Sous la direction de
Francis Fortin

Cybercriminalité

Entre inconduite et crime organisé

PRESSES
INTERNATIONALES
POLYTECHNIQUE

Cybercriminalité – Entre inconduite et crime organisé
Francis Fortin (Sous la direction de)

Cet ouvrage a été réalisé à l'initiative de la Sûreté du Québec

Avis : Les renseignements fournis dans le présent ouvrage sont de nature générale. Malgré les efforts qu'ils ont faits dans ce sens, les auteurs ne peuvent garantir que ces informations sont exactes et à jour. Ces renseignements ne peuvent en aucune façon être interprétés comme des conseils juridiques. Toute personne ayant besoin de conseils juridiques pour un cas particulier devrait consulter un avocat.

Coordination éditoriale : Luce Venne-Forcione,
Révision et correction d'épreuves : Nicole Blanchette
Mise en pages : Danielle Motard
Couverture : Cyclone Design

Pour connaître nos distributeurs et nos points de vente, veuillez consulter notre site Web à l'adresse suivante : www.pressespoly.ca

Courriel des Presses internationales Polytechnique : pip@polymtl.ca

Nous reconnaissons l'aide financière du gouvernement du Canada par l'entremise du Fonds du livre du Canada pour nos activités d'édition.

Gouvernement du Québec – Programme de crédit d'impôt pour l'édition de livres – Gestion SODEC.

Tous droits réservés
© Presses internationales Polytechnique et Sûreté du Québec, 2013

On ne peut reproduire ni diffuser aucune partie du présent ouvrage, sous quelque forme ou par quelque procédé que ce soit, sans avoir obtenu au préalable l'autorisation de l'éditeur.

Dépôt légal : 1er trimestre 2013
Bibliothèque et Archives nationales du Québec
Bibliothèque et Archives Canada

ISBN 978-2-553-01647-9
Imprimé au Canada

Chapitre

14

Comprendre le cyberterrorisme : du concept à la réalité

Benoit Gagnon[1]

Le cyberterrorisme est un sujet hautement à la mode depuis le début des années 2000, et les événements du 11 septembre 2001 ont eu pour effet d'accroître l'intérêt qu'on lui porte. Bon nombre de livres et d'articles scientifiques – ou pseudo-scientifiques – traitent de ce thème. Par exemple, une recherche sur les moteurs de recherche d'articles scientifiques permet de découvrir un millier d'articles rédigés sur le sujet depuis 2010[2]. C'est d'autant plus surprenant, car il demeure encore difficile aujourd'hui de faire la part des choses quand de supposés actes de cyberterrorisme sont rapportés dans les médias.

En fait, selon la majorité des spécialistes traitant du sujet, le cyberterrorisme fait partie des menaces qui sont souvent considérées comme émergentes. Toutefois, son caractère mal défini et encore relativement obscur, voire opaque, fait du cyberterrorisme une menace beaucoup plus flottante que tangible. Selon bon nombre de spécialistes, tôt ou tard, les terroristes vont finir par se tourner vers les technologies de l'information pour lancer des cyberattaques contre les sociétés, et ce,

1. Doctorant à l'École de criminologie de l'Université de Montréal.
2. Une recherche effectuée en février 2012 sur Google Scholar (scholar.google.com) a permis de recenser plus de 1 080 articles sur le sujet.

parce que les dégâts pouvant être engendrés sur les infrastructures clés, comme celles du secteur de l'énergie ou du système financier, sont potentiellement critiques (Denning, 2001, p. 27). Cependant, il serait encore très difficile de connaître le niveau d'adoption de ces méthodes et, surtout, de classer les cyberattaques comme des actes de terrorisme.

Ce chapitre a essentiellement trois objectifs. Tout d'abord, il donne un aperçu des éléments à considérer pour comprendre le cyberterrorisme. Ensuite, il fournit certaines balises permettant de voir où se situent les limites de cette notion. Enfin, il propose des pistes de réflexion sur la portée réelle du phénomène et ainsi amène le lecteur à réfléchir au concept de cyberterrorisme. En cours de route, nous verrons l'état de la législation et des statistiques, nous présenterons un cas pratique afin de décrire le phénomène et nous examinerons les tendances en matière de cyberterrorisme.

14.1 Problématique et aperçu du phénomène

Qu'est-ce que le cyberterrorisme exactement? Le cyberterrorisme est probablement la forme de terrorisme qui est la moins bien comprise. En effet, trop souvent, ce phénomène fait l'objet d'analyses de la part de personnes qui n'ont pas nécessairement les bases nécessaires à la compréhension du sujet (voir notamment Denning, dans Arquilla et Ronfeldt, 2001, p. 239-288).

Si les tentatives de définition du cyberterrorisme sont nombreuses, elles se heurtent fréquemment à de grands obstacles. Il est possible de déceler trois facteurs majeurs qui nuisent à la création d'une définition claire du cyberterrorisme :

1. La définition de ce qu'est le terrorisme ne fait pas encore l'unanimité chez les spécialistes.
2. Le cyberterrorisme est un phénomène encore très récent.
3. Il s'agit d'un concept difficile à comprendre, car il exploite des notions oscillant entre la science politique, la criminologie, la sociologie, la philosophie, la théologie, l'informatique et même la science-fiction.

Pour ces raisons, certains spécialistes, comme Abraham D. Soafer et Seymour E. Goodman (2001), affirment que le cyberterrorisme est une problématique qui demande une vision à la fois transnationale et transdisciplinaire.

Ces problèmes de conceptualisation ont pour effet d'engendrer des définitions manquant de rigueur. Notons par exemple celle de Matthew J. Littleton (1995), qui affirme : « Le terme de cyberterrorisme réfère à l'utilisation de tactiques et de techniques issues de la guerre de l'information par des organisations terroristes, et ce, dans le but d'influencer le cyberespace. » Certains auteurs, comme ce dernier, introduisent le concept de guerre de l'information dans le champ du terrorisme. Or, quand on jette un rapide coup d'œil sur ce qu'est la guerre de l'information (*information warfare*), on se rend compte qu'il s'agit d'un concept fourre-tout comprenant des éléments aussi divers que la guerre psychologique, la désinformation, la propagande, la guerre électronique ou la guerre informatique. Si ces concepts sont intéressants au plan de la réflexion spéculative, ils demeurent encore on ne peut plus flous et évoluent surtout dans le champ théorique, sans nécessairement avoir des assises empiriques solides.

Même si ce genre de définitions imprécises foisonne, il est toutefois possible de trouver des définitions qui ont plus de portée et qui peuvent être mieux opérationnalisées. Celle qui sera utilisée dans ce chapitre provient des travaux effectués par Pollit (1997, p. 3), qui en vient à voir le cyberterrorisme comme « une attaque préméditée et politiquement motivée contre l'information, les systèmes informatiques, les logiciels et les données résultant ainsi en une violence contre des cibles non combattantes ».

Il est néanmoins nécessaire de faire une différence entre le technoterrorisme et le cyberterrorisme (Littleton, 1995). Le technoterrorisme impliquerait qu'un terroriste vise un système d'information en faisant du sabotage électronique ou physique pour conséquemment détruire ou déstabiliser ledit système d'information ou une infrastructure qui en dépendrait. Le cyberterrorisme, quant à lui, consisterait à manipuler et à exploiter des systèmes d'information en altérant des données, en volant des données ou en forçant un système à opérer de manière imprévue (Pollit, 1997).

En d'autres termes, le technoterrorisme serait donc une forme de terrorisme qui vise les infrastructures d'information de manière physique. Il s'agirait, par exemple, de détruire un système informatique avec une bombe. De son côté, le cyberterrorisme viserait à frapper les infrastructures de manière virtuelle à des fins de destruction, de contrôle ou de vol de données.

Il est aussi important de souligner que le terme « cyberterrorisme » est peut-être plus une forme de « terme marketing » qu'autre chose. En effet, si l'on jette un coup d'œil sur l'histoire du terrorisme, il est possible de distinguer des formes de terrorismes qui étaient bien spécifiques.

Prenons par exemple le cas de Theodore Kaczynski (FBI, 2008), mieux connu sous le nom de Unabomber. Kaczynski agissait complètement seul et avait pour habitude d'envoyer des colis postaux piégés. Au total, il a commis plus d'une quinzaine d'attentats étalés sur les années 1970, 1980 et 1990. Or, en analysant les actes de Kaczynski, personne n'a jamais parlé de terrorisme postal : il s'agissait tout simplement d'actes terroristes.

Quand on parle de terrorisme, l'outil, l'instrument servant à perpétrer l'acte ne sert habituellement pas à qualifier le geste. Donc, parler de cyberterrorisme est un mauvais emploi du préfixe « cyber ». Il s'agit encore de terrorisme, mais il est commis avec des outils issus des technologies de l'information et des communications (TIC).

Dans la réalité, il faut constater que ces définitions reflètent difficilement ce qui se produit dans le réel. Prenons par exemple le cas d'Anonymous. Si le groupe de pirates se défend bien de faire dans le cyberterrorisme, de plus en plus de gouvernements, notamment le gouvernement des États-Unis (U.S. Department of Homeland Security, 2011), le voient comme un vecteur d'actes de cyberterrorisme. On ne peut s'empêcher de noter une forme d'instrumentalisation de la définition, puisque, pour l'heure, il demeure encore impossible de prouver qu'Anonymous est un vecteur de violence contre des civils.

Ainsi, il serait probablement plus juste de catégoriser ce regroupement comme des « hacktivistes », soit des activistes exploitant des outils technologiques, notamment des outils permettant le piratage de systèmes informatiques divers, pour alimenter leur cause. Dire qu'Anonymous cherche à engendrer la terreur dans le cœur de la population est, au

moment d'écrire ces lignes, une lubie. Il est en effet encore difficile de croire que le fait de révéler des documents compromettants sur certains individus ou sur des organisations puisse être considéré comme un acte de violence servant à engendrer la peur chez une population. En fait, il est même possible de voir une forme de soutien moral offert par la population envers les actions d'Anonymous. Le cyberterrorisme est plus spécifiquement consacré à la cause, celle principalement de la religion ou de l'idéologie religieuse, et va très souvent à l'encontre des croyances de la population en général.

14.2 Avantages du cyberterrorisme

La question souvent soulevée par les gens s'intéressant au cyberterrorisme est la suivante : pourquoi les terroristes voudraient-ils se tourner vers des attaques cybernétiques? L'interrogation est pertinente. Assurément, les effets physiques sont habituellement ce que les terroristes recherchent; ils veulent impressionner, frapper l'inconscient collectif avec des images fortes, des morts et des dégâts (Norris, Kern et Just, 2003). Dans cette optique, les attaques cybernétiques ne seraient peut-être pas appropriées pour permettre aux terroristes d'atteindre leurs objectifs.

En fait, il faut comprendre que le cyberterrorisme comporte, dans l'imaginaire des analystes en cybersécurité, des avantages qui ne cadrent pas nécessairement avec le terrorisme classique. Il faut conceptualiser la dynamique du cyberterrorisme dans un cadre qui est encore spéculatif, voire futurologique, mais qui demeure tout de même plausible sur le plan argumentaire. En usant de cette approche, il est possible de déceler bon nombre de raisons pour lesquelles des terroristes voudraient se tourner vers des attaques cybernétiques. Ainsi, sept avantages s'offriraient aux terroristes qui voudraient se saisir du potentiel des TIC pour faire des actes de cyberterrorisme. Soulignons qu'heureusement, comme nous le verrons un peu plus loin, nul terroriste n'a encore pu bénéficier de ces avantages.

Premièrement, le cyberterrorisme utiliserait des moyens limités, réduits et disponibles. En d'autres termes, il serait on ne peut plus facile pour les terroristes de se doter des outils requis pour faire du cyberterrorisme : les ordinateurs sont légaux, et l'écriture de logiciels et de scripts est

relativement facile à faire. De plus, les ordinateurs sont de moins en moins dispendieux, de plus en plus puissants et l'accès au réseau informatique mondial est, somme toute, aisé.

À cela s'ajoute le fait que les méthodes permettant de commettre des cyberattaques se retrouvent sur Internet, offrant ainsi l'avantage aux terroristes de pouvoir devenir autodidactes et donc de limiter leurs mouvements. Les terroristes « classiques » doivent souvent se rendre dans des camps d'entraînement afin de suivre une formation concernant l'utilisation d'armes et d'explosifs. Ces déplacements et les transactions effectuées avec des membres du monde interlope rendent les terroristes plus faciles à détecter par les agences d'application de la loi.

Or, avec le cyberterrorisme, la situation ne serait plus la même. Grâce à Internet, qui est une source inépuisable d'informations sur le piratage informatique, les cyberterroristes pourraient apprendre par eux-mêmes à faire des cyberattaques tout en demeurant dans leur foyer. Il est donc possible de spéculer que, dans les années à venir, on risque d'assister à une montée des cyberterroristes agissant seuls; des cyberterroristes à la sauce « Unabomber », en somme.

Deuxièmement, les attaques cybernétiques seraient faciles à commettre, et certaines de ces attaques pourraient être grandement dommageables. En fait, l'histoire est remplie d'attaques informatiques qui auraient pu avoir de graves répercussions, mais qui se sont effectuées avec une facilité déconcertante. Pensons simplement au cas du barrage Roosevelt qui, en 1998, a été piraté par un enfant de 12 ans. Ce dernier était rendu tellement loin dans le système qu'il aurait pu ouvrir les valves et inonder les villes voisines de Mesa et de Tempe (Borger, 2002). Évidemment, ce n'est pas un acte de cyberterrorisme en soi. Par contre, ce que cela démontre, c'est la facilité avec laquelle un individu motivé peut infiltrer des systèmes importants. Or, ce type de cas n'est pas isolé (Chirillo, 2001). Des centaines de cas de ce genre ont été répertoriés partout dans le monde, frôlant quelquefois la catastrophe (Soafer et Goodman, 2001, p. 14).

Troisièmement, le cyberterrorisme aurait l'avantage de donner une sécurité et une pérennité aux terroristes, et ce, même après la perpétration de l'attentat. En effet, contrairement au terrorisme classique, ce type d'attaque n'a pas besoin d'actions éclatantes pour être efficace. C'est plutôt l'élément de surprise qui serait une des forces principales du cyberterrorisme (Dunnigan, 2002, p. 5). Dans cette optique, quand

elles sont bien menées, les cyberattaques demeurent furtives et ne se font pas détecter. Les cyberterroristes peuvent donc rester dans l'ombre et mettre sur pied des attaques subséquentes de manière répétitive, tout en demeurant à l'abri des contre-mesures.

Quatrièmement, les cyberattaques profitent du fait qu'Internet réduit l'espace et le temps. Les cyberattaques peuvent provenir de différents endroits en même temps, peuvent être diffusées à travers le globe et exploitent le fait qu'elles peuvent passer d'un pays à l'autre avant de se concrétiser. Elles peuvent également se faire de façon retardée, ce qui permet aux terroristes de changer d'endroit avant que l'attaque se concrétise. De ce point de vue, le cyberterrorisme devrait être considéré comme la façon la plus avancée de commettre du terrorisme international (Miyawaki, 2001, p. 9).

Cinquièmement, les cyberattaques ne demandent pas d'actions suicides; les membres peuvent perpétrer leur attentat sans avoir à se sacrifier pour la cause. Cela a donc pour résultat qu'un réseau terroriste peut continuer à bénéficier de l'expertise de ses membres pendant une longue période de temps. Néanmoins, il est éventuellement possible de faire face à des cyberattentats suicides. Dans le cas d'une attaque informatique, l'instigateur de l'attaque tente habituellement de laisser le moins de traces possible pour ne pas se faire retracer par les autorités en matière de sécurité. Or, pour ce faire, l'attaquant doit généralement limiter les dégâts qu'il peut engendrer sur les systèmes informatiques visés – il y a donc présence d'un ratio « discrétion de l'attaque » sur « dégâts potentiels ». On peut donc facilement s'imaginer que certains individus voudront maximiser l'ampleur des dégâts engendrés par les cyberattaques, en ne prenant pas en considération le facteur de discrétion de l'attaque. Ce mode de fonctionnement les mettra en danger et fournira les indices nécessaires aux responsables de la sécurité pour arrêter ces individus. Cela constituera, en somme, un attentat « suicide » au sens où l'individu aura sacrifié la sûreté de sa propre personne pour perpétrer la cyberattaque.

Sixièmement, le cyberterrorisme offre des avantages liés à son efficacité. Comme le mentionne Dorothy E. Denning (2001), le cyberterrorisme devient de plus en plus intéressant alors que le monde virtuel et le monde réel deviennent interconnectés. En effet, le cyberterrorisme offre la possibilité d'attaquer des points névralgiques des réseaux informatiques, avec des conséquences importantes dans le monde réel.

Cela fait directement référence au concept d'armes de perturbation massive (APM) avancé par Thomas Homer-Dixon au lendemain des attentats du 11 septembre 2001 (Homer-Dixon, 2002). Dans son esprit, les terroristes ne cherchent pas tant à causer de la destruction qu'à déstabiliser les sociétés. Pour y arriver, ils chercheraient de plus en plus à viser les infrastructures critiques (centres financiers, centres politiques, hôpitaux, infrastructures énergétiques, réseaux de distribution alimentaire, etc.) en détournant le sens social donné à des objets du quotidien[3] afin de les transformer en armes. Le 11 septembre 2001 est l'archétype de ce genre d'attentat : viser des tours symboliques qui sont également des centres financiers, en utilisant des avions civils, soit des engins qui ne sont de prime abord pas destinés à des actes violents.

De plus, les cyberattaques représenteraient des armes asymétriques potentiellement très performantes. En théorie, les attaques informatiques pourraient mettre hors de combat une armée qui fonde sa doctrine sur des moyens de haute technologie (O'Hanlon, 2000). Or, cela pourrait s'avérer une arme de choix pour ceux qui manifestent leur désaccord avec la puissance américaine, cette dernière basant une grande partie de sa force militaire sur les TIC.

Septièmement, dans les années à venir, les terroristes pourraient voir d'un bon œil la mise sur pied de combinaisons d'attaques physiques traditionnelles et d'attaques cybernétiques. Sans pour autant entrer dans une vision apocalyptique du cyberterrorisme, où les sociétés deviennent complètement paralysées après des assauts combinés, il est effectivement possible d'anticiper ce genre d'attaques. Si l'on se souvient, une des grandes critiques qui avait été portée aux services d'urgence pour la gestion de l'attentat terroriste du 11 septembre 2001 concernait les difficultés communicationnelles (The National Commission on Terrorist Attacks Upon the United States, 2004, p. 566-568). Or, on peut prédire que des attaques savamment orchestrées pourraient viser la destruction physique par l'intermédiaire d'attentats traditionnels tout en nuisant aux systèmes de communication des services d'urgence au moyen de cyberattaques.

3. Par exemple, avant le 11 septembre 2001, peu de gens voyaient les avions commerciaux comme de véritables bombes volantes. Les événements du 11 septembre 2001 ont donc transformé l'interprétation que l'on a de « l'objet » et plusieurs voient désormais les avions de ligne comme des armes ambulantes. Voir à ce sujet Homer-Dixon (2002).

14.3 Législation : quelles sont les dispositions de la loi?

Il faut bien comprendre qu'au Canada, les actes de cyberterrorisme ne sont pas strictement visés par le cadre juridique. Dans les faits, soit les actes tombent sous les articles touchant à la criminalité informatique (notamment l'article 342 du Code criminel canadien), soit ils touchent à la question du terrorisme (notamment l'article 83 du Code criminel canadien).

Un cas récent démontre de manière assez explicite comment les tribunaux risquent de traiter les dossiers de terrorisme ayant un volet touchant aux TIC : le dossier Saïd Namouh, accusé d'avoir fomenté un complot terroriste à Trois-Rivières en 2007 (Cour du Québec, 2009). Monsieur Namouh avait notamment entretenu un grand nombre d'activités en ligne dans son complot terroriste, entre autres en diffusant des vidéos propagandistes et en distribuant d'autres informations du genre. C'est ainsi qu'on a pu invoquer dans le jugement les articles du Code criminel concernant le fait de faciliter une activité terroriste. Rien ne touchait à la question de la criminalité informatique en tant que telle.

Bref, même si des experts du cyberterrorisme sont venus témoigner en cour, rien ne démontre que Saïd Namouh a été actif dans les attaques informatiques. Ses actions ont été considérées essentiellement sous l'angle de la logistique terroriste et du complot dans le but de commettre un attentat. En d'autres mots, rien ne permet d'établir une jurisprudence solide en matière de « cyberterrorisme ».

14.4 Statistiques

Les statistiques touchant précisément au cyberterrorisme sont, pour ainsi dire, inexistantes. En fait, cela découle d'une problématique fondamentale de la recherche entourant le terrorisme : l'accès aux données est difficile. Le peu de statistiques disponibles sur le phénomène est fédéré au travers de bases de données payantes – celle de Mickolus ou celle de la RAND Corporation, par exemple. Les données ouvertes sont disponibles dans la Global Terrorism Database (GTD) [2011].

La base de données GTD contient un total de 98 000 incidents terroristes, soit une moyenne de 2 450 par année – il est à noter que le terme

« incident » n'est pas dénué de sens, car tous les éléments colligés ne sont pas automatiquement des attentats. Mentionnons dès le départ que cette base de données ne contient aucune donnée sur le phénomène du cyberterrorisme au sens strict.

De fait, un aperçu rapide des statistiques descriptives du terrorisme ramène vite à la réalité : le terrorisme est, dans les faits, un phénomène grandement isolé. Considérant que le terrorisme est un acte de criminalité politique, et que la criminalité est un élément social déjà marginal, nous sommes donc en présence d'une exception dans l'exception. Quant à lui, le cyberterrorisme est une autre exception dans le spectre terroriste.

Autre élément à considérer : la méthode terroriste est, la plupart du temps, grandement inefficace. Les statistiques offertes par la GTD indiquent que la vaste majorité des attentats terroristes n'engendrent aucun décès. De plus, seulement 1 % des attentats terroristes engendrant des décès vont générer 25 décès ou plus. Cette analyse est d'ailleurs confirmée par le spécialiste en sécurité Bruce Schneier (2007).

La question des cas de cyberterrorisme se caractérise donc par une manifestation si isolée qu'il n'existe à peu près aucune donnée fiable à son sujet. Bref, pour l'heure, il faut conclure que le cyberterrorisme n'existe pas, faute d'incidence empirique suffisante pour être considérée.

14.5 Cas pratiques : le Pearl Harbor cybernétique pour demain?

Plusieurs spécialistes, comme Michael A. Vatis (dans Howitt et Pangi, 2003, p. 219-249), soutiennent qu'il est fort probable que le cyberterrorisme devienne très présent dans les années à venir. L'argumentation de Vatis se fonde surtout sur des événements s'étant précédemment produits et qui, somme toute, soulèvent des questions sur les vulnérabilités des infrastructures cybernétiques critiques. Sans en faire une liste exhaustive, et sans non plus affirmer qu'ils sont annonciateurs d'actes de cyberterrorisme en devenir, il est possible d'en mentionner au moins deux qui font rapidement sourciller.

En 2000, un individu œuvrant dans une station de traitement des eaux usées en Australie se fait congédier. Frustré par la situation, il

retourne chez lui et pirate le système informatique de ladite station et finit par en prendre le contrôle à distance. Par la suite, il inverse le système de pompes, engendrant ainsi un déversement de plusieurs centaines de litres d'eaux usées dans les rues de Queensland. Le responsable de l'attaque a été condamné à deux ans de prison pour son action (Smith, 2001).

Plus récemment, il a été révélé que des infrastructures américaines responsables de la distribution de l'eau potable auraient été piratées par un hacker en provenance de Russie (BBC, 2011). Si, pour l'heure, les dégâts sont encore difficiles à jauger, il n'en demeure pas moins que ce genre d'annonce a surtout pour effet de soulever des questions. Or, sans nécessairement tomber dans une analyse paranoïaque, force est d'admettre que de poser des questions sur les conséquences de l'intégration tous azimuts des TIC dans les infrastructures critiques est tout de même sain.

Il faut aussi calmer les tenants de la thèse du Pearl Harbor informatique en soulignant que l'emploi des armes informatiques comporte des risques. Comme le souligne Dorothy E. Denning, les systèmes informatiques sont complexes et difficiles à manipuler de manière précise. Ainsi, il est plus facile de saisir le potentiel de dégât engendré par une attaque physique que par une attaque informatique. Le fait qu'Internet soit un réseau interrelié à bon nombre d'entités physiques et virtuelles peut provoquer des effets pervers lors d'éventuelles cyberattaques :

1. Les cyberattaques peuvent paralyser le réseau, rendant des cyberattaques subséquentes impossibles.
2. Les cyberattaques peuvent se retourner contre les intérêts des cyberguerriers. Par exemple, un virus informatique lancé dans les infrastructures informatiques d'un adversaire peut aisément se retrouver en quelques secondes dans des infrastructures informatiques « amies ».
3. Les attaques informatiques peuvent nuire au bon fonctionnement des TIC, notamment d'Internet. Or, comme nous l'avons mentionné au début de ce chapitre, les TIC représentent un instrument de choix pour l'organisation et la gestion des activités terroristes. Une cyberattaque d'envergure pourrait donc avoir pour effet de nuire au fonctionnement même des organisations terroristes qui basent une bonne partie de leurs activités logistiques autour des réseaux informatiques (Lewis, 2002).

Ainsi, si le cyberterrorisme peut paraître avantageux sur certains aspects, il demeure une arme à deux tranchants.

De plus, il y a gros à parier que, puisque ces attaques demandent une technicité importante, les terroristes préféreront utiliser des armes plus traditionnelles qui ont un impact psychologique beaucoup plus grand. Après tout, quand on regarde les conséquences du 11 septembre 2001, force est d'admettre que le détournement des avions s'est à la base effectué en utilisant de simples couteaux à lames rétractables.

14.6 Perspectives d'avenir

Si le concept de cyberterrorisme semble encore plutôt nébuleux, une situation grandement tributaire du fait que le terrorisme « classique » est lui-même encore mal compris, il est tout de même clair que les terroristes exploitent les TIC. C'est un secret de Polichinelle que les organisations terroristes utilisent les différents outils présents sur le Web pour s'aider dans leurs desseins. Après tout, ce qui est souvent omis dans la réflexion sur les terroristes, c'est que ces individus sont dans les mêmes sociétés que les citoyens « ordinaires »; ils ont donc accès aux mêmes types d'outils et aux mêmes évolutions technologiques que la majorité des gens.

14.6.1 Cyberterrorisme ou terrorisme exploitant les TIC?

Ainsi, les terroristes vont déployer toute une série d'outils technologiques qui vont les aider dans leur cause. Sans faire une description exhaustive de toutes les utilisations particulières que les terroristes peuvent faire d'Internet, il est tout de même possible d'en dresser une typologie simple se divisant essentiellement en cinq catégories : le soutien idéologique, le recrutement, le financement, l'apprentissage et la manipulation médiatique.

La première catégorie d'utilisation qu'il est possible d'identifier au regard des activités terroristes en ligne est en lien avec le soutien idéologique de l'organisation. Les définitions du terrorisme s'entendent généralement sur le fait que l'action terroriste est sous-tendue par une volonté sociopolitique quelconque (changement politique, changement social, revendication religieuse, etc.). Ainsi, l'activité de soutien idéologique

sert surtout à appuyer cette action, que ce soit par l'entremise d'activités de discussion en ligne ou par la diffusion de la pensée des dirigeants de l'organisation – les réflexions d'Oussama ben Laden sont des exemples patents de ce genre d'activités.

En outre, les sites Web sont des espaces de plus en plus efficaces pour effectuer du recrutement. En étalant les différents faits d'armes du groupe, les terroristes peuvent attirer l'attention d'éventuelles recrues intéressées par les activités du groupe et son idéologie. Les récentes études menées sur le contenu des activités terroristes en ligne tendent à démontrer que les organisations terroristes, notamment les organisations jihadistes, sont de plus en plus actives dans la diffusion de vidéos, principalement les vidéos de type « documentaire », fournissant ainsi aux recrues potentielles des raisons pour lesquelles elles devraient joindre la lutte (Salem, Reid et Chen, 2008).

La question du financement en ligne des organisations terroristes demeure, quant à elle, nébuleuse. S'il apparaît clair qu'il existe effectivement des activités de financement terroriste qui se déroulent en ligne, il est toutefois plus difficile de dire si elles sont marginales ou si, au contraire, elles constituent la nouvelle donne en matière de financement. Pour plusieurs, l'utilisation d'Internet dans la question du financement terroriste sert beaucoup plus dans le processus de transfert des fonds que dans le processus de collecte des fonds.

Il est aussi important de constater que l'activité du financement terroriste emprunte un chemin inverse de ce que l'on peut observer dans le monde criminel « classique ». En effet, le monde criminel classique va généralement tenter de blanchir de l'argent sale obtenu au travers d'une transaction criminelle (vente de stupéfiants, de services sexuels, de matières illicites, etc.), tandis que le financement des activités terroristes va bien souvent aller dans une direction inverse, c'est-à-dire que ces activités vont tenter de se noircir. Dans ce cas-ci, le financement va bien souvent passer au travers d'organismes de bienfaisance légaux (voir notamment Basile, 2004), mais une partie des fonds seront cachés – noircis – afin qu'on puisse les faire glisser vers des activités terroristes. Néanmoins, plusieurs spécialistes en appellent à la prudence et signalent que la tendance pourrait aisément changer rapidement dans les années à venir, principalement en raison du fait 1) que les technologies changent rapidement et 2) que le système financier devient de

plus en plus dépendant de la technologie. Ainsi, il n'est pas dit que les activités terroristes à venir ne prendront pas une direction tout autre et qu'elles ne seront pas principalement construites autour de versements en ligne de la part de différents partisans situés partout dans le monde (Jacobson, 2010).

La question de l'apprentissage revient bien souvent au cœur des arguments entourant les activités terroristes en ligne. Ainsi, on avance que les informations présentes en ligne sont suffisantes pour permettre à des organisations terroristes d'apprendre à se créer des armes de toutes sortes – principalement des explosifs. À cela s'ajoute le fait que bon nombre des éléments qui se trouvent en ligne contiennent des informations sur des cibles potentielles. Bref, pour les organisations terroristes, Internet est une source intarissable d'informations, ce qui leur permet d'échafauder des opérations plus efficaces et, surtout, d'échapper aux mailles du filet (voir entre autres Rudner, 2008).

Il est toutefois important de mettre un bémol à cet argument. Il est en effet intéressant de constater que des études précédentes menées sur les groupes de pirates informatiques tendent à démontrer que les apprentissages en ligne ne sont pas aussi forts qu'il est possible de le croire. Grosso modo, les différents agents œuvrant en ligne ne sont pas si enclins qu'il est possible de le croire à transmettre de l'information pertinente, et ce, pour des raisons de confiance (Skinner et Fream, 1997).

Cette exploitation d'Internet par les organisations terroristes est, encore une fois, difficile à jauger. Il est toutefois clair qu'Internet est un formidable outil permettant d'alimenter adéquatement la machine médiatique traditionnelle. Les TIC amènent une libéralisation extrême dans la production de contenu audiovisuel, une démocratisation permettant aux organisations terroristes elles-mêmes de devenir productrices et diffuseuses de leur propre contenu – une situation difficilement envisageable il y a à peine quelques décennies.

Or, le fait que les organisations terroristes puissent être maîtresses de leur message modifie grandement la chaîne de production de l'information « grand public ». En effet, il est de plus en plus commun de voir que les bulletins d'information télévisés utilisent les images tournées par les groupes terroristes eux-mêmes – bien souvent des images d'attentats qui servent surtout à vendre les activités du groupe à d'éventuelles recrues. Insidieusement, cela engendre deux effets.

Tout d'abord, cela donne un second souffle de terreur à un attentat terroriste ayant déjà eu lieu. Normalement, un attentat terroriste a un effet de terreur immédiat – un effet se produisant chez les personnes vivant l'attentat de visu – et un effet de terreur diffus qui se véhicule au travers des médias. Les TIC permettent donc de changer grandement la donne, car non seulement le stockage de ces images sur différents sites Web permet de garder une trame de fond de terreur – il est difficile de faire disparaître complètement ce qui se trouve sur le Web –, mais en plus, les médias traditionnels reprennent ces images, relançant ainsi l'effet psychologique recherché par les terroristes.

L'exemple le plus marquant de ce genre de manipulation médiatique se voit probablement au travers de l'utilisation des images de la décapitation de Nick Berg. La vidéo de la mise à mort de l'otage américain a tout d'abord été versée sur le Web, mais rapidement, ces images ont été reprises dans les grands médias traditionnels comme la BBC, CNN et Fox (BBC, 2004). C'est là une excellente preuve de la capacité offerte aujourd'hui par les TIC : elles permettent aux organisations terroristes d'effectuer une forme d'ingénierie médiatique en manipulant les canaux médiatiques classiques.

Ensuite, le fait que les organisations terroristes soient maintenant productrices et diffuseuses de leur propre contenu a pour effet de les garder plus en contrôle du message qu'elles veulent envoyer. Certes, les médias traditionnels pourront toujours remâcher leur message, mais le contenu original pourra toujours se retrouver en ligne et pourra servir de balise contrecarrant le discours dominant.

14.6.2 Internet : la nouvelle zone secondaire d'action?

À la lumière du fait que les TIC deviennent de plus en plus utilisées par les organisations terroristes, il est possible de se demander si c'est la naissance d'une nouvelle façon de voir la zone d'activité secondaire qui est actuellement en train de se produire.

Il faut comprendre que le terrorisme agit essentiellement dans deux zones : la zone primaire et la zone secondaire. La zone primaire correspond principalement à l'endroit géographique dans lequel l'organisation terroriste agit au niveau opérationnel direct – organisation des attentats, perpétration des attentats, etc. La zone secondaire, quant à

elle, représente l'endroit où l'organisation terroriste effectue la majorité de ses activités de logistique (financement, entraînement, recrutement, etc.). Évidemment, il est possible que la zone primaire et la zone secondaire se trouvent au même endroit. Par contre, ce qu'il est intéressant de constater, c'est qu'Internet tend à devenir une zone secondaire de terrorisme de plus en plus importante. Or, le fait qu'elle soit déterritorialisée pourrait engendrer des défis grandissants pour les autorités de sécurité dans les années à venir.

14.7 Conclusion

Au final, il est clair que la notion de cyberterrorisme devra être précisée par les spécialistes du sujet. Il est en effet encore difficile de comprendre les tenants et les aboutissants de cette notion et elle semble encore mal s'appliquer à des cas concrets provenant du réel.

Idem du côté du système législatif actuel : les lois encadrant les actes de terrorisme et de cyberterrorisme se penchent beaucoup plus sur les actes « traditionnels » de terrorisme, soit l'attentat, le complot pour fomenter des attentats et les activités entourant la logistique terroriste. Les actes de piratage de systèmes informatiques ayant pour objectif d'engendrer la terreur sont ignorés, notamment dans la législation canadienne. Cette situation est probablement tributaire du fait que, en soi, les actes de cyberterrorisme sont si peu nombreux – voire absents – qu'ils représentent des événements isolés pouvant bien souvent être gérés d'une autre façon qu'avec les lois sur les actions terroristes.

Le caractère exceptionnel du cyberterrorisme amène d'ailleurs à une réflexion sur l'importance même que l'on peut attribuer au sujet. Considérant que le terrorisme est une forme de criminalité politique exceptionnelle, notamment au Canada – les statistiques sur le terrorisme démontrent que le nombre d'attentats au Canada frôle une moyenne de zéro depuis la fin des années 1990 –, force est d'admettre qu'il faut également considérer le cyberterrorisme comme une exception dans l'exception. Doit-on donc craindre le pire? Peut-être. Mais de toute évidence, la catastrophe annoncée ne risque pas d'être autre chose qu'un acte isolé dans le temps. Tout comme l'amplitude des effets des attentats terroristes du 11 septembre 2001 semble être une « anomalie statistique ».

Bibliographie

ARQUILLA, J., et RONFELDT, D. F. (2001). *Networks and Netwars : the Future of Terror, Crime, and Militancy*, Santa Monica, RAND Corporation.

BASILE, M. (2004). « Going to the Source : Why Al Qaeda's Financial Network Is Likely to Withstand the Current War on Terrorist Financing », *Studies in Conflict and Terrorism*, vol. 27, nº 3, p. 169-185.

BBC (2004). « "Zarqawi" Beheaded US Man in Iraq », *BBC* [En ligne] news.bbc.co.uk/2/hi/middle_east/3712421.stm (consulté le 18 décembre 2011).

BBC (2011). « Hackers "Hit" US Water Treatment System », *BBC* [En ligne] www.bbc.co.uk/news/technology-15817335 (consulté le 28 novembre 2011).

BORGER, J. (2002). « US Fears al-Qaida Hackers Will Hit Vital Computer Networks », *The Guardian* [En ligne] www.guardian.co.uk/internetnews/story/0,7369,745628,00.html (consulté le 1er novembre 2011).

CHIRILLO, J. (2001). *Hack Attacks Encyclopedia : A Complete History of Hacks, Cracks, Phreaks, and Spies Over Time*, New York, John Wiley & Sons.

COUR DU QUÉBEC (2009). *Décision - R. c. Namouh - 2009 QCCQ 9324*, Société québécoise d'information juridique.

DENNING, D. E. (2001). *Information Warfare and Security*, New York, Addison-Wesley.

DUNNIGAN, J. F. (2002). *The Next War Zone : Confronting the Global Threat of Cyberterrorism*, New York, Citadel Press.

FBI (2008). « FBI 100 : The Unabomber », *FBI, The Federal Bureau of Investigation* [En ligne] www.fbi.gov/news/stories/2008/april/unabomber_042408 (consulté le 20 novembre 2011).

GLOBAL TERRORISM DATABASE (2011). *Global Terrorism Database* [En ligne] www.start.umd.edu/gtd (consulté le 26 décembre 2011).

HOMER-DIXON, T. (2002). « The Rise of Complex Terrorism », *Foreign Policy*, janvier-février, p. 52 à 62.

HOWITT, A. M., et PANGI, R. L. (2003). *Countering Terrorism : Dimension of Preparedness*, Cambridge, MIT Press.

JACOBSON, M. (2010). « Terrorist Financing and the Internet », *Studies in Conflict and Terrorism*, vol. 33, nº 4, p. 353-363.

LEWIS, J. A. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Washington, D.C., Center for Strategic and International Studies [En ligne] csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (consulté le 27 janvier 2012).

LITTLETON, M. J. (1995). *Information Age Terrorism : Toward Cyberterror* [En ligne] www.fas.org/irp/threat/cyber/docs/npgs/terror.htm (consulté le 19 novembre 2011).

MIYAWAKI, R. (2001). *International Cooperation to Combat Cyber Crime and Cyber Terrorism*, Standford, Présentation Keynote.

NORRIS, P., KERN, M., et JUST, M. (2003). *Framing Terrorism : The News Media, the Government and the Public*, New York, Routledge.

O'HANLON, M. (2000). *Technological Change and the Future of Warfare*, Washington, D.C., Brookings Institution Press.

POLLIT, M. M. (1997). *Cyberterrorism – Fact or Fancy?* [En ligne] www.cs.georgetown.edu/~denning/infosec/pollitt.html (consulté le 20 novembre 2011).

RUDNER, M. (2008). « Misuse of Passports : Identity Fraud, the Propensity to Travel, and International Terrorism », *Studies in Conflict and Terrorism*, vol. 31, nº 2, p. 95-110.

SALEM, A., REID, E., et CHEN, H. (2008). « Multimedia Content Coding and Analysis : Unraveling the Content of Jihadi Extremist Groups' Videos », *Studies in Conflict and Terrorism*, vol. 31, nº 7, p. 605-626.

SCHNEIER, B. (2007). « Terrorism Statistics », *Schneier on Security* [En ligne] www.schneier.com/blog/archives/2007/06/terrorism_stati.html (consulté le 26 décembre 2011).

SKINNER, W. F., et FREAM, A. M. (1997). « A Social Learning Theory Analysis of Computer Crime Among College Students », *Journal of Research in Crime and Delinquency*, vol. 34, nº 4, p. 495-519.

SMITH, T. (2001). « Hacker Jailed for Revenge Sewage Attacks », *The Register* [En ligne] www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage (consulté le 8 décembre 2011).

SOAFER, A. D., et GOODMAN, S. E. (2001). *The Transnational Dimension of Cyber Crime and Terrorism*, Standford, Hoover Institution Press.

THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (2004). *The 9/11 Report*, New York, St. Martin's Press.

U.S. DEPARTMENT OF HOMELAND SECURITY (2011). *Assessment of Anonymous Threat to Control Systems* [En ligne] info.publicintelligence.net/NCCIC-AnonymousICS.pdf (consulté le 1er novembre 2011).