La rétribution et la dissuasion du cyber terrorisme

John J. Klein, PhD*

Depuis son entrée en fonction, le président Barack Obama n'a cessé de présenter la cyber sécurité comme l'un des principaux défis auxquels font face les États-Unis[1]. Ce faisant, il n'a pas manqué de relever l'ironie du fait que les technologies qu'utilisent les États-Unis pour accomplir de grandes choses peuvent également servir à compromettre leur sécurité et à nuire à leurs citoyens. Les technologies de l'information et les systèmes de défense qui confèrent à l'armée américaine sa supériorité sont pris pour cible par des hackers chinois et russes, dont les attaques pourraient accroître les vulnérabilités. Par conséquent, les cyber attaques continues et persistantes sont considérées comme une menace pour la sécurité nationale des États-Unis[2].

Le cyber terrorisme figure parmi les grands enjeux de la cyber sécurité évoqués par le président Obama. Malheureusement, bien qu'examinée depuis le début des années 2000, sa définition fait encore débat. La confusion autour du cyber terrorisme découle en partie des récentes tentatives d'élargir le concept pour y inclure l'hacktivisme ainsi que l'utilisation de l'Internet par les terroristes en vue de faciliter des actes terroristes traditionnels[3]. Par ailleurs, certains stratèges et responsables politiques soutiennent qu'il est impossible de prévenir les actes de cyber terrorisme, qu'ils soient perpétrés par des états ou par des acteurs non étatiques[4].

Ce point de vue est cependant erroné ou, tout au mieux, à moitié vrai[5]. L'histoire et le déroulement des conflits dans les autres médias de guerre ont montré que la menace crédible d'une force écrasante ou d'autres mesures sévères pouvait, si les conditions étaient réunies, dissuader les agresseurs potentiels de s'engager dans une confrontation directe.

---

*John J. Klein est chercheur résident au sein de la société Falcon Research, en Virginie du Nord (États-Unis). Il est titulaire d'un doctorat en science politique, centré sur les études stratégiques, de l'université de Reading et d'un Master en études stratégiques et sécurité intérieure du U.S. Naval War College, où il a participé au programme Mahan Scholars. Auparavant, il a été Federal Executive Fellow dans le cadre du programme d'études en politique étrangère de la Brookings Institution. John J. Klein publie régulièrement des articles sur la politique nationale, la stratégie militaire et les implications du droit des conflits armés.

Les opinions exprimées dans cet article n'engagent que leur auteur et ne reflètent pas nécessairement les points de vue de Falcon Research ou ceux du gouvernement des États-Unis.

KLEIN, John J., « Deterring and Dissuading Cyberterrorism », *Journal of Strategic Security* 8, no 4, 2015, pp. 23-38. DOI : http://dx.doi.org/10.5038/1944-0472.8.4.1460 consultable sur : http://scholarcommons.usf.edu/jss/vol8/iss4/2.

Cyberespace et cyber terrorisme

Le domaine cybernétique, ou cyberespace, a été défini comme suit par Andrew Krepinevich :

> Les réseaux d'ordinateurs [du monde], à la fois ouverts et fermés, y compris les ordinateurs eux-mêmes, les réseaux transactionnels qui transmettent des données relatives aux transactions financières et les réseaux dotés de systèmes de contrôle qui permettent aux machines d'interagir[6].

Ainsi, le domaine cybernétique utilise des canaux de communication étendus, composés d'un réseau global et de hubs d'activités au niveau des grappes de serveurs ou des emplacements du matériel réseau[7]. Parmi les activités cybernétiques figurent la finance et le commerce international, les réseaux sociaux, le partage d'informations et, plus récemment, certaines activités militaires[8].

Pour déterminer dans quelle mesure il est possible de rétribuer les actes terroristes dans le cyberespace, on peut s'appuyer sur la définition du cyber terrorisme proposée par Dorothy Denning en 2000 devant la Commission des forces armées de la Chambre des représentants des États-Unis :

> Le cyber terrorisme est la convergence entre le cyberespace et le terrorisme. Il fait référence aux attaques illégales et aux menaces d'attaques contre des ordinateurs, des réseaux et les informations qui y sont stockées, dans le but d'intimider ou de faire pression sur un gouvernement ou sa population à des fins politiques ou sociales. En outre, pour être qualifiée de cyber terrorisme, une attaque doit s'accompagner de violence contre des personnes ou des propriétés, ou causer suffisamment de tort pour susciter la peur. C'est le cas notamment des attaques qui causent la mort ou des blessures, provoquent des explosions ou entraînent d'importantes pertes économiques. Les graves attaques contre les infrastructures critiques peuvent relever du cyber terrorisme, en fonction de leur impact. Celles qui perturbent des services non essentiels ou représentent avant tout un désagrément coûteux ne sont pas considérées comme actes terroristes[9].

Les attaques dont l'ampleur est limitée, mais qui causent la mort, des blessures, des coupures d'électricité prolongées, des accidents d'avion, la contamination de l'eau ou une perte de confiance importante dans certains secteurs de l'économie peuvent également être qualifiées d'actes cyber terroristes[10].

La définition susmentionnée n'inclut pas l'hacktivisme dans le cyber terrorisme. *Hacktivisme* est un terme employé par de nombreux universitaires pour désigner l'alliance du piratage informatique et de l'activisme politique[11]. À l'image des hackers, les hacktivistes mènent des actions clandestines en ligne visant à révéler, à manipuler ou à exploiter les vulnérabilités des systèmes d'exploitation informatiques et autres logiciels. Contrairement aux hacktivistes, les simples hackers ne poursuivent généralement pas d'objectifs politiques[12].

Bien que motivé par des raisons politiques, l'hacktivisme n'est pas une forme de cyber terrorisme. Si les hacktivistes s'efforcent habituellement de perturber le trafic Internet ou les réseaux informatiques en signe de protestation publique, ils ne cherchent pas pour autant à tuer, mutiler ou terrifier[13]. Leurs récents succès mettent toutefois en lumière

la menace que représente le cyber terrorisme, un petit nombre d'individus peu scrupuleux étant à même d'emprunter les méthodes des hackers pour semer le trouble, susciter la peur et provoquer des blessures graves ou la mort[14]. Toutefois, la frontière entre cyber terrorisme et hacktivisme est parfois poreuse. C'est notamment le cas lorsque les groupes terroristes recrutent des hackers doués ou les rallient à leur cause, ou lorsque les hacktivistes décident d'intensifier leurs actions en attaquant les systèmes qui contrôlent les composants critiques de l'infrastructure nationale, comme les réseaux électriques et les services de secours[15].

Les experts en sécurité soutiennent depuis un certain temps que le secteur de l'énergie est devenu la cible potentielle de cyber attaques basées sur la création de connexions Internet, à la fois physiques et sans fil, interférant avec les systèmes de contrôle, de surveillance et d'acquisition des données (SCADA) utilisés par les réseaux de distribution électrique[16]. Les systèmes SCADA assurent la gestion des flux d'électricité et de gaz naturel et sont utilisés pour contrôler les systèmes industriels et les installations des usines de traitement chimique, les opérations d'épuration et de distribution de l'eau, les installations de gestion des eaux usées et un bon nombre d'entreprises manufacturières[17]. Diverses études ont montré que les infrastructures critiques dotées de systèmes SCADA sont susceptibles d'être la cible d'attaques cyber terroristes, car la complexité de l'infrastructure et des systèmes informatiques utilisés est telle qu'il est quasiment impossible d'éliminer toutes les vulnérabilités potentielles[18]. Nombre d'experts en sécurité pensent que la capacité d'un terroriste à contrôler, perturber ou modifier les fonctions de commandement et de surveillance des systèmes SCADA pourrait menacer la sécurité régionale ou nationale[19].

De manière générale, le cyber terrorisme peut aussi bien être le fait d'acteurs étatiques que d'acteurs non étatiques, mais les calculs et les implications peuvent varier sensiblement d'une catégorie à l'autre. Il convient de noter que le département d'État des États-Unis a listé en 2015 trois États considérés comme soutenant le terrorisme : l'Iran, le Soudan et la Syrie[20]. Le cyber terrorisme financé par un état cherchera probablement à atteindre les objectifs fixés par les dirigeants politiques de l'état en question et ses actions tendront à appuyer les objectifs de sécurité nationale à long terme. Bien que le domaine cybernétique offre un minimum d'anonymat, s'il est possible de remonter à la source à un réseau ou à l'adresse Internet d'une cyber attaque, l'emplacement physique de ceux qui l'ont perpétré pourra être établi dans les frontières de l'état qui l'aura autorisée. Étant donné que les états ont des frontières physiques et les réseaux informatiques susceptibles de déclencher une attaque sur un emplacement physique, la probabilité que ses instigateurs soient identifiés est plus élevée si la cyber attaque est soutenue par un état que si elle est perpétrée par des acteurs non étatiques.

En revanche, les acteurs non étatiques, qui regroupent de nombreuses organisations terroristes, n'auront pas forcément une action uniforme ou fondée sur les mêmes convictions profondes, et la plupart des organisations les plus violentes sont motivées par une idéologie qui s'appuie sur le martyre et sur une vision apocalyptique[21]. Cette idéologie peut être fondée sur la religion ou sur la volonté de renverser un gouvernement. Les terroristes qui agissent par idéologie et envisagent de lancer des cyber attaques contre les

Etats-Unis ou leurs intérêts ne se soucient peut-être pas des répercussions d'un acte cyber terroriste, qu'elles soient d'ordre militaire ou non. Dans un tel scénario, il peut s'avérer difficile, selon certains stratèges, de rétribuer les leaders d'une organisation terroriste par des moyens militaires traditionnels[22]. Certains experts en sécurité affirment que malgré des motivations disparates, de nombreuses organisations terroristes, y compris Al-Qaïda et l'État islamique autoproclamé, fonctionnent de manière stratégique et rationnelle[23]. Si les leaders d'une organisation terroriste sont enclins à prendre des décisions rationnelles, la rétribution peut à certains moments apparaître comme une méthode adéquate pour influencer leurs futures actions. Elle doit, par conséquent, être considérée comme un élément essentiel au succès d'une stratégie nationale visant à prévenir le cyber terrorisme.

Les avantages du cyber terrorisme

L'utilisation du domaine cybernétique dans la réalisation d'actes terroristes présente plusieurs avantages. Premièrement, le cyber terrorisme peut se révéler nettement moins coûteux que les méthodes terroristes traditionnelles[24]. Il suffit de se procurer un ordinateur personnel et une connexion Internet, au lieu de devoir acheter des armes comme des fusils et des explosifs ou d'acquérir des moyens de transport[25]. Deuxièmement, le cyber terrorisme offre un anonymat accru par rapport aux méthodes cinétiques traditionnelles[26]. Les services de police et de sécurité peuvent avoir des difficultés à retrouver l'identité des terroristes qui utilisent en ligne des « noms d'écran » ou se connectent comme « utilisateur invité » sans s'identifier[27]. Troisièmement, le nombre de cibles potentielles est énorme comparé au nombre de cibles généralement visées par les actions cinétiques. Les cyber terroristes peuvent s'attaquer aux réseaux informatiques des gouvernements, des individus, des services publics, des compagnies aériennes privées, ainsi qu'aux systèmes SCADA et autres réseaux critiques. On considère que le nombre incalculable de cibles cybernétiques potentielles augmente la probabilité qu'un adversaire trouve une faiblesse ou une vulnérabilité à exploiter dans l'un des différents réseaux. Enfin, le cyber terrorisme peut être mené à distance, un aspect qui peut s'avérer particulièrement attrayant pour certains agresseurs potentiels.

Une menace exagérée ?

De nombreuses voix critiques ont toutefois souligné que, si la menace potentielle que représente le cyber terrorisme est alarmante, malgré toutes les prévisions funestes annonçant une attaque imminente, aucun exemple concret d'acte de cyber terrorisme n'a été relevé[28]. Jusqu'ici, aucun cas d'attaque cyber terroriste contre les installations publiques, les réseaux de transport, les centrales nucléaires, des réseaux d'électricité, ou tout autre élément clé de l'infrastructure nationale des États-Unis n'a été enregistré. Si les cyber attaques contre les composantes critiques de l'infrastructure nationale ne sont pas rares, elles ne sont pas menées de façon à causer le type de dommages ou les graves conséquences caractéristiques d'un acte cyber terroriste[29]. La vaste attaque par déni de service qui a touché l'Estonie en 2007, paralysant le système bancaire pendant trois semaines, n'a

causé aucun dégât catastrophique et n'a fait aucune victime[30]. Même le logiciel malveillant Stuxnet, découvert en juin 2010 et considéré comme « la première arme numérique au monde » en raison de sa capacité à détruire physiquement les ordinateurs et autres équipements, n'a pas eu d'effets destructifs graves et généralisés[31].

On peut alors se demander dans quelle mesure le cyber terrorisme représente véritablement une menace réelle. S'il peut apparaître comme une option attrayante pour les terroristes modernes qui apprécient l'accès à distance, l'anonymat, la possibilité de provoquer d'importants dégâts et l'impact psychologique, certaines voix critiques affirment que les craintes sont exagérées[32]. Par ailleurs, les cyber experts ne sont pas d'accord sur le fait que les systèmes informatiques des infrastructures critiques, y compris les systèmes SCADA, représentent pour les terroristes une cible efficace pour parvenir à leurs fins[33].

Nombreux sont les spécialistes en sécurité informatique estimant qu'il n'est pas possible de causer des dommages, des blessures ou la mort à grande échelle en utilisant l'Internet[34]. Certains affirment que les investissements en temps, argent et expertise injectés dans la conception et le développement des systèmes informatiques critiques garantissent leur résilience aux attaques. Ainsi, le Département de la Défense (DoD), la Central Intelligence Agency (CIA) et le Federal Bureau of Investigation (FBI), par exemple, protègent leurs systèmes les plus critiques en les isolant de l'Internet et de tous les autres réseaux informatiques internes grâce à la méthode de l'air gap[35].

Indépendamment du débat en cours pour savoir si la menace cyber terroriste est exagérée ou pas et si les potentiels effets destructeurs sont suffisamment graves pour soulever des inquiétudes, les rapports des médias comme des gouvernements indiquent que certaines organisations terroristes ont désormais recours à l'Internet pour communiquer, recruter, collecter des fonds et coordonner de futures attaques[36]. Bien qu'aucune information publique ne confirme que des organisations terroristes aient attaqué directement et avec succès des serveurs Internet ou d'importants réseaux informatiques, les rapports suggèrent que nombre d'entre elles seraient prêtes à employer des moyens virtuels pour parvenir à leurs fins si l'occasion se présentait[37]. Étant donné que certaines organisations terroristes semblent nourrir le désir permanent d'utiliser tous les moyens possibles, y compris les cyber attaques, pour atteindre leurs objectifs, les responsables politiques et les stratèges militaires doivent impérativement prendre les mesures préventives nécessaires pour empêcher de tels actes et minimiser les conséquences d'une éventuelle attaque. Les mesures de rétribution font partie de ces actions préparatoires.

La rétribution et le droit des conflits armés

Selon une définition largement reprise, la rétribution consiste à « persuader un ennemi potentiel qu'il est dans son propre intérêt d'éviter certaines actions[38] ». Le principe qui sous-tend la théorie de la rétribution cybernétique, une sous-catégorie de la rétribution générale, repose sur l'idée qu'une force crédible et potentiellement écrasante ou d'autres actions menées contre un adversaire potentiel seraient suffisantes pour dissuader la plupart des agresseurs éventuels de lancer des cyber attaques, y compris les actes rele-

vant du cyber terrorisme. Quand on s'intéresse à la rétribution dans le domaine cybernétique, il convient de prendre en compte le conseil de Colin Grey : « Étant donné que la rétribution fonctionne uniquement, quand elle fonctionne, dans l'esprit des leaders ennemis, c'est leur vision du monde, et non la nôtre, qui détermine son succès ou son échec[39] ». Par conséquent, pour dissuader un adversaire potentiel, il convient de dissuader ses dirigeants ou responsables.

La théorie de la rétribution part du principe que la rétribution ne fonctionne que s'il existe une menace crédible de représailles ou de recours à la force. Les mesures de représailles considérées comme crédibles au sein de la communauté de défense américaine sont généralement régies par le droit des conflits armés (DCA), également appelé droit de la guerre. Bien qu'ils ne constituent pas une directive ou un moyen de prévenir toute action future, les idées et les principes énoncés dans le DCA s'appliquent aux mesures visant à lutter contre le terrorisme, et contre le cyber terrorisme.

Le DCA est la partie du droit international qui régit la conduite des hostilités armées[40]. Il s'appuie sur deux sources principales. Le droit international coutumier, d'une part, qui découle des hostilités et lie tous les états, et le droit international des traités, d'autre part, qui découle des traités internationaux et lie uniquement les états qui ont ratifié un traité donné[41]. Le DCA vise à réduire les dommages et les pertes de vie humaine occasionnés par tout conflit, à protéger les combattants et les non-combattants de souffrances inutiles, à sauvegarder les droits fondamentaux des combattants et des non-combattants, et à faciliter le rétablissement de la paix à l'issue du conflit.

Deux des principes énoncés dans le droit des conflits armés sont particulièrement pertinents pour le suivi des actes de cyber terrorisme, à savoir la nécessité militaire et le ciblage licite. Le premier exige d'utiliser uniquement le degré et le type de force nécessaire pour soumettre partiellement ou totalement l'ennemi, tout en veillant à minimiser les pertes de temps, de vie et de ressources physiques[42]. Il vise à limiter l'application de la force requise à des fins militaires licites. Si le principe de nécessité militaire admet que des dommages collatéraux et des blessures accidentelles peuvent être subis par la population civile en cas d'attaque d'une cible militaire légitime, il n'excuse pas la destruction de vies humaines et de biens disproportionnée par rapport à l'avantage militaire visé[43].

Le deuxième principe, celui du ciblage licite, repose sur trois hypothèses : le droit du belligérant à infliger des pertes à l'ennemi n'est pas illimité ; le ciblage des populations civiles est interdit ; les combattants doivent être distingués des non-combattants afin d'éviter autant que possible d'épargner les non-combattants[44]. Il présuppose donc que toutes « les précautions raisonnables » soient prises pour s'assurer de cibler uniquement des objectifs militaires afin d'éviter autant que possible tout dommage causé à des biens civils (dommages collatéraux) ou la mort et les blessures des civils (blessures accidentelles)[45].

Dérivé du concept de rétribution, la rétribution élargie fait actuellement l'objet d'études et de débats au sein du département de la Défense des États-Unis. La « rétribution élargie » consiste à renforcer la rétribution régionale et à rassurer les alliés et les partenaires des États-Unis par la menace crédible de représailles[46]. Le Commandement stratégique des États-Unis, qui supervise le Cyber commandement US, a récemment

organisé une conférence afin de discuter et d'évaluer la capacité du département de la Défense à rétribuer des états ou des acteurs non étatiques particuliers de mener des cyber attaques susceptibles d'avoir de graves conséquences sur le territoire et pour les intérêts américains, telles que la perte de vies humaines, la destruction massive de propriété, ou un impact considérable sur les intérêts économiques et étrangers des États-Unis[47]. La conférence s'est également penchée sur l'identification de méthodes qui permettraient de dissuader la Russie, la Chine, l'Iran et la Corée du Nord de lancer des cyber attaques contre les alliés internationaux, ce qui relève du domaine de la rétribution élargie[48]. Basée sur plusieurs centaines d'années de primauté des traités, la rétribution élargie apparaît comme un concept stratégique viable pour le cyberespace. Ainsi, l'article 51 de la Charte des Nations Unies reconnaît, par exemple, l'autodéfense collective comme un droit inhérent à un ou plusieurs états[49]. Les états parties à un accord de rétribution élargie, ou signataires d'un traité d'autodéfense, doivent servir à décourager les conflits ou contribuer à la défense de leurs alliés en cas d'échec de la rétribution. Ce concept demeure pertinent dans le cyberespace.

Les réponses appropriées au cyber terrorisme

Si l'on se fonde sur les principes de la nécessité militaire et du ciblage licite précédemment évoqués, toute réponse militaire au cyber terrorisme se doit de cibler et d'attaquer uniquement des objectifs militaires, c'est-à-dire les combattants et les objets qui, par leur nature, leur emplacement, leur but ou leur utilisation, contribuent effectivement aux combats et à l'entretien du conflit[50]. Les objectifs militaires incluent également les objets dont la destruction totale ou partielle, la saisie ou la neutralisation procurerait un net avantage militaire à l'attaquant dans les circonstances données au moment de l'attaque[51]. Par ailleurs, quand on examine les cyber objets militaires à prendre pour cible et attaquer, il est important de comprendre qu'il n'est pas illégal de causer des blessures accidentelles aux civils ou des dommages collatéraux aux objets civils, dans le cadre d'une attaque licite contre un objectif militaire. Les blessures accidentelles et les dommages collatéraux ne doivent cependant pas être excessifs par rapport à l'avantage anticipé de l'attaque[52].

S'appuyant sur les principes du DCA, l'administration Bush a publié en février 2003 un rapport intitulé *The National Strategy to Secure Cyberspace* (Stratégie nationale de défense du cyberespace), stipulant que le gouvernement des États-Unis se réserve le droit de répondre « de manière appropriée » à toute attaque informatique dirigée contre le pays[53]. Cette réponse peut impliquer l'utilisation d'armes cybernétiques ou de codes malveillants américains conçus pour perturber les systèmes informatiques ciblés de l'adversaire[54]. Pour être considérée comme « appropriée », toute mesure de réaction militaire doit s'inscrire dans l'esprit du DCA.

La question est donc de savoir ce qui constitue ou non une réponse appropriée à un acte cyber terroriste. Premièrement, considérant le degré et le type de force requise pour soumettre partiellement ou totalement l'ennemi, toute réponse, qu'elle soit cinétique ou cybernétique, ne doit pas apparaître comme excessive ou disproportionnée par rapport à

l'avantage militaire escompté. Par conséquent, si l'attaque d'un agresseur blesse ou cause la mort d'une douzaine de personnes et la contre-attaque fait un millier de victimes, avec un résultat disproportionné par rapport à l'avantage ou au gain militaire obtenu, la situation sera considérée comme inappropriée au regard du DCA. Deuxièmement, partant du fait que toute contre-attaque doit cibler des objectifs militaires contribuant effectivement à la capacité de l'ennemi à mener des combats et à entretenir le conflit, la mise hors service ou la destruction des serveurs réseau et de l'infrastructure informatique que l'adversaire utilise pour lancer ses attaques pourra sembler conforme aux principes du DCA.

La réponse à une cyber attaque n'est pas forcément de nature militaire, mais pourra comprendre des actions non militaires, telles que des mesures économiques ou financières. Ainsi, alors que le nombre démesuré et toujours croissant de cyber attaques perpétrées contre les systèmes américains atteignait un seuil permettant d'envisager une situation d'urgence nationale, le président Obama a publié en avril 2015 un décret visant à nuire aux finances de leurs instigateurs. Le décret du président stipule :

> À compter d'aujourd'hui, nous mettons en garde tous ceux qui menacent sérieusement notre sécurité ou notre économie, en portant atteinte à notre infrastructure critique, en perturbant ou en piratant nos réseaux informatiques ou en volant les secrets commerciaux des entreprises américaines ou les données personnelles des citoyens américains à leur profit[55].

Ce décret donne au département du Trésor américain le pouvoir d'imposer des sanctions aux individus ou entités responsables de cyber attaques ou de cyber espionnage. En réalité, il autorise le gel des actifs transitant par le système financier américain et interdit aux responsables des cyber attaques d'effectuer des transactions avec les sociétés américaines.

Les contre-arguments

Il existe plusieurs contre-arguments à l'hypothèse soutenant que la rétribution serait efficace contre le cyber terrorisme. Jim Lewis estime, par exemple, que la rétribution ne fonctionnera pas dans le domaine cybernétique[56]. Il affirme que la vulnérabilité asymétrique face aux attaques, de nouvelles classes d'adversaires avec une tolérance au risque très différente et la difficulté d'élaborer une réponse proportionnelle et crédible réduisent la capacité de rétribution dans les domaines cybernétiques et spatiaux[57]. Il souligne qu'aux États-Unis les organisations publiques et privées sont la cible de cyber attaques quotidiennes et que s'il était possible de rétribuer ces attaques, alors les efforts du gouvernement américain pour tirer parti de ces capacités seraient déplorables[58].

D'autres critiques affirment que l'utilisation d'armes cybernétiques en réaction à une cyber agression aurait des conséquences graves et généralisées, débordant du cadre du DCA[59]. Ces effets pourraient s'avérer difficiles à limiter ou à maîtriser. On peut craindre qu'à la suite d'une attaque informatique dirigée contre un groupe terroriste, le code malveillant se répande par inadvertance via l'Internet. Un tel scénario pourrait gravement affecter, voire mettre hors service, les systèmes des infrastructures critiques d'autres pays

non-belligérants, y compris les systèmes exploités par les États-Unis et leurs alliés et partenaires.

D'autres voix critiques soutiennent de leur côté que le choix d'une cible réelle pour une réponse militaire à un acte de cyber terrorisme perpétré par un acteur non étatique peut s'avérer problématique. Les terroristes non soutenus par un état ne sont, en effet, pas forcément confinés dans des frontières géographiques claires, et il est donc difficile d'éviter de toucher la population civile. Une cyber attaque lancée par les États-Unis contre les ordinateurs et les réseaux des terroristes peut affecter les systèmes informatiques civils critiques du pays hébergeant le groupe terroriste et avoir ainsi des effets non conformes au principe du ciblage licite. C'est précisément pour cette raison que certains stratèges et responsables politiques ont longtemps affirmé que la rétribution était inefficace contre les leaders terroristes, car la réponse crédible à une cyber attaque terroriste peut se révéler non viable.

Enfin, d'autres critiques pourraient arguer que les États-Unis et les autres états ne sont pas liés par le DCA en cas de cyber attaque terroriste, car les terroristes sont des combattants illégaux qui ne respectent pas les dispositions du DCA. En définitive, les combattants illégaux sont par définition des individus qui participent directement à des hostilités sans y être autorisés par une autorité gouvernementale, et les terroristes non parrainés par un état appartiennent à cette catégorie. Il n'en demeure pas moins que toute réponse des États-Unis à une cyber attaque menée par des terroristes, c'est-à-dire par des combattants illégaux, doit respecter les principes du DCA. En effet, le DCA traite spécifiquement des actes terroristes, précisant que les combattants illégaux engagés dans des hostilités violent le DCA et deviennent de ce fait des cibles licites[60]. Ils peuvent, par conséquent, être tués ou blessés et, s'ils sont capturés, jugés comme des criminels de guerre pour leurs actions[61].

Une stratégie de prévention holistique

L'objectif d'une stratégie visant à prévenir un acte cyber terroriste consiste à persuader les dirigeants d'une organisation terroriste que les coûts d'une attaque sont beaucoup plus élevés que le résultat escompté ou que l'attaque échouera à atteindre les objectifs visés. Une stratégie de prévention de ce type devrait ainsi amener les dirigeants ou les responsables à renoncer à mener un acte cyber terroriste. Si la menace crédible d'une réponse ou d'un recours à la force militaire est indispensable à l'efficacité de la dissuasion, il existe d'autres moyens de prévention à prendre en compte dans l'élaboration d'une stratégie adaptée. Ces moyens incluent notamment les mesures non militaires qui contribuent à décourager un adversaire potentiel de mener un acte cyber terroriste. Une stratégie de prévention globale doit donc comprendre des approches aussi bien militaires que non militaires qui intègrent et hiérarchisent les activités. Une telle stratégie repose sur une approche holistique de lutte contre la menace que représente le cyber terrorisme. Ces activités militaires et non militaires associées au service de l'objectif de prévention peuvent être regroupées sous les catégories *rétribution* et *dissuasion*.

Rétribution

Comme évoqué précédemment, et malgré ses effets limités sur la prise de décision de certains dirigeants, la rétribution demeure un concept pertinent pour décourager le cyber terrorisme. On considère que de nombreuses organisations terroristes, dont Al-Qaïda et l'État islamique, ont un raisonnement stratégique et rationnel[62]. C'est pourquoi la rétribution demeure une considération pertinente. Aucune disposition du DCA n'interdit explicitement de répondre par une intervention militaire à un acte cyber terroriste, même quand il n'est pas parrainé par un état. Si les principes de nécessité militaire et de ciblage licite sont dûment respectés, les réponses aussi bien militaires que non militaires sont des options viables.

Par des opérations antiterroristes persistantes et agressives visant à repérer les organisations terroristes les plus militantes, les États-Unis peuvent augmenter chez leurs adversaires potentiels la perception d'une menace crédible de représailles et de conséquences inacceptables, en cas d'attaque contre les États-Unis.

La conviction qu'à la suite d'un acte cyber terroriste les États-Unis se retourneraient systématiquement contre eux par des moyens militaires et non militaires et menaceraient leur survie et la base de leur autorité pourrait dissuader les dirigeants d'Al-Qaïda ou de l'État islamique de mener une cyber attaque mortelle.

En ce qui concerne le terrorisme d'état, le fait de savoir que les États-Unis ont la possibilité de répondre « de manière appropriée » à une cyber attaque peut augmenter la probabilité de dissuader les états impliqués dans le cyber terrorisme. Par conséquent, si un état hostile permet à des terroristes de perpétrer des cyber attaques contre les États-Unis ou leurs intérêts, la réponse américaine peut comprendre des mesures aussi bien d'ordre cybernétique que non cybernétique. Si les problèmes inhérents au choix d'un objectif militaire approprié ont été mentionnés précédemment dans le cas d'un acte de terrorisme non parrainé par un état, ils sont atténués dans un scénario impliquant un état qui appuie ou facilite le terrorisme, car les frontières géographiques claires permettent de prendre des précautions raisonnables afin d'éviter autant que possible les dommages collatéraux et les blessures accidentelles.

Dissuasion

Outre la rétribution, la stratégie holistique intègre également la dissuasion qui vise à influencer les dirigeants de potentiels adversaires en décourageant l'instauration d'une concurrence militaire[63]. Pour être efficaces, ces efforts de dissuasion doivent intervenir avant que la menace ne se manifeste. Ils incluent des « mesures formatrices », qui sont habituellement de nature non militaire et généralement conduites en temps de paix[64]. Selon le dictionnaire des services militaires américains, la dissuasion agit en dehors de la menace potentielle d'une action militaire. Une stratégie intégrant la dissuasion pour influencer des cyber adversaires potentiels insisterait sur la futilité des cyber attaques afin d'amener les dirigeants de cet adversaire potentiel à renoncer à une confrontation militaire[65]. Il convient de noter que certains stratèges sont d'avis que la rétribution ne serait pas nécessaire contre des ennemis convaincus grâce à la dissuasion de ne pas s'attaquer

aux États-Unis[66]. L'approche visant à dissuader les potentiels auteurs de cyber attaques doit reposer sur trois aspects : la résilience, la criminalistique et l'interception monétaire.

Les efforts de résilience, notamment concernant la redondance du matériel réseau et de la connectivité Internet, promettent d'améliorer considérablement la situation à l'issue d'une cyber attaque généralisée et potentiellement dévastatrice. Les vastes préparatifs qui améliorent la cyber résilience et permettent d'atténuer et de gérer les conséquences d'un acte cyber terroriste peuvent amener les dirigeants d'un adversaire à considérer qu'une cyber attaque n'aura pas les effets destructeurs escomptés. Ils pourront, par conséquent, s'abstenir de mener une telle attaque, ou décider d'opter pour une autre forme de destruction, comme les attaques cinétiques conventionnelles.

Le deuxième aspect de la dissuasion consiste à disposer d'une capacité de cyber criminalistique fiable et réactive. Telle que définie ici, la cyber criminalistique est la science qui permet d'analyser et d'identifier la source et le cheminement d'une cyber attaque dans le but de faire respecter la loi ou à des fins de contre-espionnage militaire. À l'issue d'un acte cyber terroriste, les services criminalistiques tenteront d'utiliser toutes les « empreintes électroniques » possibles et autres informations réseaux ou logicielles pour faciliter l'attribution de la source et identifier les responsables de l'attaque. Il faut reconnaître que l'identification et l'attribution peuvent être difficiles, car les attaquants peuvent utiliser des ordinateurs intermédiaires ou canaliser leur attaque via des proxies anonymes qui dissimulent leur adresse IP (Internet Protocol)[67]. Néanmoins, une capacité solide et connue du public permettant d'identifier et d'attribuer la source de la cyber attaque pourrait dissuader les cyber terroristes potentiels ou ceux qui soutiennent leurs efforts. L'identification et l'attribution d'une cyber attaque peuvent conduire à des poursuites devant les tribunaux civils ou, dans le cas d'agressions plus importantes, à un ciblage avec des armes cinétiques ou non.

Le dernier aspect de la dissuasion implique des efforts agressifs visant à intercepter et à minimiser les flux de financement utilisés par les personnes impliquées dans le cyber terrorisme. Ces mesures d'interception peuvent également être considérées comme des contre-menaces financières et des sanctions[68]. Le financement est incontestablement essentiel aux activités de nombreuses organisations terroristes, y compris celles des acteurs non étatiques. Par le passé, ce type de financement provenait d'associations caritatives, d'activités illégales et de sociétés-écrans. Les constants efforts d'interdiction fiscale internationaux pourraient réduire considérablement le financement disponible pour les organisations les plus enclines au cyber terrorisme.

Les mesures actuellement mises en place par le département d'État américain pour lutter contre et sanctionner ce financement visent les transactions financières qui profitent aux organisations terroristes, qu'elles proviennent d'états, d'organisations non gouvernementales ou de sociétés privées[69]. Un effort soutenu pour éliminer ou minimiser les sources de financement utilisées par les organisations terroristes pourrait contribuer à freiner les ralliements à leur cause. Associées à la résilience cybernétique et aux efforts de la criminalistique, ces mesures peuvent inciter les dirigeants d'une organisation terroriste à renoncer à toute confrontation directe par le cyber terrorisme.

Conclusion

Quand une stratégie globale de prévention associe la rétribution et la dissuasion, la probabilité de décourager les dirigeants d'un adversaire potentiel de perpétrer des actes cyber terroristes est plus élevée. L'histoire a cependant montré que la rétribution échoue parfois en raison d'erreurs de calcul, d'incertitudes ou du hasard. Ce risque peut également s'appliquer à la rétribution des actes cyber terroristes. En cas d'échec de la rétribution, la mise en place de mesures visant à gérer les conséquences d'une cyber attaque généralisée et destructrice pourrait réduire ou limiter les dommages. Une stratégie combinant la rétribution et la dissuasion a également pour avantage de décourager un éventail plus vaste d'adversaires étatiques potentiels de mener des cyber attaques relativement « routinières » ou banales contre les États-Unis ou leurs intérêts, car il apparaît peu probable que les effets souhaités puissent être atteints ou qu'il vaille la peine de lancer une telle attaque. Paradoxalement peut-être, on a constaté que le succès de « la 'guerre contre le terrorisme' risquait fort d'inciter les terroristes à se tourner de plus en plus vers des armes non conventionnelles telles que le cyber terrorisme[70] ». Bien que certains experts en matière de terrorisme en concluent que, pour le moment tout au moins, les camions piégés, le financement et le recrutement de terroristes semblent constituer une menace plus grave que le cyber terrorisme, on ne peut ignorer la menace potentielle qu'il représente.

Si un acte cyber terroriste peut sembler peu probable, un attentat comme celui du 11 septembre l'était tout autant avant qu'il ne se produise. Nombre de citoyens et responsables politiques américains regrettent que les capacités et les stratégies antiterroristes n'aient pas été améliorées avant les attentats du 11 septembre, d'autant plus que bon nombre de ces améliorations nécessaires se sont révélées évidentes par la suite. De la même manière, il est désormais temps d'agir pour mettre en œuvre une stratégie de rétribution et de dissuasion solide et globale contre le cyber terrorisme, sans attendre qu'un attentat de ce type ne se produise.

Notes

1. Office of the Press Secretary, *Fact Sheet: Administration Cybersecurity Efforts 2015*, Washington, D.C. : The White House, 9 juillet 2015 www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administrationcybersecurity-efforts-2015.

2. Président Barack Obama (remarques, *Cybersecurity and Consumer Protection Summit*, Stanford University, 13 février 2015), www.whitehouse.gov/the-press-office/2015/02/13/remarks-presidentcybersecurity-and-consumer-protection-summit.

3. KENNEY, Michael, « Cyber-Terrorism in a Post-Stuxnet World », *Orbis* 59, no 1, 2015, pp. 111-128, www.sciencedirect.com/science/article/pii/S0030438714000787.

4. LEWIS, Jim, « The Role of Deterrence », (discours, Space Security Symposium, Stimson Center, 15 novembre 2012), www.stimson.org/about/news/jimlewis-of-csis-speaks-at-stimson-on-cyber-deterrence/.

5. GRAY, Colin S., *National Security Dilemmas: Challenges & Opportunities,* Dulles, VA : Potomac Books, Inc., 2009, p. 62.

6. KREPINEVICH, Andrew F., *Cyber Warfare: A 'Nuclear Option'?* Washington, DC : Center for Strategic and Budgetary Assessments, 2012, p. 8, http://csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/.

7. KLEIN, John J., « Some Principles of Cyber Strategy », *ISN Security Watch*, 21 août 2014, www.isn .ethz.ch/DigitalLibrary/Articles/Detail/?id=182955.

8. SANGER, David E., BARBOZA, David et PERLROTH, Nicole, « Chinese Army Unit Is Seen as Tied to Hacking Against U.S. », *NYTimes.com*, www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-tohacking-against-us.html?pagewanted=all&_r=0.

9. DENNING, Dorothy, « Cyberterrorism », témoignage devant le Comité de surveillance du terrorisme, Commission des forces armées, Chambre des représentants des États-Unis, 23 mai 2000, www.stealthiss.com /documents/pdf/cyberterrorism.pdf.

10. DENNING, Dorothy, « Is Cyber Terror Next? » in *Understanding September*, éds. CALHOUN, Craig, PRICE, Paul, et TIMMER, Ashley, New York : The New Press, 2002.

11. WEIMANN, Gabriel, *Cyberterrorism: How Real Is the Threat?* Washington, D.C. : United States Institute of Peace, décembre 2004, p. 4, www.usip.org/sites/default/files/sr119.pdf.

12. *Id.*

13. *Id.*, p. 5.

14. *Id.*

15. *Id.*

16. WILSON, Clay, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report RJ32114, Washington, D.C. : Bibliothèque du Congrès, Service de recherche du Congrès, 17 octobre 2003, pp. 12-13.

17. STOUFFER, Keith, FALCO, Joe et KENT, Karen, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security,* Washington, D.C. : ministère du Commerce des États-Unis, 2006, pp. 2-1. www.dhs.gov/sites/default/files/publications/csd-nistguidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf.

18. WEIMANN, *Cyberterrorism*, p. 6.

19. *Id.*, p. 7.

20. « State Sponsors of Terrorism », département d'État, 2015, www.state.gov/j/ct/list/c14151.htm.

21. PAYNE, Keith B., *How Much is Enough?: A Goal-Driven Approach to Defining Key Principles*, Fairfax, VA : National Institute for Public Policy, 2009, p. 5.

22. Bureau du président, *The National Security Strategy of the United States*, Washington, D.C. : White House, mai 2002, p. 15, www.state.gov/documents/organization/63562.pdf.

23. GRAY, *National Security Dilemmas*, p. 72.

24. WEIMANN, *Cyberterrorism*, p. 6.

25. En revanche, certains experts affirment que les cyber attaques sophistiquées exigeraient des moyens plus importants et une expertise plus vaste. Voir CHEN, Thomas M., *Cyberterrorism after Stutxnet*, Carlisle Barracks, PA : United States Army War College Press, juin 2014, pp. 22-23, www.strategicstudiesinstitute. army.mil/pdffiles/PUB1211.pdf.

26. *Id.*, p. 10.

27. WEIMANN, *Cyberterrorism*, p. 6.

28. CHEN, *Cyberterrorism after Stuxnet*, p. 20.

29. *Id.*

30. RICHARDS, Jason, « Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security », *International Affairs Review*, www.iar-gwu.org/node/65.

31. HOLDEN, Dan, « Is Cyber-Terrorism the New Normal », *Wired*, www.wired.com/insights/2015/01 /is-cyber-terrorism-the-new-normal/.

32. WEIMANN, *Cyberterrorism*, p. 8.

33. CLAY, *Computer Attack and Cyber Terrorism*, p. 12.

34. WEIMANN, *Cyberterrorism*, p. 8.

35. GREEN, Joshua, « The Myth of Cyberterrorism », *Washington Monthly*, novembre 2002, www.washingtonmonthly.com/features/2001/0211.green.html.

36. KENNEY, « Cyber-Terrorism in a Post-Stuxnet World ».

37. CHEN, *Cyberterrorism after Stuxnet*, p. 13.
38. SCHELLING, Thomas, *The Strategy of Conflict*, Cambridge, MA : Harvard University Press, 1960, p. 9.
39. GRAY, *National Security Dilemmas*, p. 56.
40. U.S. Joint Chiefs of Staff, Joint Publication 1–02, *Dictionary of Military and Associated Terms*, Washington, DC : Department of Defense, 8 novembre 2010, p. 214, http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf.
41. U.S. Department of the Navy, NWP 1–14M, *The Commander's Handbook on the Law of Naval Operations*, Washington, DC : Department of the Navy, juillet 2007, pp. 6–5, www.lawofwar.org/naval_warfare_publication_N-114M.htm.
42. *Id.*
43. *Id.* Ce concept est également appelé principe de proportionnalité.
44. *Id.*, pp. 8-1.
45. *Id.*
46. Cette définition est tirée du contexte de la dissuasion nucléaire élargie. Voir Department of Defense, *Nuclear Posture Review Report*, Washington, D.C. : Department of Defense, avril 2010.
47. « U.S. Military Symposium Will Mull Role of 'Extended Deterrence' In Cyberspace », *Inside Defense*, 27 juillet 2015.
48. *Id.*
49. Article 51, *Charte des Nations Unies et Statut de la Cour internationale de justice*, San Francisco, CA : Nations Unies, 1945, https://treaties.un.org/doc/publication/ctc/uncharter.pdf.
50. U.S. Department of the Navy, NWP 1–14M, para 8.1.1.
51. *Id.*
52. *Id.*, para. 8.1.2.1.
53. Executive Office of the President, *The Strategy to Secure Cyberspace*, Washington, D.C. : White House, 2003, p. 50, www.uscert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
54. CLAY, *Computer Attack and Cyber Terrorism*, pp. 18-19.
55. DANIEL, Michael, « Our Latest Tool to Combat Cyber Attacks: What You Need to Know », *The White House* (blogue), 1er avril 2015, www.whitehouse.gov/blog/2015/04/01/our-latest-tool-combat-cyber-attackswhat-you-need-know.
56. Stimson Center, « Jim Lewis of CSIS Speaks at Stimson on Cyber Deterrence », *Stimson.org*, 15 novembre 2012, www.stimson.org/about/news/jim-lewis-of-csis-speaks-at-stimson-on-cyberdeterrence/.
57. *Id.*
58. *Id.*
59. CLAY, *Computer Attack and Cyber Terrorism*, p. 19.
60. Comité international de la Croix-Rouge, « The Relevance of IHL in the Context of Terrorism », Genève, Suisse : CICR, 1er janvier 2011.
61. U.S. Department of the Navy, NWP 1–14M, para. 12.7.1.
62. GRAY, *National Security Dilemmas*, p. 72.
63. Department of Defense, *Annual Report to the President and the Congress* , Washington, D.C. : Department of Defense, 2002, p. 18.
64. Chairman, Joint Chiefs of Staff, *Combating Weapons of Mass Destruction*, JP 3–40, Washington, D.C. : Department of Defense, 10 juin 2009, x.
65. *Id.*, I–3.
66. GRAY, *National Security Dilemmas*, p. 59 ; DENNING, « *Cyberterrorism* ».
67. CHEN, *Cyberterrorism after Stuxnet*, p. 4.
68. « Counter Threat Finance and Sanctions », département d'État, www.state.gov/e/eb/tfs/.
69. *Id.*
70. WEIMANN, *Cyberterrorism*, p. 11.