La cyber-dissuasion est-elle une stratégie illusoire ?

Emilio Iasiello*

Depuis la reconnaissance, par le gouvernement américain (G-US) d'une part, de la gravité des menaces cybernétiques, en particulier contre ses infrastructures critiques, et par le ministère de la Défense (DOD) d'autre part, qui a officiellement qualifié le cyberespace de zone de combat, les experts en sécurité, les décideurs politiques et les chercheurs de divers groupes de réflexion ont ressuscité une stratégie de la Guerre froide pour lutter contre les nouvelles menaces qui germent sur le cyberespace[1]. Les mêmes principes qui ont contribué à la dissuasion nucléaire soviétique pourraient ainsi potentiellement s'appliquer au cyberespace et aux ennemis qui y opèrent. Même si la théorie est convaincante, nous devons garder à l'esprit que ces stratégies, bien que similaires, ne sont pas transférables : les facteurs clés qui ont permis la dissuasion nucléaire n'ont pas la même valeur dans le cyberespace. Alors que seule une poignée d'états ont démontré leur capacité à mettre au point des armes nucléaires, plus de 140 pays ont mis, ou sont en train de mettre au point, des armes cybernétiques. Selon certaines estimations, plus de 30 pays auraient créé des cyber-unités militaires ou seraient en passe de le faire. Ajoutons encore que ce contingent d'ennemis ne se compose pas uniquement d'états-nations, mais qu'il comprend notamment des cybercriminels, des pirates informatiques et des hacktivistes, aux multiples niveaux de sophistication, et des ressources prêtes à mettre leurs capacités aux services d'intentions malveillantes[2].

D'aucuns défendent la mise en œuvre d'une stratégie de cyber-dissuasion pour atténuer le volume d'activités cybernétiques hostiles aux intérêts des secteurs public et privé. Mais un trop grand nombre de facteurs, y compris les défis liés à l'attribution et l'ampleur du combat à mener face à un spectre de menaces d'une telle envergure, ne permettent pas aux stratégies de dissuasion cybernétique d'atteindre le résultat escompté à court terme.

---

*Emilio Iasiello travaille comme responsable de l'unité d'analyse de la menace au sein d'un cabinet de cyber-renseignement international qui aide les entités fédérales et les entreprises à gérer les risques cybernétiques auxquels elles font face, à mieux comprendre les vulnérabilités de leur environnement et à prioriser leurs investissements face aux menaces qui pèsent sur leurs activités ou leur mission. Emilio Iasiello a écrit plusieurs articles portant sur l'élaboration d'une nouvelle méthodologie d'analyse de la cyber-menace et sur la cyber-menace dans le domaine de l'aéronautique. Il a également proposé des solutions visant à améliorer l'efficacité des efforts entrepris par les États-Unis en matière de cybersécurité nationale et de sécurisation de la chaîne d'approvisionnement informatique.

IASIELLO, Emilio, « Is Cyber Deterrence an Illusory Course of Action? », *Journal of Strategic Security* 7, no. 1, 2013, pp. 54-67. DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5. Disponible à l'adresse : http://scholarcommons.usf.edu/jss/vol7/iss1/6.

Qui plus est, d'autres stratégies de dissuasion, telles que celles utilisées contre l'utilisation d'armes nucléaires, le terrorisme et les comportements des états voyous, ne sont pas des modèles appropriés pour le cyberespace. Malgré quelques points communs, le domaine du cyberespace manque en effet de transparence et de traçabilité des acteurs pour développer des mesures de dissuasion. En dépit de ces obstacles, les états-nations devraient s'efforcer d'élaborer, de perfectionner et de mettre en œuvre des stratégies nationales de cybersécurité qui mettent l'accent sur l'amélioration de la cyberdéfense et impliquent un principe de responsabilisation. Si les acteurs les plus sophistiqués resteront capables d'exploiter les failles des systèmes de défense les plus robustes, le succès des intrusions sur les réseaux nationaux résulte en grande partie de mauvaises pratiques de cybersécurité, telles que la mise en place de systèmes défaillants et un manque de formation des utilisateurs aux principes de sécurité de l'information. La cyber-sécurité implique un effort continu et un suivi permanent. Elle doit aussi être adaptée à un environnement de menace en constante évolution.

Qu'est-ce que la cyber-dissuasion ?

Avant d'aborder la conception et l'élaboration d'une stratégie nationale de cyber-dissuasion, il est important de comprendre les concepts fondamentaux de la dissuasion et ce qu'ils impliquent sur la mise en place d'une possible stratégie. Une stratégie de dissuasion cherche, par définition, à inciter un ennemi potentiel à ne pas attaquer une cible en lui faisant croire que les coûts et les conséquences qui résulteront de l'attaque seront supérieurs aux avantages potentiels qu'il pourra en retirer. Nous pourrions ainsi définir le concept de la cyber-dissuasion, avec surtout ses répercussions et ses effets escomptés, comme suit :

> La cyber-dissuasion est une stratégie par laquelle un état, désireux de défendre son intégrité, affiche son intention de convaincre tout adversaire de renoncer à une activité cybernétique destructrice en ciblant et en influençant son appareil décisionnel dans le but de susciter dans son chef la crainte de représailles dont l'ampleur dépasserait celle de l'attaque initiale.

Cette définition fondamentale posée, il est tout aussi essentiel d'identifier les types de dissuasion possibles en analysant le cours de l'histoire. Bien qu'il y ait une myriade d'itérations et de sous-ensembles, on peut distinguer deux types de stratégies de dissuasion utilisées par les États-Unis : la dissuasion par punition et la dissuasion par déni.

- **La dissuasion par punition** ou crainte du châtiment laisse entendre à l'agresseur que toute attaque sera suivie de représailles d'envergure[3]. Dans ce scénario, les représailles ne doivent pas se limiter à des actions spécifiques et peuvent aussi intégrer d'autres moyens, tels que les frappes cinétiques ou des moyens plus diplomatiques tels que les sanctions économiques[4]. Parmi les exemples de dissuasion par punition, citons la doctrine de destruction mutuelle pendant la guerre froide, qui

impliquait que la menace d'un recours à l'arme nucléaire dissuadait tout adversaire d'y recourir lui aussi.

Appliquant le même principe au cyberespace, la dissuasion par punition peut prendre la forme d'actions numériques telles qu'une frappe cybernétique de représailles contre les auteurs d'une cyberattaque, ou une frappe préventive contre les auteurs potentiels d'une attaque réseau. Cette forme de dissuasion pourrait toutefois également entraîner des attaques cinétiques, des négociations diplomatiques ou des sanctions économiques. Ainsi, ceux qui pensent que les États-Unis sont à l'origine de l'attaque STUXNET (qui visait les centrifugeuses nucléaires iraniennes) pourraient la voir une dissuasion préventive à l'encontre de l'Iran, qui a continué à affiner ses procédures d'enrichissement de l'uranium.

- **La dissuasion par le déni** est moins motivée par le conflit et cherche plutôt à convaincre les agresseurs potentiels que leurs efforts ne seront pas couronnés de succès et que les avantages qu'ils recherchent leur seront refusés[5]. L'avantage de cette stratégie est qu'elle peut être basée sur des mesures défensives et donc non seulement être un moyen d'empêcher l'ennemi d'agir, mais aussi une solution au cas où il passerait tout de même à l'action[6]. Le blocus naval américain autour de Cuba en 1962 constitue un exemple de ce type de dissuasion. Dans ce cas précis, les États-Unis ont choisi de refuser aux navires russes l'entrée dans les eaux cubaines plutôt que de déployer des frappes aériennes contre des sites de missiles cubains.

  Dans le cyberespace, la dissuasion par le déni assume un rôle défensif plus traditionnel en décourageant ou en faisant échouer les attaques au moyen de défenses robustes, proactives et coûteuses. Elle exige un engagement important et ciblé de la part du gouvernement pour sécuriser les systèmes et les réseaux dont il a le contrôle, avec la pleine coopération des propriétaires privés de l'infrastructure[7]. Cette forme de dissuasion implique un coût considérablement plus élevé compte tenu de l'ampleur de l'entreprise, en ce compris l'utilisation de pratiques de sécurité avancées et l'adoption de composants matériels et logiciels fiables[8].

Les facteurs nécessaires à une dissuasion cybernétique efficace

La cyber-dissuasion est difficile à mettre en œuvre, car il faut tenir compte de plusieurs facteurs pour atteindre les résultats de l'un ou l'autre sous-ensemble de la stratégie de dissuasion. Une stratégie de cyber-dissuasion doit déterminer au préalable les paramètres sur lesquels elle se fonde. À défaut, l'ennemi ne pourra pas comprendre et traiter l'intention du défenseur, qui risque donc d'être mal comprise ou mal interprétée, augmentant ainsi le risque d'escalade et probablement aussi, celui de la confrontation entre états.

La communication

Toute stratégie de dissuasion implique, en partie, une capacité de communication efficace avec la communauté internationale, et les adversaires en particulier, sur ce qui est acceptable et sur les lignes rouges à ne pas dépasser. Dans *Arms and Influence*, Thomas Schelling note que le succès de la dissuasion par punition ou déni dépend de l'efficacité de la communication entre un état et l'entité qu'il souhaite dissuader[9]. Parallèlement à la communication, la notion de crédibilité est également primordiale. Un état-nation ne peut en effet se contenter de décréter qu'une activité a franchi la ligne rouge, il doit être prêt à agir en conséquence. À défaut, un état-nation risque de perdre sa crédibilité internationale. En 2012, par exemple, le président Barack Obama a proclamé que l'utilisation d'armes chimiques par le gouvernement syrien contre ses citoyens était la ligne rouge à ne pas franchir[10]. Pourtant, lorsque les services de renseignements ont confirmé que des armes chimiques avaient été utilisées six mois plus tard, Obama n'avait toujours pas donné suite à sa déclaration[11]. En manquant à sa parole, Barack Obama a causé du tort à la crédibilité des États-Unis. Il avait certes accepté ensuite, en juillet 2013, de fournir des armes aux rebelles syriens, mais de nombreux membres de la communauté internationale ont estimé cette réaction « trop faible et tardive[12] ».

Au sein du cyberespace, la communication relève d'une importance capitale en raison du caractère ambigu de ce domaine. Une communication efficace nécessiterait un consensus sur les normes de comportement à adopter dans le cyberespace, une entreprise difficile à réaliser, comme en témoigne l'incapacité des États-Unis et de la Chine à définir un langage commun dans le cadre du Dialogue stratégique et économique de juillet 2013[13]. Les États-Unis orientent leur propos sur les technologies et les réseaux de machines automatisées et préfèrent utiliser le terme « cyber-sécurité », tandis que des pays comme la Chine et la Russie préfèrent utiliser le terme plus large « sécurité de l'information » pour inclure les informations résidant sur les réseaux ou transitant par ces derniers, ainsi que pour désigner les technologies elles-mêmes[14]. La raison de cette divergence réside dans les activités qui se déroulent dans le cyberespace ; la Chine favorise une interprétation plus large pour pouvoir dicter et contrôler le contenu et l'information auxquels ses citoyens ont accès, alors que les États-Unis soutiennent les libertés sur Internet. Depuis la deuxième réunion du Groupe de travail sur la cyber-sécurité Chine–États-Unis en décembre 2013, les deux pays sont dans l'impasse et ne parvienne pas à trouver un terrain d'entente sur le contenu de la définition. En l'absence d'un lexique commun et concerté et de consensus sur la manière dont Internet devrait être utilisé, la communication entre les deux parties est vouée à l'échec. De même, lorsqu'il s'agit de faire face à des activités hostiles dans le cyberespace où les acteurs sont étrangers les uns aux autres, cette communication défaillante favorise l'incapacité à envoyer des messages clairs et à désamorcer les tensions. La Convention sur la cybercriminalité, dirigée par le Conseil de l'Europe en 2001, fournit un cadre propice à l'adoption d'une terminologie commune. La convention identifie la terminologie convenue par tous les signataires. À ce jour, on dénombre 41 ratifications ou adhésions. Notons que la Russie, qui figure néanmoins sur la liste des états

non-membres, n'a donc pas ratifié la charte, pas plus que la Chine, ce qui indique la réticence de ce pays à accepter la terminologie acceptée par les états occidentaux[15].

Le jeu de signal

La logique du jeu de signal de l'équilibre bayésien parfait a été appliquée à de nombreux domaines de la politique internationale au cours de la dernière décennie, y compris lors des décisions d'entrer en guerre, des négociations de crise, des négociations économiques internationales, de l'intégration régionale et des politiques étrangères des états démocratiques[16]. Que ce soit en temps de paix ou en temps de guerre, l'un des éléments clés de toute stratégie de cyber-dissuasion est la capacité de signaler correctement ses intentions au destinataire. Sans cette capacité de « signalement », la dissuasion cybernétique par punition devient inefficace et risque d'être mal comprise ou mal interprétée, ce qui augmente le risque d'escalade et de conflit. Ainsi, avant l'exécution de la dissuasion par punition, l'état qui se défend doit clairement signaler son mécontentement à l'agresseur (que ce soit un état-nation ou un acteur non étatique) de manière à ce que ce dernier l'interprète correctement, le comprenne et en conclue que les coûts potentiels d'une telle action l'emportent largement sur ses avantages potentiels. Il convient cependant de noter que l'état-nation signalant doit disposer, pour que le signalement soit efficace, des capacités et de la crédibilité nécessaires lui permettant d'exercer des représailles cybernétiques destructrices. Si l'adversaire ne croit pas en la crédibilité d'un état signalant, ou s'il ne s'en soucie pas outre mesure, le signalement n'a plus de valeur. Dans ce cas, l'agresseur ne sera pas dissuadé par la menace de punition.

À l'instar de la communication, le signalement dans le cyberespace peut être facilement mal interprété, ignoré ou même ignoré par l'agresseur. Il peut se faire ouvertement, secrètement ou par voie diplomatique, économique ou militaire. Prenons l'exemple de STUXNET. Si le gouvernement des États-Unis avait été responsable du déploiement de STUXNET dans les systèmes informatiques des centrifugeuses iraniennes, le gouvernement des États-Unis aurait été susceptible de signaler par la voie diplomatique au gouvernement iranien qu'une telle action—sans révéler la cible visée—se produirait si l'Iran ne mettait pas fin à son processus d'enrichissement. Lorsque les centrifugeuses ont été détruites et remplacées, le monde aurait compris que les États-Unis étaient derrière l'événement. Un autre exemple de signalement potentiel dans le cyberespace serait l'utilisation d'attaques de déni de service distribué (DDoS). Sur la base du même scénario, les banques américaines ont été la cible d'attaques DDoS peu après la découverte de STUXNET. De nombreux législateurs américains ont immédiatement soupçonné le gouvernement iranien d'avoir mené ou orchestré les attaques par proxys[17]. Si l'Iran avait été responsable, le fait d'avoir signalé au préalable par la voie diplomatique, ou par des voies tierces, sans révéler de cibles précises aurait clairement indiqué au gouvernement américain que l'Iran non seulement répondait à l'attaque STUXNET, mais que le pays disposait également de la capacité cybernétique.

L'attribution

Il est extrêmement difficile de déterminer l'attribution dans le cyberespace, où les opérateurs avisés disposent d'une multitude de techniques de brouillage pour empêcher les défenseurs d'identifier correctement leur véritable point d'origine. Qu'il s'agisse de compromettre une série d'ordinateurs dans différents pays avant exécution ou d'utiliser des anonymiseurs et des proxys, le cyberespace est un environnement propice aux attaques malveillantes. L'attribution est un élément nécessaire de toute stratégie de dissuasion, car il incombe à l'état qui se défend d'identifier l'attribution d'un agresseur avant le début de toute mesure de représailles. Il n'est toutefois pas nécessaire de procéder à une attribution complète pour exercer un effet dissuasif par déni lorsque d'autres formes d'actions non destructives peuvent être dirigées contre un agresseur. Jason Healey, du Conseil atlantique, propose un moyen efficace pour déterminer le « spectre de la responsabilité de l'état » ; un outil conçu pour aider les analystes ayant des connaissances imparfaites à attribuer la responsabilité d'une attaque particulière ou d'une campagne d'attaques avec plus de précision et de transparence[18]. Le spectre attribue dix catégories, chacune d'entre elles étant caractérisée par un degré de responsabilité différent, selon qu'une nation ignore, soutienne ou mène une attaque[19]. Le niveau de culpabilité attribué à l'état-nation servirait de guide pour le type et le niveau de réponse approprié, allant de l'ignorance de l'attaque initiale à la riposte de l'agresseur identifié.

Les pratiques d'attribution réussies dans le cyberespace devraient idéalement combiner l'analyse technique, cognitive et comportementale pour mieux identifier les agresseurs, ainsi que les influences qui peuvent les aider à guider leurs opérations. L'analyse technique n'est pas suffisante aux fins d'attribution, étant donné que de nombreux acteurs hostiles mettent en œuvre les mêmes tactiques, techniques, procédures et outils, ou se livrent à des opérations de « faux signalement » dans le cadre d'activités malveillantes[20]. Aucune norme ne permet actuellement d'établir un degré de confiance dans la détermination de l'attribution cybernétique[21]. Lorsqu'il s'agit de déployer éventuellement une cyber-dissuasion par punition, le défenseur doit être en mesure d'identifier l'auteur de la cyber-dissuasion afin de prendre les mesures qui s'imposent. Plusieurs problèmes empêchent les processus d'attribution rapides et précis, notamment : la mauvaise attribution, le temps nécessaire à la collecte et à l'analyse de la méthode d'attaque employée et l'identification du mobile, du comportement et des influences extérieures de l'acteur. Néanmoins, afin d'éviter de perdre la face en public et de réduire le volume et la probabilité des dommages collatéraux, un niveau acceptable d'attribution doit être établi avant le début de toute mesure de représailles.

La proportionnalité

Sur la base des Conventions de Genève de 1949 sur le droit des conflits armés et des principes de proportionnalité, ainsi que de ceux exprimés par l'OTAN dans le Manuel de Tallinn prônant l'assimilation de la cyberguerre à la guerre conventionnelle, une cyber-action de représailles doit être proportionnelle, en particulier si elle est dirigée contre un

état suspect ou un acteur parrainé par l'état. En d'autres termes, « la cyber-action de représailles doit être de valeur comparable à l'attaque initiale et ne pas s'assimiler à une escalade[22] ». La crédibilité d'un état-nation est donc liée à la proportionnalité, en ce sens que l'état-nation doit non seulement riposter contre l'agresseur, mais qu'il doit le faire d'une manière telle qu'il fasse valoir son point de vue, il doit riposter de façon énergique, mais pas au point de solliciter une réaction négative au sein la communauté mondiale. La crédibilité d'un état-nation sur la scène mondiale réside dans sa capacité à tenir parole et à faire preuve de suffisamment de tact pour ne pas être perçu comme un état autoritaire. Il doit également tenir compte des conséquences involontaires résultant de représailles cybernétiques. Prenons à nouveau l'exemple du ver STUXNET utilisé contre les centrifugeuses nucléaires iraniennes. Le malware a été écrit pour cibler des exigences de configuration spécifiques, dans ce cas, le logiciel Siemens des centrifugeuses.

Cependant, bien qu'il ait été subrepticement inséré et déployé sur un réseau non connecté à Internet, le virus s'est échappé, infectant des ordinateurs en Azerbaïdjan, en Indonésie, en Inde, au Pakistan et aux États-Unis[23]. Ce type de situation peut non seulement porter atteinte à l'image publique d'un état-nation, mais aussi risquer d'entraîner dans le conflit des états-nations tiers ou des acteurs politiques ou idéologiques (parmi les exemples, citons les attaques de pirates informatiques contre des sites Web du gouvernement américain après le bombardement accidentel de l'ambassade de Chine en Yougoslavie en 1999 et le déclenchement du conflit de 2001 entre la Chine et les États-Unis après la collision d'un avion espion américain et d'un jet chinois[24]).

La proportionnalité dans le cyberespace est difficile à atteindre pour diverses raisons. Pour atténuer le risque d'escalade, la proportionnalité devrait impliquer un niveau de représailles proportionnel à celui que la victime a subi. De façon peut-être encore plus importante, lorsqu'un état-nation agit indépendamment du mandat d'une organisation internationale respectée comme les Nations Unies, il court le risque d'un revers diplomatique, voire économique. Il convient par conséquent de prendre en compte, dans le processus décisionnel, du type de réaction cinétique ou non cinétique, de la rapidité des représailles, des conséquences envisagées, de l'évaluation des dommages, ainsi que les retombées politiques potentielles avant l'exécution des représailles.

Les autres stratégies de dissuasion

D'autres stratégies de dissuasion ont connu des succès mitigés et peuvent servir de repères potentiels à la cyber-dissuasion. Dans ces cas, bien qu'il existe des points de convergence, dont la diversité du contingent d'acteurs potentiels, le caractère asymétrique des capacités (militaires) des défenseurs et des agresseurs, chacune de ces stratégies se caractérise par ses propres défis et aucune d'elles n'est assimilable au cyberespace. Un bref examen des modèles de dissuasion nucléaire, du terrorisme et des états voyous servira de paradigme comparatif. Nous évaluerons ainsi leur applicabilité au domaine cybernétique.

La dissuasion nucléaire

Il n'est pas de meilleur exemple de stratégie dissuasive réussie que celle des États-Unis et de l'Union soviétique pendant la guerre froide. La dissuasion nucléaire visait par définition des états déjà dotés d'armes nucléaires, dont elle entendait dissuader l'utilisation[25]. Au début des années 1970, la théorie de la « destruction mutuelle assurée » prévalait ; ni les États-Unis ni l'Union soviétique n'étaient suffisamment motivés, insensés, ignorants ou incohérents pour accepter le risque d'une guerre nucléaire[26]. La dissuasion nucléaire a été dans ce cas un franc succès, car aucun état-nation n'a depuis lors déployé une arme nucléaire contre une cible, car les coûts en vies humaines, en dommages matériels, en prestige international et en ressources naturelles l'emportent largement sur les avantages potentiels de l'utilisation des armes nucléaires.

Les principes de la dissuasion nucléaire peuvent-ils donc s'appliquer au cyberespace ? Largement considéré comme une puissance/menace asymétrique, analogue à son homologue nucléaire, le domaine du cyberespace est facilement transposable en un paradigme similaire dans certains domaines. On trouvera ci-après les principales similitudes entre les stratégies de cyber-dissuasion et de dissuasion nucléaire :

Les principales similitudes entre les cyber-conflits et les conflits nucléaires :

1. Les deux opèrent aux trois niveaux d'opérations militaires : stratégique, opérationnel et tactique, avec la possibilité de produire des effets sur tout le spectre allant de la petite échelle à l'ensemble de la population.
2. Tous deux ont la capacité de créer des effets destructeurs à grande échelle, voire planétaires.
3. Les deux peuvent être menés entre états-nations, entre un état-nation et des acteurs non étatiques, ou entre des groupes hybrides impliquant des états-nation et des mandataires non étatiques.
4. Le conflit nucléaire et le cyber-conflit « pourraient signifier pour l'adversaire une défaite totale, qui rendrait les guerres conventionnelles inutiles ».
5. Les deux peuvent provoquer intentionnellement ou involontairement des *effets de cascade* susceptibles de dépasser la cible d'attaque initiale[27].

Mais en dépit de certains recoupements, trop d'incohérences empêchent une adoption même partielle du modèle de dissuasion nucléaire. Celles-ci vont du volume d'acteurs opérant dans le cyberespace à la comparaison de la puissance des armes, en passant par la nature à double usage des outils eux-mêmes.

Principales différences :

1. Les états-nations n'assument généralement pas la responsabilité des actes hostiles commis dans le cyberespace.
2. Aucune cyberattaque n'a jusqu'à présent été en mesure de démontrer son potentiel de façon suffisamment impressionnante. Même si des attaques telles celle du malware

STUXNET et de logiciels malveillants de type essuie-glace, qui ont détruit 30 000 disques durs de la compagnie pétrolière saoudienne Saudi Aramco, n'ont conduit à des perturbations importantes, elles n'ont pas suffi à perturber de façon critique les opérations de l'installation nucléaire ou de la compagnie pétrolière.

3. L'attribution dans le cyberespace est extrêmement difficile et ne peut être aussi précise que l'identification d'un état-nation qui a lancé une arme nucléaire.

4. Contrairement à la mise au point d'armes nucléaires qui permet une surveillance, il n'y a pas de transparence similaire applicable à la production d'armes cybernétiques par les états et il n'existe pas non plus d'organisme international de surveillance[28].

Si on ajoute l'implication de groupes mandataires et de tierces parties, la nature grandissante et transfrontalière de l'environnement opérationnel et l'incertitude qui plane sur la réelle possibilité de dissuader les acteurs, il devient alors évident que la même transparence, fondamentale, qui a fait de la dissuasion nucléaire un succès n'a pas la même applicabilité dans le cyberespace.

La dissuasion antiterroriste

Plusieurs auteurs sont d'avis que la dissuasion antiterroriste peut, dans une certaine mesure, aboutir à des résultats, surtout si une organisation terroriste présente les attributs d'un état-nation, en ce sens où la destruction potentielle des actifs de celle-ci peut inciter le leadership terroriste à restreindre ses politiques pour les préserver[29]. Un auteur fait ainsi valoir que l'assassinat de dirigeants de haut niveau et de commandants opérationnels a eu un effet dissuasif temporaire, ne serait-ce que pour créer une période d'accalmie au cours de laquelle ces groupes ont dû se réorganiser[30]. Un autre auteur avance que pour assurer la réussite d'une politique de dissuasion antiterroriste, la partie menacée doit comprendre la menace (implicite ou explicite) et être amenée à calculer les coûts et les avantages de ses attaques lors de sa prise de décision[31]. Un autre encore affirme que même si les terroristes ne sont généralement pas « dissuadables », certaines attaques spécifiques peuvent l'être aujourd'hui[32].

On dénombre toutefois beaucoup plus d'obstacles que d'avantages à décourager le terrorisme, dont un grand nombre sont communs au domaine du cyberespace, en particulier lorsqu'il s'agit d'essayer de décourager un adversaire persévérant qui ne réside pas nécessairement au même endroit. Comment décourager les activités d'une personne ou d'un groupe sans savoir qui ils sont et où ils résident ?

La motivation est un autre facteur qui complique les efforts de dissuasion. Même si les dirigeants terroristes peuvent accorder de l'importance à leur propre vie, les groupes sont pleins d'individus prêts à mourir pour une cause. John Gearson, spécialiste de la sécurité nationale au Royaume-Uni, suggère que les concepts traditionnels de dissuasion ne fonctionneront pas contre un ennemi terroriste dont les tactiques avouées sont la destruction gratuite et l'assassinat d'innocents, dans la mesure où les soldats autoproclamés des groupes terroristes, dont la plus grande protection est l'absence d'appartenance à un pays, cherchent le martyre et la mort[33]. Un examen plus attentif révèle que la première moitié

de la réflexion de Gearson s'applique aussi aux cyber-acteurs hostiles. Les acteurs motivés par une cause, qu'elle soit politique, idéologique ou financière, ont du mal à être dissuadés, à moins qu'une action ne puisse leur causer des torts physiques, émotionnels ou financiers dont l'ampleur serait suffisante que pour freiner leur engagement.

Un autre élément perturbateur du succès d'une stratégie de dissuasion consiste à vouloir constamment influencer le comportement terroriste. Pour réussir, une menace dissuasive doit être conditionnée au comportement de l'adversaire. Or, si des individus et des groupes politiques croient qu'ils seront pris pour cible dans le cadre de la guerre anti-terroriste des États-Unis, ils seront moins enclins à faire preuve de retenue, quelles que soient leurs actions[34]. À ce jour, on ne compte aucun incident ou preuve avérée de succès d'une quelconque tentative de cyber-dissuasion par déni ou punition.

Les états voyous

Les États-Unis adoptent également des stratégies de dissuasion contre les états voyous qui menacent leur sécurité nationale. Des réflexions peuvent être faites des deux côtés de l'équation si l'on souhaite évaluer le succès des politiques menées par les États-Unis dans leur volonté de dissuader des États comme la Syrie et la Corée du Nord. D'une part, il n'y a pas eu de conflit militaire entre les États-Unis et ces ennemis, ce qui laisse entendre que les efforts de dissuasion ont été couronnés de succès. D'autre part, ces états poursuivent des programmes considérés par le gouvernement américain comme hostiles, indépendamment des efforts diplomatiques et économiques déployés par les États-Unis pour freiner leurs progrès. Au cours de son deuxième mandat, l'administration Bush a annoncé une nouvelle stratégie de « dissuasion sur mesure » afin d'exercer un effet de levier contre ces États voyous[35]. Ce raisonnement était fondé sur le fait que différentes stratégies pouvaient être élaborées pour différents états et différentes situations. Les États-Unis devaient ainsi avoir connaissance de ce à quoi les régimes étaient le plus attachés afin d'élaborer une stratégie dissuasive qui ciblerait les profils psychologiques de leurs dirigeants[36]. Mais plusieurs exemples récents, certes anecdotiques, illustrent pourquoi la dissuasion des états voyous est difficile à mettre en œuvre.

- **La Corée du Nord :** En 2013, la Corée du Nord a effectué son troisième essai nucléaire. En réponse, les États-Unis ont envoyé en vols d'entraînement des bombardiers B-52 suivis de bombardiers furtifs B-2 au-dessus de la Corée du Sud. Le pays a réagi par une rhétorique hostile et semblait prêt à lancer un vol d'essai d'un nouveau missile. Préoccupés par l'escalade de la situation, les États-Unis ont baissé le ton et réduit leurs manœuvres militaires[37]. Dans ce cas, les actions militaires dissuasives n'ont pas réduit les tensions entre les États-Unis et la Corée du Nord, et ont même risqué de provoquer une escalade vers un conflit militaire.
- **La Syrie :** En août 2012, en réponse à la tentative des rebelles syriens de renverser le régime syrien de Bachar al-Assad, le président Barack Obama a déclaré que toute utilisation d'armes chimiques serait considérée comme un franchissement de

la « ligne rouge ». Le président a appuyé ces commentaires en décembre en ajoutant que l'utilisation d'armes chimiques aurait des « conséquences », le langage diplomatique pour désigner des actions cinétique ou militaire potentielles[38]. Mais les États-Unis n'ont pas réagi à l'utilisation effective d'armes chimiques par l'Iran et le gouvernement américain a perdu une grande partie de sa crédibilité, un élément nécessaire à toute stratégie de dissuasion par punition.

La destitution potentielle n'est pas toujours un facteur dissuasif lorsqu'il s'agit de traiter avec des états-nations voyous dirigés par des régimes autoritaires. Qui plus est, la révocation de certains dirigeants n'a toujours pas dissuadé les autres dirigeants totalitaires d'agir. Ainsi, l'éviction de Mouammar Kadhafi lors de la guerre civile en 2011, conjuguée à sa disparition définitive avec l'appui matériel et logistique des États-Unis, n'a rien fait pour convaincre le al-Assad syrien de démissionner.

De façon analogue, les opérateurs des états-nations, les groupes mercenaires, les hacktivistes ou les criminels ne seront probablement pas découragés par l'application de la loi, par les activités de renseignement, ni même par l'engagement militaire. Des cybercriminels poursuivent leurs activités malgré plusieurs arrestations internationales d'envergure[39]. Les acteurs présumés des états-nations continuent de s'adonner au cyberespionnage en dépit de leur convocation dans des forums publics[40].

Les hacktivistes de l'opération Ababil continuent à mener des opérations DDoS contre les institutions financières américaines sans conséquence[41]. Ainsi, l'application d'une stratégie de dissuasion des états voyous sur le cyberespace est potentiellement inefficace en raison de la complexité et de la diversité du contingent d'acteurs hostiles. Nombre de ces acteurs ne fonctionnent pas comme un état voyou, dont le but ultime est la stabilité du régime et la préservation du leadership ; en tant que tels, ces acteurs ne chérissent pas les mêmes valeurs. Même les acteurs présumés des états-nations suivent les ordres de leur chaîne de commandement et ne s'arrêteraient qu'après en avoir reçu l'ordre de leur hiérarchie.

De l'(in)efficacité de la cyber-dissuasion

Martin Libicki avance que l'objectif de la cyber-dissuasion est de réduire « le risque d'attaque cybernétique à un niveau acceptable à un coût acceptable » ; une stratégie par laquelle l'état-nation qui se défend atténue les actions offensives potentielles par la menace de représailles[42]. Une telle politique peut-elle être réellement efficace ? S'il est tout à fait possible que la cyber-dissuasion ne soit pas exécutée en vase clos, dans sa *Strategy for Operating in Cyberspace* de 2011, le DOD a justifié le recours à des mesures de cyberdéfense active par une volonté de prévenir les intrusions et les activités adverses sur les réseaux et systèmes du DOD[43]. Cette responsabilité, associée à la divulgation du mémorandum, pourtant classé comme confidentiel, « Presidential Policy Directive-20 » (en partant du principe qu'il s'agit d'un document légitime) indique que les États-Unis peuvent se livrer à des attaques cybernétiques pour endiguer une menace imminente ou des attaques

en cours qui ne nécessitent pas l'approbation préalable du président, ce qui suggère que des actions cybernétiques dissuasives peuvent être menées de façon isolée[44]. Par conséquent, dans ce contexte, il est nécessaire d'apporter certains éclaircissements au sujet de la cyber-dissuasion. En aucun cas, le fait de préconiser des actions offensives à des fins défensives n'annule la nécessité d'adopter une politique de cyberdéfense bien établie. Ainsi, certaines vérités demeurent :

1. **Les cyberdéfenses traditionnelles doivent toujours être en place.** On peut faire valoir qu'une politique de « dissuasion par punition » efficace réduirait considérablement les dépenses associées à la cybersécurité traditionnelle en faisant baisser le coût des dispositifs informatiques, des programmes, de l'entretien, de la maintenance et du remplacement. Mais il ne faut pas s'y méprendre. Une stratégie de dissuasion ne peut s'attaquer à tous les acteurs hostiles du cyberespace. Si la dissuasion vise à dissuader des acteurs sérieux tels que les états-nations ou les cybercriminels plus sophistiqués et les groupes hacktivistes, qu'est-ce qui arrêtera la majorité des autres « nuisances » qui ciblent les réseaux ? Selon Jim Lewis, cyber-expert au Center of Strategic & International Studies, « les études menées révèlent que 80 à 90 pour cent des instruisons sur les réseaux des entreprises ne requièrent que des techniques élémentaires et que 96 pour cent d'entre elles auraient pu être évitées si des contrôles de sécurité adéquats avaient été mis en place[45] ». Un même son de cloche nous revient de l'Australian Signals Directorate (ASD), qui a dressé, en partenariat avec la National Security Agency des États-Unis, une liste de mesures qui auraient permis de contrecarrer la majorité des attaques relevées en 2009 et 2010[46]. Ainsi, même les pratiques de sécurité informatique les plus élémentaires resteraient nécessaires pour atteindre une couverture maximale.

2. **La dissuasion par punition repose sur la raison des acteurs.** La dissuasion est une option qui ne fonctionnera que si les personnes, les groupes et le gouvernement qui en font l'objet ont un comportement rationnel : ils peuvent être dissuadés parce qu'ils ne veulent pas risquer de perdre quelque chose de plus précieux. À l'heure actuelle, les adversaires opèrent dans le cyberespace parce qu'ils n'y craignent pas les représailles en raison des problèmes d'attribution. Ajoutons que l'environnement connecté, nébuleux et non sécurisé dans lequel ils agissent favorise leurs manœuvres. C'est pourquoi un état-nation est potentiellement plus sensible à la dissuasion qu'une organisation terroriste ou hacktiviste. Si l'adversaire n'a pas une vision rationnelle du monde et de la place qu'il y occupe, ou s'il n'a rien à perdre, il peut être très difficile de l'empêcher d'adopter une ligne de conduite particulière.

3. **L'adversaire doit posséder des biens de valeur.** En se basant sur la déclaration précédente, l'adversaire doit posséder des biens de valeur pour qu'une attaque préventive ou de représailles soit efficace. Si ce n'est pas le cas, la menace de cyber-dissuasion sera sans conséquence. Un état-nation possède potentiellement de nombreux actifs connectés à l'Internet ou en réseau. Et s'il s'agit d'un état fermé ? La Corée du Nord a par exemple très peu d'actifs en ligne connectés à l'Internet pouvant être ciblés à distance

(ce qui suggère que toute opération cybernétique efficace contre une cible de grande valeur devrait être menée par le biais d'opérations de proximité, comme lors de l'incident STUXNET). Et si l'adversaire est un groupe terroriste ou hacktiviste à structure cellulaire dispersé à l'échelle mondiale, quel point de valeur peut-il être exploité pour influer sur les actions de l'ensemble du groupe ?

En gardant ces vérités à l'esprit et en examinant les stratégies actuelles de dissuasion contre d'autres cibles, il est évident que la cyber-dissuasion par punition repose sur trois axiomes fondamentaux :

- **L'attribution.** La précision est frappée du sceau du bon sens, mais il est essentiel qu'un gouvernement sache qui l'a attaqué avant de lancer une contre-attaque. Mais comment gagner raisonnablement confiance dans un domaine qui se nourrit de l'ambiguïté ? Tant de facteurs sont à considérer avant de lancer une frappe de représailles, en ce compris sans toutefois s'y limiter : l'identité de l'agresseur (si elle est liée à un état-nation, l'agresseur a-t-il reçu des ordres de sa hiérarchie ou agit-il seul ? S'il s'agit d'une tierce partie, travaille-t-elle au nom d'un gouvernement d'état-nation ou agit-elle pour le soutenir ? S'agit-il d'une opération sous fausse bannière, pourquoi ou pourquoi pas ?) ; les motivations de l'attaque (Qu'est-ce qui a motivé l'attaque ? S'agissait-il de représailles ? Pour quel motif ?) ; et l'intention de l'attaque (L'intention de l'attaque était-elle de détruire, dégrader ou perturber ? Ou est-ce autre chose ? L'attaque avait-elle un but autre que ne le laissent croire les apparences ?). Autres éléments à prendre en considération : si l'attaque d'origine est considérée comme motivée par une cause, plusieurs états, hackers ou hacktivistes ont donc des raisons de mener une attaque. Même si ces tiers agissent au nom de l'état, qui de l'état ou des acteurs doit-on tenir pour responsables ? Qui est exactement la cible, l'état-nation qui tire les ficelles ou les auteurs de l'attaque ?

  L'attribution est-elle suffisante ? Si l'on considère le nombre de gouvernements qui ont désigné la Chine comme leur principale menace de piratage informatique, rien n'est fait pour arrêter ou décourager l'espionnage informatique chinois. Le président Obama a eu plusieurs entretiens avec son homologue chinois, Xi Jinping, qui n'ont abouti à aucun résultat concret[47]. Bien qu'il n'y ait eu à ce jour aucune tentative américaine connue pour mener une attaque de représailles à l'encontre des Chinois, cela prouve que l'attribution n'est pas la panacée, même si l'on confronte directement l'auteur présumé et que le défi reste de convaincre l'agresseur qu'il a effectivement été pris en flagrant délit[48].

- **La répétabilité**. La répétabilité entre les différents acteurs de la menace est une facette importante de la dissuasion cybernétique, et aussi l'une de ses plus grandes questions. Les acteurs individuels, les groupes cybercriminels, les services de renseignement étrangers, les unités militaires peuvent-ils tous être dissuadés par la même stratégie ? On peut répondre par la négative. Différentes stratégies et applications devraient être appliquées à différentes cibles d'acteurs. Ainsi, la façon dont

un gouvernement pourrait dissuader un groupe criminel ciblant sa base industrielle de défense peut être différente de celle dont il pourrait dissuader un état-nation adverse, ou même un état allié, de mener des activités d'espionnage. Pour de nombreux grands états nationaux disposant d'un bon réseau, les acteurs de la cybermenace ciblant ses ressources sont multiples. Il suffit de dire que les acteurs individuels et les petits groupes moins compétents (à moins de travailler au nom d'un état-nation ennemi) sont fort peu susceptibles d'être la cible d'une cyberattaque de représailles. En revanche, les groupes de cybercriminalité plus importants et plus sophistiqués, les hacktivistes et les acteurs des états-nations sont plus enclins aux représailles, car ils génèrent généralement plus de publicité et causent le plus de dégâts. Pour que la dissuasion par punition fonctionne efficacement, la cible doit comprendre que les représailles résultent directement de l'action incriminée. Si une cible ne comprend pas les représailles, il peut être nécessaire de les répéter en utilisant des tactiques plus fortes et plus visibles. Mais cette approche risque d'être mal interprétée par la cible, et si la cible n'a pas compris qu'il s'agissait de représailles, elle peut considérer cette attaque comme un acte d'origine. Cette situation pourrait rapidement dégénérer en conflit cybernétique.

- **Le succès**. Dans le cas de la cyber-dissuasion par punition, l'objectif tactique est d'arrêter une cyber-attaque pendant qu'elle a lieu, de punir les agresseurs après qu'elle a eu lieu ou de les punir avant qu'ils ne lancent l'attaque initiale. Dans le cas d'une punition pendant une attaque en cours, l'objectif serait de stopper cette dernière ; dans le cas d'une attaque ayant déjà eu lieu, l'objectif serait d'empêcher l'agresseur de se livrer pas à une activité similaire à l'avenir ; et enfin, dans le cas d'une attaque préventive, l'objectif serait d'empêcher l'agresseur de commettre une attaque. Sur le plan tactique, ces objectifs sont tous valables, mais sont-ils stratégiquement viables ? Autrement dit, gagnerait-on la bataille faute de pouvoir remporter la guerre ? Le fait de s'engager dans une cyber-attaque préventive ou de représailles présuppose que vous avez réussi à identifier la cible, vraisemblablement grâce à l'attribution de l'ordinateur à partir duquel l'ennemi opère. Bien que la frappe préventive ou de représailles puisse détruire cet ordinateur, l'adversaire peut avoir dix ou cinquante ordinateurs de plus pour continuer à fonctionner. Dans cet exemple, la nation qui se défend peut-elle croire qu'elle a vraiment gagné la bataille ? Autre exemple : si la frappe préventive ou de représailles vise une cible différente (par exemple un réseau électrique, une infrastructure essentielle, etc.), comment l'état victime tient-il compte de la proportionnalité, surtout si l'adversaire n'a même pas mené d'attaque ? Comment l'état sait-il avec certitude que l'ennemi comprendra que l'attaque préventive est en réalité une réponse à une action potentielle et que le message de dissuasion sera reçu et accepté ? Et si l'adversaire est un état-nation, comment expliquer l'éventuelle escalade qui pourrait découler de représailles perçues comme disproportionnées ? Libicki souligne que :

> une escalade est possible si les assaillants 1) estiment les représailles cybernétiques injustifiées ; 2) font face à des pressions internes les obligeant à réagir avec force ; ou 3) sont convaincus de leur supériorité dans d'autres domaines en cas de défaite cybernétique potentielle[49].

Conclusion

Dans le cyberespace, les efforts visant à lutter contre les actes hostiles par le recours à des frappes préventives ou de représailles semblent être un pas dans la bonne direction, surtout si l'on considère les échecs subis par certains états pour atténuer la menace d'activités malveillantes. Cependant, des milliers de cyberattaques se produisent chaque jour, ce qui suggère qu'il est très difficile de distinguer les menaces graves des menaces mineures[50]. Écraser une fourmi sur le sol de notre cuisine ne nous prémunira pas contre une possible infestation du reste de la colonie. De façon analogue, la cyber-dissuasion n'est pas la panacée pour les acteurs hostiles cherchant à exploiter les réseaux des secteurs public et privé. À l'heure actuelle, un trop grand nombre de variables sont encore inexplorées et nous ne disposons pas de plan suffisamment élaboré pour pouvoir s'en servir efficacement.

Les difficultés liées à l'attribution, l'incapacité de réagir rapidement, efficacement et avec précision, ainsi que l'impossibilité de créer et de maintenir un modèle reproductible contre différents acteurs resteront insurmontables à court terme pour que les pays victimes puissent lancer des cyberattaques préventives ou de représailles. La dissuasion cybernétique par déni a de meilleures chances de succès, mais seulement dans une mesure limitée, car les responsables de la protection des réseaux n'ont cessé d'être battus par des adversaires cachés dans l'immensité cyberespace qui se sont en outre montrés plus intelligents et plus agiles qu'eux. Au lieu de riposter contre des ennemis, les organisations doivent évaluer leur environnement de sécurité pour déterminer son efficacité dans le climat cybernétique actuel.

La cybersécurité n'est pas une solution statique ; à mesure que les assaillants acquièrent plus de connaissances et d'expérience, leurs tactiques, leurs techniques et leurs procédures évolueront avec le temps. Les stratégies de défense qui ont fonctionné il y a un an n'auront probablement pas le même succès aujourd'hui, compte tenu du rythme auquel ce paysage change. Selon l'équipe d'intervention d'urgence informatique du département de la Sécurité intérieure des États-Unis,

> un programme de cybersécurité efficace tire parti des normes et des bonnes pratiques de l'industrie pour protéger les systèmes et détecter les failles potentielles. Il a également recours à des systèmes de détection des menaces actuelles qui permettent une intervention et une reprise rapide des activités[51].

Les organisations doivent mettre en œuvre des plans de sécurité adaptables qui tiennent compte des aspects dynamiques du cyberespace et qui comprennent des jalons et des indicateurs de performance pour s'assurer de l'atteinte en temps opportun des objectifs visés. Des normes de sécurité plus strictes, telles que des correctifs de vulnérabilités

et des campagnes de sensibilisation des utilisateurs, doivent être adoptées afin de faire comprendre aux parties prenantes qu'elles sont responsables des défauts de conformité. Le très respecté SANS Institute, chef de file dans la formation et la certification en sécurité informatique, préconise la mise en œuvre de vingt contrôles de sécurité. Il affirme que les organisations de cyberdéfense qui ont réussi à incorporer ces contrôles ont réduit leur risque de sécurité[52]. En définitive, la diligence raisonnable en matière de cybersécurité reste, encore et toujours, le facteur déterminant dans la lutte contre les activités cybernétiques hostiles.

Notes

1. La Maison Blanche, *International Strategy for Cyberspace*, Washington, DC, mai 2011 ; département de la Défense, *Department of Defense's Strategy for Operating in Cyberspace*, Washington, DC, juillet 2011, www.defense.gov/news/d20110714cyber.pdf.

2. « Nuclear Weapons: Who Has Them At a Glance | Arms Control Association », avril 2013, www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat ; BRENNER, Susan W. et CLARKE, Leo L., « Civilians in Cyberwarfare: Casualties », *SMU Science & Technology Law Review* 13, 2010, p. 249 ; TODD, Graham H., « Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition », *Air Force Law Review* 64, rev 96, 2009 ; LYNN, William J. III, « The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack », *Foreign Affairs,* 28 septembre 2011, www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later.

3. KNOPF, Jeffrey W., « Use with Caution: The Value and Limits of Deterrence Against Asymmetric Threats **»,** *World Politics Review,* 11 juin 2013, www.worldpoliticsreview.com/articles/13006/use-with-cautionthe-value-and-limits-of-deterrence-against-asymmetric-threats.

4. LUPOVICI, Amir, « Cyber Warfare and Deterrence: Trends and Challenges in Research », *Military and Strategic Affairs* 3, no. 3, décembre 2011, p. 54.

5. KNOPF, « Use with Caution ».

6. LUPOVICI, « Cyber Warfare and Deterrence », p. 54.

7. ELLIOTT, David, « Deterring Strategic Cyberattack », *IEEE Security & Privacy* 9, no. 5, septembre /octobre 2011, pp. 36-40.

8. CLARK, W.K., et LEVIN, P.L., « Securing the Information Highway », *Foreign Affairs*, novembre/décembre 2009, pp. 2-10.

9. SOLOMON, Jonathan, « Cyberdeterrence between Nation States: Plausible Strategy or Pipe Dream? », *Strategic Studies Quarterly* 5, no. 1, 2011, p. 2.

10. « Obama Warns Al-Asad Against Chemical Weapons, Declares 'World is Watching' », *CNN Online*, 3 décembre 2012, www.cnn.com/2012/12/03/world/meast/syria-civil-war.

11. BURLIJ, Terrence et BELLANTONI, Christina, « Syria Crossed Obama's Redline. What Happens Next? » *PBS Online*, 14 juin 2013, www.pbs.org/newshour/rundown/2013/06/administration-sharpens-focus-onsyria-with-chemical-weapons-report.html.

12. « Few Satisfied, But U.S. Presses Syrian Arms Effort », *Las Vegas Sun Online*, 26 juillet 2013, www.lasvegassun.com/news/2013/jul/26/us-obama-aid-to-syria/.

13. GERTZ, Bill, « U.S., China Strategic and Economic Dialogue Criticized », *Washington Free Beacon*, 16 juillet 2013, http://freebeacon.com/u-s-china-conclude-strategic-and-economic-dialogue-talks/.

14. « China and Russia Submit Cyber Proposal | Arms Control Association », novembre 2011, www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal.

15. « Convention sur la cybercriminalité », *Conseil de l'Europe*, CETS no. 185, 25 novembre 2013, https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures.

16. WALSH, James Igoe, « Do States Play Signaling Games? », *Cooperation and Conflict: Journal of the Nordic International Studies Association* 42, no. 4, 2007, p. 441.

17. NAKASHIMA, Ellen, « Iran Blamed for Cyberattacks on U.S. Banks and Companies », *The Washington Post*, 21 septembre 2012, http://articles.washingtonpost.com/2012-09-21/world/35497878_1_web-sites-quds-force-cyberattacks.

18. HEALEY, Jason, « Beyond Attribution: Seeking National Responsibility for Cyber Attacks », *Conseil atlantique*, janvier 2012, www.acus.org/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF.

19. *Id*.

20. HIGGINS, Kelly Jackson, « The Intersection Between Cyberespionage and Cybercrime », *Dark Reading*, 21 juin 2012, www.darkreading.com/attacks-breaches/the-intersection-betweencyberespionage/240002514 ; HIGGINS, Kelly Jackson, « Attackers Engage in False Flag Attack Manipulation », *Dark Reading*, 1er octobre 2012, www.darkreading.com/attacks-breaches/attackers-engage-in-falseflag-attack-ma/240008256.

21. IASIELLO, Emilio, « Identifying Cyber-Attackers to Require High-Tech Sleuthing Skills », *National Defense*, décembre 2012, http://www.nationaldefensemagazine.org/archive/2012/December/Pages/IdentifyingCyber-AttackerstoRequireHigh-TechSleuthingSkills.aspx.

22. JENSEN, Eric Talbon, « Cyber Deterrence », *Emory International Law Review* 26, no. 2, 2012, p. 799.

23. « W32.Stuxnet », *Symantec*, 26 février 2013, www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

24. MESMER, Ellen, « Kosovo Cyber War Intensifies ; Chinese Hackers Targeting U.S. Sites, Government Says », *CNN Online*, 12 mai 1999, www.cnn.com/TECH/computing/9905/12/cyberwar.idg/ ; SMITH, Craig S., « May 6-12: The First World Hacker War », *The New York Times*, 13 mai 2001, www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html.

25. RECORD, Jeffrey, « Nuclear Deterrence, Preventative War, and Counterproliferation », *The Cato Institute* 519, 8 juillet 2004, www.cato.org/sites/cato.org/files/pubs/pdf/pa519.pdf.

26. PAYNE, Keith B. et WALTON, C. Dale, « Deterrence in the Post-Cold War World », *Strategy in the Contemporary World, An Introduction to Strategic Studies*, éd. BAYLIS, John, WIRTZ, James, COHEN, Eliot et COLINS, Gray, New York : Oxford University Press, 2002, p. 169.

27. MULVENON, James C. et RATTRAY, Gregory J., « Addressing Cyber Instability: Executive Summary », *Conseil atlantique*, 8 juillet 2004, www.acus.org/files/CCSA_Addressing_Cyber_Instability.pdf.

28. IASIELLO, Emilio, *Cyber Attack: A Dull Tool to Shape Foreign Policy*, Tallinn : NATO CCD COE Publications, mai 2013, p. 398.

29. BAR, Shmuel, « Deterring Terrorists », *Hoover Institution*, 2 juin 2008, www.hoover.org/publications/policy-review/article/5674.

30. Ibid.

31. TRAGER, Robert F. et ZAGORCHEVA, Dessislava P., « Deterring Terrorism », *International Security* 30 no. 3, hiver 2005/2006, p. 87.

32. DAVIS, Paul K. et JENKINS, Brian Michael, *Deterrence & Influence in Counterterrorism: A Component in the War on Al Qaeda*, Santa Monica, CA : RAND Corp., 2002, p. 59.

33. GEARSON, John, « Deterring Conventional Terrorism: From Punishment to Denial and Resilience », *Contemporary Security Policy* 33, no. 1, 2012, p. 171.

34. KROENIG, Matt et PAVEL, Barry, « How to Deter Terrorism », *The Washington Quarterly* 5, no. 2, printemps 2012, p. 21.

35. KNOPF, « Use with Caution ».

36. *Id*.

37. *Id*.

38. *Id*.

39. « FBI: More Arrests in International Cyber Crime Takedown », *Infosec Island*, 13 juillet 2012, www.infosecisland.com/blogview/21907-FBI-More-Arrests-in-International-Cyber-Crime-Takedown.html ; O'TOOLE, James, « Global Financial Cybercrime Sting Yields 24 Arrests », *Money CNN Online*, 26 juin 2012, http://money.cnn.com/2012/06/26/technology/cybercrime-arrests/index.htm.

40. RAGAN, Steve, « China's APT 1 Still Operating with the Same Modus Operandi », *Security Week*, 1er mai 2013, www.securityweek.com/chinas-apt1-still-operating-same-modus-operandi.

41. KITTEN, Tracy, « DDoS: Attackers Announce Phase 4 », *Bank Info Security*, 23 juillet 2013, www.bankinfosecurity.com/ddos-attackers-announce-phase-4-a-5929/op-1.

42. LIBICKI, Martin, *Cyberdeterrence and Cyberwar,* Santa Monica, CA : RAND Corp., 2009, www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

43. Département de la Défense. *Strategy for Operating in Cyberspace*, Washington, DC : département de la Défense, juin 2011, www.defense.gov/news/d20110714cyber.pdf.

44. « Obama Tells Intelligence Chiefs to Draw up Cyber Target List – Full Document Text », *The Guardian*, 7 juin 2013, www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text.

45. LEWIS, James A., « Raising the Bar on Cyber Security », *Center for Strategic & International Studies*, 12 février 2013, http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf.

46. *Id*.

47. NEUMANN, Scott, « Chinese Cyber Hacking Discussed at Obama-Xi Summit », *NPR Online*, 9 juin 2013, www.npr.org/blogs/thetwo-way/2013/06/09/190058558/chinese-cyber-hacking-discussed-at-obama-xisummit ; CONSTANTIN, Lucian, « The Chinese Hacker Group that Hit the New York Times is Back with Updated Tools », *Computerworld*, 12 août 2013, www.computerworld.com/s/article/9241577/The_Chinese_hacker_group_that_hit_the_N.Y._Times_is_back_with_updated_tools.

48. LIBICKI, *Cyberdeterrence and Cyberwar*.

49. *Id*.

50. KRAMER, Franklin D, « Policy Recommendations for a Strategic Framework », in *Cyberpower and National Security*, éd. KRAMER, Franklin D., STARR, Stuart H., et WENTZ, Larry K., Dulles, VA : Potomac Books Inc. et National Defense University Press, 2009, p. 15.

51. BYERS, Eric, « Essential Cyber Security Concepts for CEOs », *Belden*, 28 février 2013, www.belden.com/blog/industrialsecurity/Essential-Cyber-Security-Concepts-for-CEOs.cfm.

52. « SANS Institute – CIS Critical Security Controls », www.sans.org/critical-security-controls/