme nous l'avons déjà mentionné, Pékin n'hésite pas à rappeler que le piratage informatique est illégal en Chine, essayant ainsi de montrer qu'en tant que pays, elle mène aussi des actions par voie légale visant à mettre fin aux activités malveillantes dans le cyberespace[82]. Enfin, la Chine, en partenariat avec la Russie, le Tadjikistan et l'Ouzbékistan, a proposé aux Nations Unies un code de bonne conduite dans le cyberespace pour les états nations[83], qu'elle a mis à jour en février 2015 après avoir reçu la contribution des états membres[84]. Deux objectifs importants ont ainsi été atteints :
    i) Cela a montré que la Chine a été proactive dans sa tentative d'établir un ensemble international de normes de bonne conduite pour les états nations dans le cyberespace ; et
    ii) Cela a démontré la volonté de la Chine de collaborer avec les autres sur un pied d'égalité. La proposition soumise à l'ONU a également mis en exergue la volonté de la Chine d'obtenir un consensus au sein

de la communauté internationale. Pris collectivement, ces efforts peuvent être interprétés comme une tentative d'atténuation de la presse négative dont la Chine a fait l'objet en se présentant comme une nation responsable et coopérative en matière de cyber-sécurité. Ce désir de collaborer avec d'autres gouvernements sur ces questions a peut-être incité les États-Unis, en juin 2015, à accepter de négocier avec la Chine un « code de bonne conduite » dans le cyberespace[85].

2. *Exploiter ses avantages* — En 2014, la Chine est devenue la plus grande économie du monde. Son produit intérieur brut a connu une croissance exponentielle de 2003 à 2013, atteignant en moyenne annuelle plus de dix pour cent[86]. Bien que les États-Unis aient empêché les entreprises chinoises de s'implanter sur les marchés américains, la Chine ne s'est pas privée de conquérir d'autres marchés où les États-Unis jouissaient historiquement d'un avantage commercial. Récemment, la Chine a dépassé les États-Unis en devenant le premier partenaire commercial de l'Afrique et du Brésil[87]. Ce changement des rapports de force s'est traduit par des avantages économiques certains, qui n'ont donc en rien subi l'influence des allégations de piratage dont la Chine a fait l'objet. Ces pays ne se soucient tout simplement pas de la menace, estimant que l'activité économique et le développement accéléré de leurs infrastructures l'emportent sur toute conséquence potentielle. Le Brésil accueille de plus en plus de clients privés chinois et ces derniers jouent un rôle majeur dans la diversification de la coopération économique bilatérale[88]. En Afrique, la Chine est le premier fournisseur d'équipements de télécommunications[89]. Les accusations adressées à la société chinoise de télécommunications Huawei constituent un parfait exemple de la façon dont la Chine exploite ses points forts. Malgré les soupçons, exprimés en grande partie par le gouvernement américain, selon lesquels Huawei pourrait agir en tant qu'agent du gouvernement chinois, l'étude menée par la Chambre des représentants n'a fourni aucune preuve attestant d'une quelconque activité illicite d'espionnage. En outre, l'entreprise est « le deuxième plus grand fournisseur de télécommunications au monde, avec des produits et des solutions déployés dans plus de 140 pays, ce qui indique qu'un grand nombre de pays ne sont pas aussi préoccupés que ne semblent l'être les États-Unis par la menace que Huawei pose en matière de renseignement[90]. » Même les alliés américains, l'Australie et le Royaume-Uni, ne semblent pas s'inquiéter outre mesure. Le Conseil consultatif de Huawei au Royaume-Uni – une entité composée à la fois de membres du personnel du Quartier général des communications du gouvernement (GCHQ), de fonctionnaires, d'acteurs du secteur et de membre du personnel de Huawei – a conclu après un audit que les activités commerciales de Huawei au Royaume-Uni ne constituaient pas une menace de sécurité nationale[91]. En 2013, Huawei a soutenu la création d'un

centre de cyber-sécurité en Australie pour tester les systèmes d'identification des infrastructures critiques[92].

3. *Miner l'opposition* — Plusieurs articles ont été écrits sur la cyber-menace de la Chine par des experts civils et gouvernementaux, régionaux, culturels et fonctionnels, en plus des médias internationaux et des chaînes d'information de la presse écrite traitant du sujet. Dans chaque cas, deux messages retentissants sont transmis : 1) La menace cybernétique chinoise est massive et omniprésente, représentant le plus important transfert de richesses de l'histoire de l'humanité[93]. 2) La Chine cherche à accéder à des réseaux informatiques non seulement pour voler des informations sensibles, mais aussi pour asseoir sa « domination de l'information[94] ». Qu'elle soit sophistiquée, rudimentaire ou quelque part entre ces deux pôles, l'activité d'espionnage de la Chine a été constante et persistante. Même le terme « menace persistante avancée », qui lui aurait été attribué par l'U. S. Air Force en 2006 pour pouvoir en discuter avec des membres du personnel non tenu aux règles de confidentialité[95], décrit l'adversaire comme compétent, implacable et, compte tenu de son manque de couverture, intrépide. Le fait que les cyber-opérateurs chinois présumés n'aient subi que peu de conséquences de leurs actions renforce l'idée qu'ils ne peuvent pas être battus ou, à tout le moins, que leur activité effrontée ne peut être endiguée. Comme l'a dit Richard Clarke, « chaque grande entreprise aux États-Unis a déjà fait l'objet d'une intrusion chinoise[96] ». Venant d'un homme considéré comme le premier tsar cybernétique du gouvernement américain, de tels propos font passer la Chine comme un adversaire pratiquement imbattable.
4. *Encourager la dissension dans le camp de l'ennemi* — Cette tâche consiste à perturber les processus cognitifs des décideurs politiques et des décideurs, ce qui entrave leur capacité à élaborer un plan d'action. La théorie suggère que la meilleure stratégie est d'attaquer l'esprit de l'ennemi, le laissant incapable de planifier[97]. Compte tenu de l'historique des décideurs politiques américains de ne pas être en conformité avec les questions cybernétiques, cette stratégie en fait une cible de premier choix. Une chose est certaine : depuis l'apparition en 2003 des premiers soupçons d'espionnage[98], aucun plan d'action concret n'a été établi avant la mise sur pied par les États-Unis de sanctions cybernétiques ; un effort visant à décourager toutes les activités cybernétiques de façon générale, et en particulier celles qui seraient menées ou approuvées par la Chine[99]. Auparavant, les organismes apportaient leur appui à diverses mesures. Il y avait ainsi les partisans de la « cyber-défense active », comme le Cyber Command des États-Unis[100] et la Defense Advanced Research Projects Agency[101]. Il s'agit essentiellement d'un moyen de dissuasion. D'autres, cependant, à l'image de Mike Rogers, membre du Congrès, étaient davantage en faveur de la mise en place préalable d'une ligne de défense solide et viable[102]. D'autres encore,

comme le Government Accountability Office (GAO), ont dénoncé l'absence de rôles et de responsabilités clairement définis au sein des organismes fédéraux, indiquant qu'il s'agissait d'un obstacle sérieux à toute politique de cybersécurité efficace[103]. L'incapacité persistante à mettre en place une stratégie nationale solide en matière de cyber-sécurité empêche le gouvernement des États-Unis d'adopter une approche unifiée et cohérente, qui implique toutes les parties prenantes et où chacun comprend le rôle qui lui est attribué dans le processus. Même le décret de février 2013 sur l'amélioration de la cybersécurité des infrastructures critiques n'a pas pu rassembler le soutien nécessaire. Bien qu'il s'agisse d'une mesure positive, ce décret n'a pas permis d'instaurer des changements significatifs, obligeant l'état à ne compter que sur le bon vouloir des entreprises. Bien qu'il n'ait pas mentionné le décret de février, le GAO, dans un rapport publié en mars, a quand même fait état de la nécessité d'une stratégie nationale intégrée en matière de cyber-sécurité, avec des jalons, des mesures de rendement et un contrôle du Congrès[104]. Que ce soit intentionnellement ou non, les campagnes de cyber-espionnage de la Chine ont profité du climat d'indécision qui régnait au sein du gouvernement américain avant l'accord conclu en 2015 entre les deux gouvernements.

5. *Instaurer des défenses psychologiques* — La Chine a également recours à d'attaques psychologiques afin de démontrer l'inefficacité des efforts de ses adversaires[105]. Le pays a toujours maintenu sa position politique en affirmant qu'elle ne se livrait pas au cyber-espionnage. Même lorsqu'il a été interpellé directement au sujet des activités d'espionnage de son pays, le président chinois Xi Jinping a détourné l'accusation en évoquant la mauvaise sécurité du réseau. Ainsi, lorsque le programme de surveillance de la NSA a été dévoilé, la Chine a immédiatement saisi l'occasion de pointer le gouvernement américain du doigt[106]. Même le géant chinois des télécommunications, Huawei, pourtant tant critiqué, en a profité pour condamner l'espionnage de la NSA et promouvoir un dialogue mondial sur la cyber-sécurité[107].

En considérant ces cinq composantes de la guerre psychologique, on ne peut que conclure que la Chine est une force cybernétique dominante. En niant les accusations qui lui sont adressées, le pays s'appuie sur cette image sans devoir le dire publiquement ou divulguer dans la presse son implication dans un événement cybernétique majeur. En définitive, contrairement aux États-Unis, la Chine n'a pas éprouvé le désir ou la nécessité de renforcer son image en tant qu'acteur dominant du cyberespace par le biais d'annonces publiques ou de stratégies nationales. De son côté, Pékin a profité de l'attitude des autres pays spéculant sur ses capacités et sa force pour concentrer ses efforts sur l'amélioration de son image, tout en maintenant ses activités d'espionnage pour servir ses intérêts nationaux.

Éviter les cyber-sanctions américaines

Bien que l'activité chinoise de cyber-espionnage jouisse d'une relative liberté depuis un certain temps déjà, la visite d'état de 2015 a fait comprendre à la Chine que les États-Unis ne toléreraient pas le cyber-espionnage à des fins commerciales. Afin d'éviter des sanctions, Pékin est parvenu à un accord quelques jours avant la visite officielle du Président Xi aux États-Unis, dans lequel les deux parties ont convenu qu'« aucun des gouvernements de ces deux pays ne mènera ou soutiendra sciemment le vol cybernétique de propriété intellectuelle, en ce compris les secrets de fabrication et toute information commerciale jugée confidentielle, dans le but de procurer des avantages concurrentiels aux entreprises ou aux secteurs de leur pays respectif[108] ». À la suite de cet accord, la Chine a arrêté plusieurs pirates informatiques identifiés par les États-Unis[109], démontrant sa détermination à mettre un terme aux pratiques des criminels du cyberespace, même s'il s'agit de ses propres citoyens. Alors que les opinions divergent sur les véritables motifs de Pékin, la mesure n'est pas sans précédent. Ainsi, en 2010, selon un témoignage d'un fonctionnaire de la NASA au Congrès, les autorités chinoises ont arrêté un ressortissant chinois pour le piratage informatique de sept systèmes de la NASA (National Aeronautics and Space Administration)[110].

Alors que Washington attend de voir si Pékin poursuivra réellement ces pirates informatiques, nous retiendrons la volonté de la Chine de démontrer ses dispositions à travailler avec les États-Unis — et peut-être aussi, par extension, avec d'autres gouvernements — sur des questions cybernétiques similaires, ce qui n'avait pas été fait auparavant. La possibilité de voir des sanctions imposées reste cependant d'actualité si les soupçons de piratage informatique commandité par Pékin contre les intérêts commerciaux des États-Unis se confirment. Dans le cas contraire, la Chine en ressortira gagnante, en voyant sa réputation réhabilitée. Conformément aux principes de la guerre juridique et médiatique énoncés *supra*, l'assurance donnée par la Chine de « s'opposer aux cyber-attaques et à l'espionnage et de lutter contre les formes de piratage par toute voie de droit[111] », associée à des exemples publics de collaboration avec les parties prenantes, peut progressivement apaiser les craintes des opposants quant à la menace que représente le pays et dépeindre la Chine comme un partenaire coopératif plutôt que comme un ennemi.

Ajoutons encore que l'instauration d'une coopération accrue en matière de cyber-sécurité avec les gouvernements régionaux renforcera le message de la Chine, qui souhaite un Internet stable, à l'abri des activités criminelles et terroristes. La Chine s'est montrée active en la matière, en s'engageant dans des discussions sur la cyber-sécurité avec le Japon[112], la Malaisie[113] et la Corée du Sud[114], ainsi que dans une série de pactes de non-agression cybernétique menant à l'accord du G20 de novembre 2015[115]. On peut s'attendre à ce que la Chine poursuive dans cette logique dans le cadre de réunions bilatérales indépendantes ou par l'intermédiaire d'organisations internationales comme l'Organisation de Shanghai pour la coopération.

Conclusion

Bien qu'accusée de mener des campagnes de cyber-espionnage de longue date et substantielles contre les États-Unis et plusieurs autres pays, la Chine a échappé à toute répercussion punitive ou économique importante. La stratégie des « Trois guerres » de la Chine, une logique de guerre de l'information en trois volets, conçue pour influencer la communauté internationale, a joué un rôle majeur dans la prévention de toute réaction dissuasive importante, tout en permettant à la Chine de se présenter comme un partenaire fiable dans le cyberespace. La Chine a cherché à influencer la perception du grand public quant à la menace croissante que le pays représente en niant les accusations, tout en tirant parti des fuites de Snowden sur les activités de surveillance américaines à l'échelle mondiale pour ternir l'image des États-Unis. Parallèlement, la Chine a eu recours à des mécanismes juridiques visant à se positionner en tant que partenaire de confiance en matière de cyber-sécurité. Le soutien témoigné envers le droit dont jouit chaque état de participer à la gouvernance de l'Internet a gagné suffisamment d'influence que pour encourager les États-Unis à renoncer à leur rôle de chef de file. Le fait de fournir aux Nations Unies un « code de bonne conduite » a aussi démontré la volonté de la Chine de faire valoir les intérêts de la communauté mondiale afin d'assurer la stabilité du cyberespace dans tous les états. La révision de sa législation sur la cybercriminalité témoigne de l'engagement de Pékin à sanctionner les pirates informatiques. Cette impression a été renforcée par l'arrestation, en 2015, de pirates présumés à la demande des États-Unis[116]. Enfin, le recours à des opérations psychologiques (PSYOPS) a permis à la Chine de se présenter comme une partie prenante respectueuse de la loi dans le cyberespace, tout en profitant discrètement des écrits l'identifiant comme une puissance cybernétique majeure. Plus les experts mettent le doigt sur la puissance des cyber-capacités chinoises, plus la Chine est perçue comme un pays influent, sans même que Pékin n'ait à intervenir.

La confluence de ces trois stratégies a ainsi empêché l'Occident, pendant une très longue période, de dissuader la Chine d'exercer ses activités de cyber-espionnage présumées. La Chine a clairement tiré parti de cette période de flottement prolongée. Au moment où les États-Unis ont envisagé la possibilité d'imposer des sanctions à la Chine, Pékin a profité de sa rencontre avec des pays comme le Japon et la Corée du Sud[117]. Elle a aussi exploité une série de « pactes de non-agression cybernétique » conclus entre la Chine et la Russie[118], le Royaume-Uni[119] et les États-Unis[120], dans un effort qui a abouti à l'accord historique de novembre 2015, par lequel les membres du G20 ont convenu de ne pas exercer d'activités d'espionnage électronique à des fins commerciales à l'encontre de leurs partenaires[121].

La Chine a accompli ce tour de force tout en devenant, dans le même temps, la plus grande économie du monde, et en se positionnant comme chef de file régional lors des efforts menés en faveur de la mise en place d'une Route de la soie maritime

(un réseau de ports, de projets et de zones économiques spéciales interconnecté en Asie du Sud-Est et dans le nord de l'océan Indien[122]) et de la fondation de la Banque asiatique d'investissement pour les infrastructures (qui compte déjà 20 gouvernements à son bord)[123]. Le dessein de la Chine est peut-être simplement de se hisser d'abord au sommet de sa région avant de monter sur le trône mondial. Dans ce contexte, le cyber-espionnage dont elle s'est rendue coupable peut être davantage considéré comme un moyen d'accroître son influence à l'échelle mondiale et moins comme une volonté de réduire celle des États-Unis.

Notes

1. ROGIN, Josh, « NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History' », *Foreign Policy: The Cable*, 9 juillet 2012, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatesttransfer-of-wealth-in-history/.

2. Office of the Director of National Intelligence, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace,* Washington DC: Office of the National Counterintelligence Executive, É.-U., octobre 2011, www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.

3. SPADE, Colonel Jayson M., *Information as Power: China's Cyber Power and America's National Security*, Carlisle, PA: U.S. Army War College, É.-U., mai 2012, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-072.pdf ; Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2014*, Washington, DC: Rapport annuel au Congrès, É.-U., 2014, www.defense.gov/pubs/2014_DoD_China_Report.pdf ; Department of Defense, *Quadrennial Defense Review 2014*, Washington, D.C.: OSD, É.-U., 2014: V, www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

4. NATHAN, Andrew J. et SCOBELL, Andrew, « How China Sees America », *Foreign Affairs,* septembre/octobre 2012, www.foreignaffairs.com/articles/138009/andrew-j-nathan-and-andrewscobell/how-china-sees-america.

5. Office of the Secretary of Defense, *Military and Security Developments*.

6. WALCOTT, John, « Chinese Espionage Campaign Targets U.S. Space Technology », *Bloomberg*, 18 avril 2012, www.bloomberg.com/news/2012-04-18/chinese-espionage-campaign-targets-u-s-space-technology.html.

7. SIMMONITE, Tom, « Chinese Hacking Team Caught Taking Over Decoy Water Plant », *Technology Review*, 2 août 2013, www.technologyreview.com/news/517786/chinese-hacking-team-caughttaking-over-decoy-water-plant/.

8. *Id*.

9. LIBERTO, Jennifer, « New Chinese Hacker Group Targets Governments, Nuclear Facilities », *CNN Money,* 4 juin 2013, http://money.cnn.com/2013/06/04/technology/security/cyber-hackergroup/index.html.

10. MAGNUSON, Stew, « Stopping the Chinese Hacking Onslaught », *NDIA*, juillet 2012, www.nationaldefensemagazine.org/archive/2012/July/Pages/StoppingtheChineseHackingOnslaught.aspx.

11. HALL, Susan D., « Chinese Hackers Targeting the Healthcare Industry », *FierceHealthIT*, 20 mars 2013, www.fiercehealthit.com/story/chinese-hackerstargeting-healthcare-industry/2013-03-20.

12. TAYLOR, Nick Paul, « Chinese Trial Data Hackers Reportedly Active Again », *Fierce BioTechIT,* 27 mai 2013, www.fiercebiotechit.com/story/chinesetrial-data-hackers-reportedly-active-again/2013-05-27.

13. HALL, Susan D., « *Chinese Hackers Targeting the Healthcare Industry* ».

14. « *China's 12th Five Year Plan: How it Actually Works and What's in Store for the Next Five Years* », APCO, 10 décembre 2010, www.export.gov.il/UploadFiles/03_2012/Chinas12thFive-Year Plan.pdf.

15. *Id*.

16. « *China's 12th Five-Year Plan: Overview* », Pékin, Chine, KPMG, mars 2011, www.kpmg.com/cn/en/IssuesAndInsights/ArticlesPublications/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf.

17. FERGUSON, Robyn E., « Information Warfare with Chinese Characteristics: China's Future View of Information Warfare and Strategic Culture », (mémoire de maîtrise, US Army Command and General Staff College, 2002, p. 15.

18. WINDREM, Robert, « Expert: U.S. In Cyber Arms Race With China, Russia », *NBC News Investigations*, 20 février 2013, http://investigations.nbcnews.com/_news/2013/02/20/17022378-expert-us-incyberwar-arms-race-with-china-russia.

19. MULVENON, James, « *The People's Liberation Army in the Information Age* », Santa Monica: RAND, 1999, p. 183.

20. THOMAS, Timothy L., « Google Confronts China's Three Warfares », *Parameters* 40, n° 2, été 2010, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2010summer/Thomas.pdf.

21. « Lawmaker: China Engaging in Cyber Spying », *Fox News*, 4 octobre 2011, www.foxbusiness.com/technology/2011/10/04/lawmaker-china-engaging-incyber-spying/.

22. « APT 1: Exposing one of China's Espionage Units », *Mandiant*, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

23. Remarques de Tom Donilon, 11 mars 2013, « The United States and the Asia-Pacific in 2013 », *The Asia Society*, https://obamawhitehouse.archives.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisor-president-united-states-an.

24. HOWARD, Steve, « Obama, China's Xi Discuss Cybersecurity Dispute on Phone Call », *Reuters*, 14 mars 2013, www.reuters.com/article/2013/03/14/ususa-china-obama-call-idUSBRE92D11G20130314.

25. JOHNSON, M. Alex et DELUCA, Matthew, « Obama Takes Diplomatic Tack on Chinese Cyberespionage Charges », *NBC News*, 7 juin 2013, http://usnews.nbcnews.com/_news/2013/06/07/18804533-obama-takes-diplomatictack-on-chinese-cyberespionage-charges.

26. BARRETT, Devlin, et GORMAN, Siobhan, « U.S. Charges Five in Chinese Military of Hacking », *The Wall Street Journal,* 19 mai 2014, www.wsj.com/articles/SB10001424052702304422704579571604060696532.

27. SEGAL, Adam, « Axiom and the Deepening Divide in U.S.-China Relations », *Council on Foreign Relations* (blogue), 29 octobre 2014, http://blogs.cfr.org/cyber/2014/10/29/axiom-and-the-deepening-divide-in-u-s-chinacyber-relations/.

28. « *China* », Cultural Savvy, www.culturalsavvy.com/china.htm.

29. TZU, Sun, *The Art of War,* www.theartofwar.ws/The_Art_of_War.pdf.

30. Office of the Secretary of Defense, *Military and Security Developments*, p. 26.

31. THOMAS, « *Google Confronts China's Three Warfares* ».

32. Office of the Secretary of Defense, *Military and Security Developments*, p. 26.
33. *Id*.
34. *Id*.
35. CHENG, Dean, *Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response*, The Heritage Foundation report n° 2745, Washington, DC, É.-U., The Heritage Foundation, É.-U., 26 novembre 2012, www.heritage.org/asia/report/winning-without-fighting-chinese-public-opinion-warfare-and-the-need-robust-american.
36. *Id*.
37. *Id*.
38. *Id*.
39. THORNBURG, Nathan, « The Invasion of the Chinese Cyberspies », *Time*, 29 août 2005, http://content.time.com/time/magazine/article/0,9171,1098961-1,00.html.
40. KOUTSOUKIS, Jason, « Chinese Waging Online Spy War », *The Age*, 10 février 2008, www.theage.com.au/news/national/chinese-waging-online-spywar/2008/02/09/1202234232007.html ; BOYES, Roger, « China Accused of Hacking into Heart of Merkel Administration », *The Times*, 27 août 2007, www.thetimes.co.uk/tto/news/world/europe/article2595759.ece ; BUENAVENTURA, Donna, « China Tried to Hack Our Computers, Says India Security Chief M.K. Narayanan », *Donna's Security Flash* (blogue), 18 janvier 2010, https://blogs.msmvps.com/donna/2010/01/18/china-tried-to-hack-our-computers-says-india-s-security-chief-m-k-narayanan/.
41. INGRAHAM, Nathan, « US Government Claims Huawei and ZTE Pose a Risk to National Security: the Accusations, Responses, and Fallout », *The Verge,* 11 octobre 2012, www.theverge.com/2012/10/11/3488584/huawei-zte-us-governmentsecurity-investigation.
42. « Admit Nothing and Deny Everything », *The Economist*, 6 juin 2013, www.economist.com/news/china/21579044-barack-obama-says-he-ready-talkxi-jinping-about-chinese-cyber-attacks-makes-one.
43. McREYNOLDS, Joe, « Cyber Transparency for Thee, But Not for Me », *The Jamestown Foundation China Brief*, 14, n° 8, www.jamestown.org/single/?tx_ttnews[tt_news]=42246&no_cache=1#.VTfXNBdSxdY.
44. RILEY, Charles, « China's Military Denies Hacking Allegations », *CNNMoney,* 20 février 2013, http://money.cnn.com/2013/02/20/technology/china-cyberhacking-denial/.
45. BARBOZA, David, « China Says Army Is Not Behind Attacks in Report », *The New York Times*, 21 février 2013, www.nytimes.com/2013/02/21/business/global/china-says-army-not-behindattacks-in-report.html?_r=0.
46. « Espionage Report: Merkel's China Visit Marred by Hacking Allegations », *Spiegel Online*, 27 août 2007, www.spiegel.de/international/world/espionage-report-merkel-s-china-visitmarred-by-hacking-allegations-a-502169.html.
47. « M Trends 2014: Beyond the Breach », *Mandiant*, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.
48. PEEK, Liz, « U.S. and China in a Lethal Game of Cyber Chess », *The Fiscal Times*, 9 avril 2014, www.thefiscaltimes.com/Blogs/Peek-POV/2014/04/09/USand-China-Lethal-Game-Cyber-Chess.
49. House, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei Technologies and ZTE*, 112th Congress, 8 octobre 2012, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf.

50. « Huawei: Leaked Report Shows No Evidence of Spying », *BBC News*, 18 octobre 2012, www.bbc.com/news/technology-19988919.

51. BLANCHARD, Ben, HUI, Li, et CARSTEN, Paul, « China Blames U.S. for Rise in Hacking Attacks », *The Fiscal Times*, 28 mars 2014, www.thefiscaltimes.com/Articles/2014/03/28/China-Blames-US-Rise-Hacking-Attacks.

52. WILDER, Charly, « Out of Hand: Europe Furious over U.S. Spying Scandal », *Spiegel Online*, 24 octobre 2013, www.spiegel.de/international/world/angry-european-and-german-reactionsto-merkel-us-phone-spying-scandal-a-929725.html.

53. WATTS, Jonathan, « NSA Accused of Spying on Brazilian Oil Company Petrobas », *The Guardian*, 9 septembre 2013, www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras.

54. MOYER, Edward, « NSA Spied on EU Antitrust Official Who Sparred With U.S. Tech Giants », *Cnet*, 20 décembre 2013, www.cnet.com/news/nsa-spiedon-eu-antitrust-official-who-sparred-with-us-tech-giants/.

55. HOSENBALL, Mark, « Obama Halted NSA Spying on IMF and World Bank Headquarters », *Reuters*, 31 octobre 2013, www.reuters.com/article/us-usasecurity-imf-idUSBRE99U1EQ20131031.

56. SAVAGE, Charlie, « Watchdog Report Says NSA Is Illegal and Should End », *The New York Times*, 23 janvier 2014, www.nytimes.com/2014/01/23/us/politics/watchdog-report-says-nsa-program-is-illegal-and-should-end.html?partner=rss&emc=rss&smid=twnytimes&_r=1.

57. « U.S., China Agree to Work Together on Cyber Issues », *Reuters*, 13 avril 2013, www.reuters.com/article/2013/04/13/us-china-us-cyberidUSBRE93C05T20130413.

58. PEEK, « *U.S. and China in a Lethal Game of Cyber Chess* ».

59. Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage*, Washington, DC, U.S. Department of Justice, É.-U., 19 mai 2014, www.justice.gov/opa/pr/us-charges-fivechinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

60. CHENG, *Winning Without Fighting*.

61. KEXIN, L., *Study Volume on Legal Warfare,* Washington, DC, É.-U., National Defense University Press, 2006, p. 18, 34-37.

62. ORTS, Eric W., « The Rule of Law in China », *Vanderbilt Journal of Transnational Law*, 1 janvier 2001, www.highbeam.com/doc/1G1-72733959.html.

63. CHENG, *Winning Without Fighting*.

64. *Id*.

65. THOMSON, Amy, « UN Telecom Treaty Approved Amid U.S. Web-Censorship Concerns », *Bloomberg*, 14 décembre 2012, www.bloomberg.com/news/articles/2012-12-13/u-s-and-u-k-refuse-to-sign-unagreement-on-telecommunications.

66. « U.S. and UK Refuse to Sign UN's Communications Treaty », *BBC News,* 14 décembre 2012, www.bbc.co.uk/news/technology-20717774.

67. Ibid.

68. TIMBERG, Craig, « U.S. to Relinquish Last Control Over the Internet », *The New York Times*, 14 mars 2014, www.washingtonpost.com/business/technology/us-to-relinquish-remaining-control-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.html.

69. RRN Prasad, « Towards Freedom of the Internet », *The Financial Express*, 4 janvier 2016, www.financialexpress.com/article/fe-columnist/towardsfreedom-of-the-internet/187447/.

70. Assemblée générale des Nations Unies, A/66/359, « Courrier daté au 12 septembre 2011 et adressé au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie, du Tadjikistan et de l'Ouzbékistan auprès de l'Organisation des Nations Unies », 12 septembre 2011, https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

71. Assemblée générale des Nations Unies, A/69/723, « Courrier daté au 9 janvier 2015 et adressé au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie, du Tadjikistan et de l'Ouzbékistan auprès de l'Organisation des Nations Unies », 9 janvier 2015, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

72. « China Says Cyber Hacking is Against the Law », *Voice of America*, 13 janvier 2010, www.voanews.com/content/china-says-cyber-hacking-is-againstlaw-81473967/111452.html.

73. JIAN, Gu, « Strengthening international cooperation and joining hands in fighting against transnational cybercrime », *China.org*, 9 novembre 2010, www.china.org.cn/business/2010internetforum/2010-11/09/content_21306503.htm.

74. FINKLE, Jim, MENN, Joseph, et VISWANATHA, Aruna, « US Accuses China of Cyber Spying on American Companies », *Reuters*, 20 novembre 2014, www.reuters.com/article/2014/11/20/us-cybercrime-usa-chinaidUSKCN0J42M520141120.

75. STOKES, Mark, *The Chinese Joint Aerospace Campaign: Strategy, Doctrine, and Force Modernization in China's Revolution in Doctrinal Affairs*, éd. MULVENON, James et FINKLESTEIN, David, Alexandria, VA, É.-U. : CNA Corporation, 2005, p. 272.

76. CHENG, *Winning Without Fighting*.

77. FERGUSON, « *Information Warfare with Chinese Characteristics* », p. 31.

78. MULVENON, James, « The PLA and Information Warfare », in *The People's Liberation Army in the Information Age*, éd. MULVENON, James et YANG, Richard H., Washington, DC, É.-U. : RAND, 1999, 180.

79. CHENG, *Winning Without Fighting*.

80. YANHUA, Guo, *Psychological Warfare Knowledge*, Washington, DC, É.-U. : National Defense University Press, 2005, pp. 14-16.

81. « Remarques du Président Obama et du Président Xi Jinping de la République populaire de Chine après une rencontre bilatérale », *The White House*, 8 juin 2013, www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obamaand-president-xi-jinping-peoples-republic-china-.

82. « China Says Cyber Hacking is Against the Law », *Voice of America*.

83. Assemblée générale des Nations Unies, A/66/359, « Courrier daté au 12 septembre 2011 ».

84. Assemblée générale des Nations Unies, A/69/723, « Courrier daté au 9 janvier 2015 ».

85. AUSTIN, Greg, « China's Cyber Turn: Recognizing Change for the Better », *The Diplomat*, 21 décembre 2015, http://thediplomat.com/2015/12/chinas-cyber-turnrecognizing-change-for-the-better/.

86. ORLIK, Tom, « Charting China's Economy: 10 Years Under Hu », *The Wall Street Journal* (blogue), 16 novembre 2012, http://blogs.wsj.com/chinarealtime/2012/11/16/charting-chinas-economy-10-yearsunder-hu-jintao/tab/print/.

87. « More than Minerals », *The Economist*, 23 mai 2013, www.economist.com/news/middle-east-and-africa/21574012-chinese-trade-africa-keeps-growing-fears-neocolonialism-are-overdone-more ; « China Overtakes U.S. as Brazil's Top Trade Partner », *Latin American Times*, 17 octobre 2013, www.laht.com/article.asp?ArticleId=333733&CategoryId=10718.

88. WENJUAN, Du, « China Investment in Brazil More Diversified », *China Daily*, 14 mai 2013, http://usa.chinadaily.com.cn/business/2013-05/14/content_16498645.htm.

89. « China's Mighty Telecom Footprint in Africa », *New Security Learning,* 14 février 2011, www.newsecuritylearning.com/index.php/archive/75-chinasmighty-telecom-footprint-in-africa.

90. IASIELLO, Emilio, « Stuffing the Genie Back into the Bottle: Can Threats to the IT Supply Chain Be Mitigated? », *Foreign Policy Journal*, 3 avril 2013, www.foreignpolicyjournal.com/2013/04/03/stuffing-the-genie-back-in-thebottle-can-threats-to-the-it-supply-chain-be-mitigated/.

91. CLARK, Liat, « Huawei Not a Threat to UK. Says Huawei Oversight Board », *Wired*, 27 mars 2015, www.wired.co.uk/news/archive/2015-03/27/huawei-nota-threat-to-national-security.

92. OSMAN, Hafizah, « Huawei Supports Australian Cyber Security Centre Development », *Arnnet.com*, 23 janvier 2013, www.arnnet.com.au/article/451519/huawei_supports_australian_cyber_security_centre_development_/.

93. ROGIN, « NSA Chief: Cybercrime ».

94. GREEN, Marcel A., « China's Growing Cyberwar Capabilities », *The Diplomat*, 13 avril 2015, http://thediplomat.com/2015/04/chinas-growing-cyberwarcapabilities/.

95. Témoignage de Richard Bejtlich devant la Commission d'examen de l'économie et de la sécurité de la Chine, lors d'une audience sur 'L'évolution des capacités cybernétiques et nucléaires de la Chine' », 26 mars 2012, U.S.-China Economic and Security Review Commission, www.uscc.gov/sites/default/files/3.26.12bejtlich.pdf.

96. FISHER, Jonathan, « China Has Hacked Every Major U.S. Company, Claims Richard Clarke », *Web Pro News*, 28 mars 2012, www.webpronews.com/china-has-hacked-every-u-s-major-company-claimsrichard-clarke-2012-03.

97. THOMAS, Timothy L., « New Developments in Chinese Strategic Psychological Warfare », *Special Warfare* 1, n° 9, 2003, www.dtic.mil/cgibin/GetTRDoc?AD=ADA434978.

98. THORNBURGH, Nathan, « Inside the Chinese Hack Attack », *Time*, 25 août 2005, http://content.time.com/time/nation/article/0,8599,1098371,00.html.

99. KOPAN, Tal, « White House Readies Cyber Sanctions Against China Ahead of State Visit », *CNN*, 24 septembre 2015, www.cnn.com/2015/08/31/politics/china-sanctions-cybersecurity-presidentobama/.

100. Department of Defense, *Strategy for Operating in Cyberspace,* Washington, DC, É.-U., U.S. Department of Defense, juillet 2011, www.defense.gov/news/d20110714cyber.pdf

101. KEROMYTIS, Angelos, « *Active Cyber Defense* », Program Information, Defense Advanced Research Projects Agency (DARPA), consulté le 28 septembre 2017, www.darpa.mil/program/active-cyber-defense.

102. REED, John, « Mike Rogers: Cool It with Offensive Cyber Ops », *ForeignPolicy.com*, 14 décembre 2012, http://foreignpolicy.com/2012/12/14/mike-rogerscool-it-with-offensive-cyber-ops/.

103. Government Accountability Office, *National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, Washington, DC, É.-U., Government Accountability Office, février 2013, www.gao.gov/assets/660/652170.pdf.

104. Government Accountability Office, *A Better Defined and Implemented National Strategy is Needed to Address Persistent Challenges*, Washington, DC, É.-U., Government Accountability Office, mars 7, 2013, www.gao.gov/assets/660/652817.pdf.

105. CHENG, *Winning Without Fighting*.

106. « China Accuses U.S. of Hypocrisy Over Internet Spying », *Sydney Morning Herald*, 28 juin 2013, www.smh.com.au/world/china-accuses-us-ofhypocrisy-over-internet-spying-20130628-2p0uk.html.

107. MESSMER, Ellen, « Don't Trust the NSA? China-based Huawei Says, 'Trust Us' », *Network World*, 18 octobre 2013, www.networkworld.com/news/2013/101813-nsa-huawei-274959.html?page=1.

108. « FACT SHEET: President Xi Jinping's State Visit to the United States », *The White House*, 25 septembre 2015, www.whitehouse.gov/the-pressoffice/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

109. « Chinese Hackers Arrested After U.S. Request », *BBC News*, 12 octobre 2015, accessible à l'adresse : www.bbc.com/news/technology-34504317.

110. House. *Déclaration de Paul K. Martin (Inspecteurr général, NASA) : NASA Cybersecurity: An Examination of the Agency's Information Security*, Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, 29 février 2012, https://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf.

111. Ministry of Foreign Affairs, *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on October 13, 2014*, Washington, DC, É.-U., Ministry of Foreign Affairs, 13 octobre 2015, www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1165638.shtml.

112. « S. Korea, Japan, China to Hold Cyber Policy Talks », *Yonhap News Agency*, 13 octobre 2015, http://english.yonhapnews.co.kr/news/2015/10/13/0200000000AEN20151013004800315.html.

113. « Malaysia, China to Work Together on Cyber Crimes », *The Malay Mail Online*, 22 août 2014, www.themalaymailonline.com/malaysia/article/malaysia-china-to-worktogether-to-combat-cyber-crimes.

114. « S. Korea, Japan, China to Hold Cyber Policy Talks », *Yonhap News Agency*.

115. NAKASHIMA, Ellen, « World's Richest Nations Agree Hacking for Commercial Benefits Is Off-Limits », *The Washington Post*, 16 novembre 2015, www.washingtonpost.com/world/national-security/worlds-richest-nationsagree-hacking-for-commercial-benefit-is-off-limits/2015/11/16/40bd0800-8ca9-11e5-acff-673ae92ddd2b_story.html.

116. NAKASHIMA, Ellen, « Chinese Government Has Arrested the Hackers Breached OPM Database », *The Washington Post*, 2 décembre 2015, www.washingtonpost.com/world/national-security/chinese-government-hasarrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

117. « S. Korea, Japan, China to Hold Cyber Policy Talks », *Yonhap News Agency*.

118. RAZUMOVSKAYA, Olga, Russia and China Pledge Not to Hack Each Other, *The Wall Street Journal* (blogue), 8 mai 2015, http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/.

119. WILLIAMS, Bo, Katie, « UK, China Mirror U.S. Anti-Hacking Pact », *The Hill*, 21 octobre 2015, http://thehill.com/policy/cybersecurity/257602-uk-china-mirror-usanti-hacking-pact.

120. « FACT SHEET: President Xi Jinping's State Visit », *The White House*.

121. NAKASHIMA, « *World's Richest Nations Agree* ».

122. BREWSTER, David, « The Bay of Bengal:« The Maritime Silk Route and China's Naval Ambitions », *The Diplomat*, 14 décembre 2014, http://thediplomat.com/2014/12/the-bay-of-bengal-the-maritime-silk-route-andchinas-naval-ambitions/.

123. PONGSUDHIRAK, Thitinan, « China's Aspiring Global Leadership », *East Asia Forum,* 25 novembre 2014, www.eastasiaforum.org/2014/11/25/chinasaspiring-global-leadership/.