Volume 2006-2

CIEM ITAC

CIEM présente

Tendances en terrorisme

L'usage d'Internet à des fins terroristes

Cet article a été rédigé par le Canadian Centre for Intelligence and Security Studies, The Norman Paterson School of International Affairs, Carleton University.

Le présent document donne un aperçu de la façon dont les terroristes utilisent Internet pour faire du recrutement et pour planifier et financer leurs activités avec plus d'efficacité. Il décrit les principaux concepts, les modes de fonctionnement actuels et les nouveaux enjeux. Une bibliographie commentée est comprise en annexe.

Introduction

La majorité des spécialistes du terrorisme et de l'antiterrorisme estiment que le nombre d'organisations et de groupes subversifs sur Internet a augmenté et continue de croître à un rythme alarmant. Bien que les estimations du nombre de sites Web terroristes actifs varient, d'après l'opinion générale, ce nombre est passé de moins d'une centaine en 1996 à plus de 5 000 à l'heure actuelle. En 2006, tous les groupes terroristes actifs (y compris ceux désignés en vertu de la loi américaine *Antiterrorism and Effective Death Penalty Act* de 1996) sont présents sur Internet sous une forme ou une autre. D'ailleurs, le Web a été l'un des principaux outils utilisés dans la planification et la coordination des attentats du 11 septembre 2001 à New York et à Washington. Les dirigeants et les experts savent maintenant qu'avant les attentats, il y a eu une forte hausse du trafic de la part des terroristes et leurs associés sur Internet, un signe qu'il faut mieux surveiller et interpréter la façon dont les groupes subversifs comme al-Qaïda utilisent Internet. Cette découverte soulève la question suivante : *Quel rapport existe-t-il entre les personnes et groupes subversifs (plus particulièrement les terroristes) et Internet?*

Tout d'abord, examinons ce qu'Internet offre à toutes les personnes et les organisations. Selon le rapport spécial *www.terror.net: How Modern Terrorism Uses the Internet* publié par le United States Institute of Peace, Internet a été salué comme « un rassembleur de cultures et un moyen pour les entreprises, les consommateurs et les gouvernements de communiquer entre eux » offrant « des occasions inouïes de constituer un forum où le 'village mondial' pourrait se réunir et échanger des idées afin de soutenir et de faire croître la démocratie dans le monde ». Certains vont même jusqu'à le qualifier d'assise de la société démocratique du XXIe siècle et font ressortir les valeurs fondamentales qu'il partage avec la démocratie : l'ouverture, la participation et la liberté d'expression pour tous.

Selon Mme Denning, les acteurs non étatiques emploient trois grandes catégories de méthodes : l'« activisme », le « cyberactivisme » et le « cyberterrorisme »

Plus précisément, Internet offre un certain nombre d'avantages importants : un accès facile; pratiquement aucune règle, censure ou autre forme de contrôle gouvernemental; un large public dans le monde entier; des communications anonymes et rapides; le faible coût lié à la création et au maintien d'une présence sur le Web; un contexte multimédia; et la capacité d'influencer les médias de masse traditionnels, qui s'appuient de plus en plus sur Internet pour couvrir l'actualité. Même si la plupart des internautes dans le monde utilisent ces avantages, certains considèrent un milieu ouvert et participatif tel qu'Internet, sans doute l'incarnation même de la liberté d'expression, comme un cadre propice à leurs activités subversives.

Concepts et expressions

L'analyse de Dorothy E. Denning sur l'influence exercée sur la politique étrangère au moyen d'Internet offre un cadre de référence qui aide à comprendre comment les personnes et les groupes subversifs (notamment les terroristes) se servent d'Internet. Selon M^me^ Denning, les acteurs non étatiques emploient trois grandes catégories de méthodes : l'« activisme », le « cyberactivisme » et le « cyberterrorisme ». Si l'on admet que ces catégories se chevauchent et sont sujettes à interprétation, la plupart des activités menées par les acteurs non étatiques (dans le présent document, il s'agit des groupes subversifs et terroristes) se classent dans l'une d'elles.

Les analystes et les experts jugent la menace du cyberterrorisme « exagérée »

L'activisme désigne l'utilisation normale et inoffensive d'Internet pour appuyer des objectifs ou une cause, par exemple la recherche sur Internet, la construction de sites Web, l'affichage d'informations sur ces sites, l'envoi de lettres et de publications électroniques par courriel, de même que l'utilisation du Web pour discuter d'enjeux, former des coalitions et planifier et coordonner des activités.

Le **cyberactivisme** associe le piratage informatique à l'activisme. Il désigne entre autres les opérations où l'on emploie des techniques de piratage contre le site Web d'une cible dans le but d'en perturber le fonctionnement, mais sans causer de dégâts importants. Les occupations de sites Web et les barrages virtuels, les bombardements électroniques automatiques, le piratage, les entrées illégales dans des ordinateurs et les virus et vers informatiques sont tous des exemples de cyberactivisme.

Le **cyberterrorisme** correspond aux activités terroristes menées dans le cyberespace, par exemple le piratage politique dont le but est de causer des torts graves comme des pertes de vies ou la ruine économique. Les préoccupations au sujet de la possibilité que des personnes ou des groupes terroristes pénètrent le système électronique du réseau énergétique, financier, des transports ou de la sécurité d'un pays et qu'ils causent des dégâts catastrophiques (panne de barrage ou de réacteur nucléaire, collisions multiples dans les airs ou écrasements d'avions, bouleversement des économies nationales par une perturbation du marché boursier, etc.) sont toutes reliées au phénomène du cyberterrorisme.

La peur des conséquences du succès d'un cyberattentat incite les autorités, les décideurs et les médias de masse à se concentrer davantage sur les dangers du cyberterrorisme que sur les autres types d'activités. En fait, les analystes et les experts jugent la menace « exagérée » et se montrent inquiets du fait qu'elle détourne l'attention des usages plus courants d'Internet (activisme), qui sont pourtant indispensables aux personnes et aux groupes subversifs ou terroristes.

D'après un article publié par l'Associated Press le 7 décembre 2005, Louis Reigel, directeur adjoint du FBI, a déclaré qu'al-Qaïda et les réseaux terroristes qui y sont associés sont actuellement incapables de monter des cyberattentats qui pourraient endommager les infrastructures essentielles des États-Unis. Il reconnaît que les groupes terroristes font preuve d'une évolution et d'une maîtrise techniques croissantes, mais affirme que selon les experts du FBI, pour l'instant, ils sont incapables de monter une campagne de cyberterrorisme appréciable.

Le cyberterrorisme pourrait même nuire à la stratégie actuelle de groupes terroristes comme al-Qaïda, qui préfèrent nettement tirer parti des avantages susmentionnés d'Internet pour atteindre leurs objectifs. Une campagne de cyberterrorisme pourrait mener principalement au renforcement des politiques de cyberdéfense nationales et internationales, qui mènerait à son tour au resserrement de la réglementation, du contrôle et de la surveillance des activités sur Internet, et éventuellement à la restriction de la liberté fondamentale dont ces groupes jouissent dans le cyberespace et dont ils ont besoin.

Le cyberactivisme est beaucoup plus fréquent, mais risque moins de causer des dommages importants à lui seul. Il soulève de plus grandes préoccupations lorsque des personnes ou des groupes subversifs le combinent à un usage d'Internet à des fins activistes. Les terroristes qui font du cyberactivisme peuvent afficher de la propagande sur des sites particuliers. Entre autres, ils peuvent afficher les attentats que les insurgés en Irak ont menés avec succès contre les forces américaines dans des sites Web gouvernementaux vulnérables et des forums occidentaux très fréquentés. La même technique peut être utilisée pour laisser des messages chiffrés sur des sites publics ainsi que pour transmettre des communications allant des manuels aux ordres d'exécution, en passant par les stratégies de coordination d'une attaque.

En outre, le cyberactivisme peut être utilisé dans le cadre d'un attentat planifié. Par exemple, on peut ralentir les réseaux de communication d'un organisme d'intervention d'urgence du gouvernement ou d'un organisme d'application de la loi au moyen d'une bombe électronique (piratage et subversion d'ordinateurs de milliers d'utilisateurs en ligne en vue de perturber un site particulier) pour retarder la détection d'un attentat et la réaction à cet attentat afin d'augmenter ses chances de succès.

Cependant, le cyberactivisme demeure une méthode de choix pour les personnes qui ont les connaissances et les aptitudes nécessaires aux activités qui y sont liées. Il s'agit d'une forme d'activisme politique plus souvent utilisée par les groupes subversifs non violents que par les groupes terroristes. Il ne fait aucun doute que la majorité des groupes terroristes préfèrent se concentrer sur l'activisme. Les analystes et les experts croient que l'utilisation inventive et de plus en plus fréquente de cette méthode constitue la plus grande menace pour la sécurité nationale et internationale à long terme. La guerre psychologique, la publicité, la propagande, la

prospection de données, la collecte de fonds, le recrutement, la mobilisation, le maillage, le partage d'informations, la planification et la coordination sont tous des exemples de ces activités.

Internet comme moyen pour les terroristes de trouver des appuis

Avant de décrire plus en détail la façon dont les groupes terroristes utilisent les activités susmentionnées, il est important de préciser pourquoi Internet est devenu l'instrument grâce auquel le terrorisme se prolonge dans le XXIe siècle. L'Internet moderne tire son origine du désir qu'avait le département de la Défense des États-Unis de rendre son infrastructure de communications moins vulnérable à une attaque nucléaire soviétique. Pour ce faire, il a élaboré et créé une toile de réseaux informatiques interconnectés qui lui permettait de réaliser deux objectifs essentiels au maintien et à la continuité de son infrastructure de communication en matière de sécurité et de défense : la décentralisation et la redondance. Ironiquement, ces deux mêmes caractéristiques jouent maintenant un rôle stratégique dans la réorganisation, le maintien et la perpétuation du « pire ennemi » déclaré des services de sécurité occidentaux du XXIe siècle : le terrorisme international.

Privés en grande partie de l'espace géographique essentiel à leurs activités, les réseaux et les groupes terroristes se sont en quelque sorte réorganisés dans le cyberespace, en tirant parti des avantages susmentionnés d'Internet pour décentraliser leurs opérations, tout en se servant de la révolution de l'information pour créer une redondance qui assure sa survie et sa continuité.

Le réseau terroriste moderne, en particulier celui du « mouvement jihadiste mondial », n'a plus de hiérarchie. Il s'agit plutôt d'un ensemble peu structuré de noeuds, parfois directement connectés au réseau, parfois indépendants. En conséquence, comme le réseau n'a plus de structure administrative à décapiter, il a plus de facilité à subsister.

De plus, même si l'on élimine plusieurs noyaux d'un seul coup, l'organisation demeure opérationnelle, et comme le systême est redondant, le moment et le lieu des activités de n'importe quel noyau peuvent être modifiés, ce qui donne à l'organisation une aptitude de régénération qu'elle ne possédait pas auparavant.

Ainsi, pour comprendre la relation entre les groupes terroristes et Internet, il faut tenir compte du rôle central qu'occupe la révolution de la technologie et des communications. à titre d'acteurs non étatiques dépourvus ou privés d'un territoire physique d'où ils pourraient mener leurs opérations, les groupes terroristes d'aujourd'hui cherchent à se tailler un territoire virtuel (ou refuge virtuel) d'où ils pourront planifier, coordonner et mener leurs activités. La reconstitution d'Internet comme une sorte de système nerveux central d'organisations telles qu'al-Qaïda est essentielle à leur survie, tant comme organisations que comme mouvements.

Le réseau d'al-Qaïda et les groupes terroristes qui y sont associés sont peut-être l'archétype de ce phénomène contemporain. Dans un article du Washington Post publié le 7 août 2005, Steve Coll et Susan B. Glasser décrivent al-Qaïda comme le premier « mouvement de guérilla de l'histoire à être passé du monde réel au monde virtuel » en utilisant les technologies de l'information et des communications modernes pour (re)créer d'anciennes bases opérationnelles qu'il avait établies dans des refuges comme en Afghanistan après 2001. Les auteurs soutiennent que le « mouvement jihadiste mondial », parfois dirigé par al-Qaïda mais comptant de plus en plus de groupes variés et de cellules ad hoc avec lesquels il a des liens plus informels, est devenu un phénomène « fondé sur le Web », qui a donné forme à une communauté virtuelle indirectement guidée par une association de convictions. En définitive, les activités des groupes comme al-Qaïda sur Internet servent non seulement à promouvoir leurs principes idéologiques et théologiques, mais aussi à convertir de vastes étendues du cyberespace en une « université du jihad ouverte ».

Al-Qaïda serait le premier « mouvement de guérilla de l'histoire à être passé du monde réel au monde virtuel »

L'activisme des groupes terroristes, dont les plus célèbres sont al-Qaïda et les groupes qui y sont affiliés, est une preuve de cette tendance. L'utilisation d'Internet pour faire de la désinformation, pour formuler des menaces qui inspirent des sentiments de peur et d'impuissance et pour diffuser des images atroces d'actes récents (bandes vidéo montrant l'exécution de ressortissants étrangers et de travailleurs humanitaires pris en otage, attaques contre l'armée américaine, etc.) s'inscrit dans une campagne psychologique délibérée et étendue qui est ouvertement menée dans le cyberespace. Comme l'affirme Gabriel Weiman, du United States Institute of Peace, « Internet – un véhicule non censuré qui propage des images, des menaces et des messages sans égard à leur validité ou à leurs conséquences – convient particulièrement bien aux groupes, même ceux de petite taille, qui veulent amplifier leur message, en gonfler l'importance et exagérer la menace qu'ils représentent ». C'est un outil de communication qui permet aux acteurs non étatiques de prétendre qu'ils jouent un rôle international, d'influencer l'opinion publique et même d'influencer les décisions en matière de politique étrangère.

La publicité et la propagande sont des activités étroitement liées à la guerre psychologique. Avant l'avènement d'Internet, la soif de publicité des terroristes était modérée par le « seuil de sélection » des médias, qui déterminaient les nouvelles et les événements dignes d'être mentionnés, et surtout, la façon de les communiquer au public. Le terroriste contemporain détermine lui-même le contenu de ses messages en les publiant sur son propre site Web ou dans ses propres forums en ligne, ce qui a pour effet d'éliminer le « seuil de sélection ». Les terroristes n'ont aucun mal à influencer l'opinion de différents publics cibles en manipulant leur propre image et celle de leurs ennemis.

Internet comme manuel d'instructions

Un article de Scott Shane publié dans le New York Times le 23 novembre 2005 mentionne les récentes mesures prises par l'appareil de renseignement américain pour intégrer l'analyse des sources ouvertes au système de renseignement des États-Unis. L'article fait l'éloge de l'abondance et du caractère exceptionnel des informations que l'on peut recueillir à l'infini grâce à la navigation et à la recherche en ligne. Cette réalité n'a pas échappé aux terroristes. La prospection active des données est sans doute l'un des services les plus utiles qu'offre Internet. Le cyberespace est une source inépuisable de connaissances et d'instructions dont les réseaux terroristes se servent activement.

Grâce à la prospection de données, les terroristes obtiennent de précieuses informations sur les réseaux de transport, les centrales nucléaires, les édifices publics, les ports, et même les activités et les stratégies de lutte contre le terrorisme des services de sécurité occidentaux.

En outre, ils peuvent réunir ces données pour créer des manuels, des instructions et une quantité considérable de documentation sur des sujets divers allant de la création d'une cellule terroriste aux moyens d'échapper aux autorités occidentales, en passant par l'acquisition d'armes et de matériel et la fabrication d'explosifs (un récent manuel détaillé indique comment fabriquer des engins chimiques, radiologiques et nucléaires).

Des imagiciels modernes mais abordables permettent de réaliser des cartes et des diagrammes interactifs que l'on peut rendre très accessibles. Les moteurs de recherche évoluée comme Google donnent un accès facile à des myriades d'informations. Les questions et les informations sensibles que les terroristes ne veulent pas afficher dans les forums électroniques publics se transmettent au moyen de listes de distribution, de salles de clavardage et de groupes de discussion.

Grâce aux sources ouvertes, il est possible de recueillir, sans même recourir à des moyens illégaux, au moins 80 p. cent de toute l'information nécessaire sur l'ennemi.

Les experts croient que les cellules terroristes sophistiquées s'appuient maintenant sur de vastes bases de données créées et tenues à jour par de nombreuses cellules qui travaillent en collaboration. Celles-ci recueillent et analysent des renseignements sur des cibles données pour faciliter la planification et la coordination des attentats. « Grâce aux sources ouvertes, il est possible de recueillir, sans même recourir à des moyens illégaux, au moins 80 p. cent de toute l'information nécessaire sur l'ennemi. » Cette citation n'est pas d'un analyste des services de sécurité et de renseignements occidentaux, mais bien d'un manuel d'entraînement d'al-Qaïda saisi en Afghanistan en janvier 2003.

Financement et recrutement

Pour subsister, un réseau terroriste doit absolument trouver et obtenir le financement nécessaire à ses activités. L'anonymat et la portée mondiale

qu'offre Internet permettent à de nombreux groupes subversifs de financer leurs activités. Par exemple, al-Qaïda et les groupes qui y sont associés dépendent beaucoup des dons recueillis au moyen d'un réseau de financement mondial composé d'organismes de bienfaisance, d'organisations non gouvernementales et d'institutions financières qui collectent activement des fonds sur des sites Web, dans des salles de clavardage et dans des forums. Les groupes publient sur leurs sites Web et sur ceux de leurs collaborateurs des numéros de compte et des informations bancaires grâces auxquels leurs partisans peuvent verser un don anonyme en signe d'appui.

Un article de Craig Whitlock publié dans le Washington Post le 8 août 2005 examine le cas de l'informaticien et ingénieur en mécanique Babar Ahmad, 31 ans, arrêté sous l'inculpation de diriger un réseau de sites Web utilisé pour diffuser de la propagande et collecter de fonds pour des islamistes, y compris les rebelles tchétchènes, les miliciens talibans et les groupes associés à al-Qaïda. Sur ses sites Web, Ahmad affichait des numéros de compte où les partisans pouvaient verser des dons. Une autre démarche plus dynamique des terroristes consiste à utiliser des logiciels modernes pour recueillir les données démographiques des internautes qui visitent leurs sites (y compris ceux des groupes qui y sont affiliés et de leurs sociétés-écran) pour repérer les personnes favorables à une question ou à une cause connexe. Ils communiquent ensuite avec chacune de ces personnes par courriel pour leur demander de verser un don à une organisation avec laquelle ils n'ont aucun lien direct.

La saisie des informations et des profils des internautes qui visitent de tels sites Web sert aussi à deux activités connexes : le recrutement et la mobilisation. Les internautes qui semblent très intéressés par la cause d'une organisation ou aptes à servir cette cause sont contactés d'une manière semblable à celle utilisée pour collecter des fonds. Grâce aux possibilités croissantes de conversations personnelles en ligne, les groupes et les recruteurs terroristes peuvent mener des campagnes de recrutement beaucoup plus dynamiques. Les recruteurs parcourent les salles de clavardage et les cybercafés et affichent des messages sur les babillards électroniques, à l'affût de personnes réceptives, plus particulièrement de jeunes personnes vulnérables, qu'ils pourraient inciter à entrer dans un groupe terroriste en les préparant et en les encourageant en ligne dans un contexte privé. Dans son rapport annuel de 2004, le Service général de renseignement et de sécurité des Pays-Bas souligne l'importance d'Internet, particulièrement dans la radicalisation de certaines parties de la communauté musulmane au pays grâce à la dawa « virtuelle » (sermons radicaux en ligne) et de plus en plus grâce aux salles de clavardage sans surveillance, où les échanges animés de vues islamiques sur l'autoroute électronique (un processus autodirigé) sont de plus en plus fréquents par rapport à l'endoctrinement personnel effectué par les prédicateurs.

Le phénomène ne se limite pas aux Pays-Bas. Une fois repérées, les recrues éventuelles sont bombardées de décrets religieux, de propagande et de manuels sur la façon de prendre part au « mouvement jihadiste mondial ». Celles qui se laissent appâter par les discours ou par leur curiosité sont guidées à travers un

dédale de salles de clavardage secrètes ou reçoivent l'instruction de télécharger le logiciel Paltalk, grâce auquel les utilisateurs peuvent se parler sur le Web sans crainte d'être surveillés. C'est à ce moment que commence l'endoctrinement personnel en ligne.

Maillage

D'après Weiman, de nombreux groupes terroristes « sont passés d'une structure strictement hiérarchique comprenant des chefs désignés à un ensemble de cellules mi-indépendantes dépourvues de hauts dirigeants communs ». La révolution de la technologie et des télécommunications qu'Internet incarne a considérablement réduit les délais et les coûts des communications tout en augmentant la diversité et la complexité des informations que l'on peut partager. Le maillage aide les organisations terroristes modernes à se restructurer en un ensemble décentralisé de groupes transnationaux qui ont des objectifs ou des convictions semblables et qui communiquent et font de la coordination de façon horizontale plutôt que verticale, de manière rapide et complexe.

De nombreux groupes terroristes sont passés d'une structure strictement hiérarchique comprenant des chefs désignés à un ensemble de cellules mi-indépendantes dépourvues de hauts dirigeants communs

La facilité avec laquelle on peut maintenant constituer des réseaux avec des cellules et d'autres groupes partout dans le monde augmente l'efficacité d'Internet comme moyen de planifier et de coordonner des activités et des attentats. Les événements du 11 septembre sont sans doute l'exemple le plus représentatif de l'utilité que peut avoir Internet pour les personnes et les organisations qui veulent planifier, coordonner et perpétrer des attentats dans les pays démocratiques occidentaux. Les agents d'al-Qaïda se servaient d'Internet dans des lieux publics et communiquaient grâce à des comptes de courriel gratuits sur le Web pour garder l'anonymat. De même, d'autres groupes comme le Hamas discutent de leurs opérations et les planifient dans des salles de clavardage, tandis que des exécutants coordonnent par courriel des actes visant la bande de Gaza, la Cisjordanie, le Liban et Israël. En outre, on communique des instructions codées par voie électronique, généralement dans des dialectes obscurs que pratiquement aucun linguiste des services de sécurité et de renseignements occidentaux n'est entraîné à déchiffrer.

Les groupes terroristes emploient aussi la méthode de la « boîte aux lettres morte virtuelle » pour transmettre certaines de leurs informations les plus sensibles en matière de planification et de coordination. Pour ce faire, ils ouvrent un compte dans un service de courriel public gratuit (p. ex. Hotmail), rédigent et enregistrent une ébauche de message, puis transmettent au destinataire le nom d'utilisateur et le mot de passe du compte de courriel en langage codé sur un babillard sécurisé. Le destinataire peut ensuite ouvrir le compte et lire l'ébauche de message. Les instructions sous forme de cartes interactives, de photographies détaillées ou de détails techniques sont communiquées secrètement par stéganographie (technique de dissimulation de fichiers ou de messages dans des fichiers graphiques).

Conclusion : Le proche avenir

Une récente dépêche du Service canadien de renseignements criminels décrit les activités d'un dénommé « Ayaf » membre d'un forum en ligne et collaborateur prolifique du site Web de l'Organisation du renouveau islamique (ORI). Dans une déclaration publiée sur le site le 3 octobre 2005, « Ayaf » annonçait qu'il avait communiqué directement avec une personne liée à al-Qaïda et que celle-ci lui avait ordonné de transmettre l'ordre de détruire un réacteur nucléaire à la division d'al-Qaïda aux États-Unis dirigée par Abu-Azzam al-Amriki.

Un article de Molly Moore et de Daniel Williams publié le 10 novembre 2005 dans le Washington Post porte sur le rôle de la messagerie textuelle et des carnets Web français dans l'organisation, la mobilisation et l'incitation à la violence des jeunes Français musulmans en banlieue de Paris et dans quelque 300 autres villes de la France.

Ces deux cas montrent clairement que, lors d'une crise, Internet est très utile pour fausser le débat et pour diffuser des images trompeuses de la réalité, de même que pour jeter de l'huile sur le feu grâce à des messages haineux et à la promotion de la violence. Ils font également ressortir l'importance de tels forums comme outils de communication d'informations opérationnelles et de coordination des activités de cellules terroristes réparties dans plusieurs régions géographiques. Peut-être un présage de l'avenir, ils montrent aussi les difficultés auxquelles se heurtent les autorités lorsqu'elles tentent de surveiller et de maîtriser de tels comportements. ◆

Bruno Nordeste
David Carment

Université Carleton,
Ottawa

ANNEXE - SOURCES

ARTICLES DE NOUVELLES ET DÉPÊCHES (par ordre chronologique)

***Washington Post* : « Terrorists Turn to Web as Base of Operations »** – de Steve Coll et Susan B. Glasser, dimanche 7 août 2005 (http://www.washingtonpost.com/wpdyn/content/ article/2005/08/05/ AR2005080501138.html)

- Article intelligent publié par le *Washington Post* dans le cadre d'une série sur la relation entre le mouvement jihadiste mondial (tel qu'il est représenté par al-Qaïda) et Internet.
- L'auteur soutient qu'al-Qaïda est le premier « mouvement de guérilla de l'histoire à être passé du monde réel au monde virtuel » en utilisant les technologies de l'information et des communications modernes pour (re)créer d'anciennes bases opérationnelles qu'il avait établies dans des refuges comme en Afghanistan après 2001.
- Le « mouvement jihadiste mondial », parfois dirigé par al-Qaïda mais comptant de plus en plus de groupes variés et de cellules ad hoc avec lesquels il a des liens plus informels, est devenu un phénomène « fondé sur le Web », qui a donné forme à une communauté virtuelle indirectement guidée par une association de convictions.
- L'article décrit la collection croissante de documents accessibles et largement distribués en ligne aux membres de cette communauté virtuelle, notamment des sermons, des cartes, des manuels ainsi que des essais théoriques, théologiques et scientifiques qui servent tous à l'endoctrinement, au recrutement, à la communication, à l'entraînement, à la collecte de fonds, à la mobilisation et à l'organisation aux fins du « mouvement jihadiste mondial ».
- En définitive, les activités des groupes comme al-Qaïda sur Internet servent non seulement à promouvoir leurs principes idéologiques et théologiques, mais aussi à convertir de vastes étendues du cyberespace en une « université du jihad ouverte ».
- Enfin, l'article décrit la nouvelle tendance des « cellules virtuelles », qui permettent à des personnes partageant les mêmes idées de discuter en gardant l'anonymat jusqu'à ce qu'elles créent des liens de confiance réciproque et qu'elles terminent leur entraînement. Elles sont alors prêtes à se rencontrer et à mener une opération sur le terrain.

***Washington Post* : « Briton Used Internet as His Bully Pulpit »** – de Craig Whitlock, lundi 8 août 2005 (http: //www.washingtonpost.com/wpdyn/content/article/2005/08/07/ AR2005080700890.html)

- Article intelligent publié par le *Washington Post* dans le cadre d'une série sur la relation entre le mouvement jihadiste mondial et Internet.
- L'article examine le cas de l'informaticien et ingénieur en mécanique Babar Ahmad, 31 ans, arrêté sous l'inculpation de diriger un réseau de sites Web utilisé pour diffuser de la propagande et collecter des fonds pour des islamistes, y compris les rebelles tchétchènes, les miliciens talibans et les groupes associés à al-Qaïda.
- Il ressort que le mouvement jihadiste mondial est non seulement un combat militaire, mais aussi une guerre de l'information, et que le jihad militaire le plus efficace consiste à utiliser Internet pour propager les idées, pour exploiter le pouvoir des mots.

***Washington Post* : « The Web as Weapon »** – de Susan B. Glasser et Steve Coll, mardi 9 août 2005 (http://www.washingtonpost.com/wpdyn/content/article/2005/08/08/ AR2005080801018.html)

- Article intelligent publié par le *Washington Post* dans le cadre d'une série sur la relation entre le mouvement jihadiste mondial et Internet.
- L'article porte sur l'incroyable succès qu'Abou Moussab al-Zarkaoui et les militants d'al-Qaïda en Irak ont obtenu en combinant leurs guérillas dans le monde physique au jihad dans le monde virtuel.
- Ce succès est remarquable, non seulement en raison de l'ampleur du contenu que les « agents de communication » d'al-Zarkaoui réussissent à diffuser dans le monde, mais aussi en raison de la complexité de l'organisation et de la présentation de ce contenu ainsi que du peu de temps qu'il a fallu pour construire un tel « empire en ligne », qui n'existait pas il y a à peine plus d'un an.
- Al-Zarkaoui est un exemple de la nouvelle génération de moudjahidin, qui sont habiles et disposés à tirer parti des commodités et des nouveautés dans le domaine des technologies de l'information et des communications modernes pour égaliser les chances autant que possible et surmonter le désavantage de la supériorité militaire écrasante des États-Unis.

***DEBKA File*, rapport spécial : « New Surge in Al Qaeda's Internal Electronic and Human Traffic »** – 13 août 2005 (http://www.debka.com/article.php?aid=1070)

- Article signalant une augmentation des communications internes, des signaux, des publications et des sites Web d'al-Qaïda (codés pour la plupart) comparable à celle constatée dans les mois qui ont précédé les attentats du 11 septembre 2001.
- Selon l'article, les communications codées diffusées dans les sites internes indiquent un mouvement des membres et des nouvelles recrues révélant que le réseau est de nouveau prêt à commettre des attentats multiples contre des cibles dispersées.
- On croit que la vague d'activités électroniques et humaines est un signe qu'al-Qaïda prépare un attentat et que, même si ce n'est pas corroboré, compte tenu de la qualité des renseignements dont disposent les services de renseignements occidentaux sur le réseau d'al-Qaïda (qui ne s'est pas améliorée, de l'avis des auteurs), le trafic électronique interne doit être considéré comme un indicateur important des intentions de l'organisation.
- La contribution probablement la plus utile de l'article est l'accent qu'il met sur l'importance qui devrait être accordée à la quantité et au ton des communications électroniques (dont la plupart sont codées et interdites aux non-initiés) entre les réseaux terroristes.

Glenmore Trenear-Harvey, condensé sur le renseignement : « Al-Qaeda embarks on Internet media campaign to terrorize US » – de Habib Trabelsi, News24.com, 19 août 2005

- Article signalant qu'une « brigade du jihad médiatique » liée à al-Qaïda s'est lancée dans une campagne sur Internet visant à terroriser les États-Unis en diffusant des images d'Américains tués ou blessés en Irak.
- Reconnaissant l'importance de la bataille médiatique dans l'issue de la guerre sur le terrain, le groupe a demandé aux militants d'afficher des images de mort et de destruction horrifiantes pour terroriser

et démoraliser l'ennemi.

- Le groupe n'emploie pas uniquement sa tactique sur les forces dirigées par les Américains, mais aussi sur leurs familles aux États-Unis. Pour ce faire, il diffuse les images dans le monde entier grâce à des envois massifs de courriels et au piratage.
- La demande a été publiée avec un document technique sur les pratiques exemplaires concernant l'utilisation des appareils photo et d'autres appareils de saisie d'images.
- L'article montre le rôle central d'Internet dans les tentatives des groupes liés à al-Qaïda pour transmettre leur message et, surtout, pour mener la guerre de l'information.

***Globe and Mail* : « Ottawa to give police more power to snoop »** – de Bill Curry, vendredi 19 août 2005

- Article sur l'intention du gouvernement canadien de présenter à l'automne 2005 un projet de loi visant à donner de nouveaux pouvoirs aux services policiers et aux organismes de sécurité nationale qui leur permettraient d'écouter les conversations sur les cellulaires et de surveiller les activités des Canadiens sur Internet.
- Le projet de loi réformerait ce que le ministre de la Justice a appelé « des lois de surveillance désuètes » rédigées avant la révolution des télécommunications (1974).
- En vertu du projet de loi, les fournisseurs d'accès Internet devraient conserver des dossiers sur l'usage que ses clients font d'Internet, notamment sur leurs habitudes de navigation et leurs pseudonymes en ligne, de manière à ce que les autorités puissent facilement les consulter.
- Certains se sont dits inquiets que les nouvelles mesures confèreraient des pouvoirs de surveillance considérables et portant atteinte à la vie privée qui pourraient donner lieu à des abus et à la divulgation d'informations sensibles sur les Canadiens à leur insu.
- Le projet de loi peut être perçu comme une tentative du gouvernement de donner aux forces de l'ordre un accès aux technologies équivalent à celui des criminels et des terroristes.

***Toronto Star* : « Terrorism/Internet – A Virtual Sanctuary for al-Qaeda networks »** – de Shawn Brimley et Aidan Kirby, 23 août 2005 (www.thestar.com/NASApp/cs/ ContentServer?pagename=thestar/layout/Article_PrinterFriendly&c=Article&cid=1124747413259&call_pageid=968256290204)

- Article contenant une analyse intelligente de la façon dont les réseaux de terroristes d'al-Qaïda se servent d'Internet comme d'un refuge virtuel.
- Al-Qaïda semble être en train de gagner la guerre du cyberspace puisque le Web est devenu le réseau de communication, le mode de recrutement, le mécanisme de financement et le camp d'entraînement de l'organisme, et qu'au moins une partie de chaque aspect du jihad mondial se passe en ligne.
- La migration d'al-Qaïda dans le cyberespace, où les sites Web terroristes sont passés de moins d'une vingtaine en 1998 à plus de 4 500 à l'heure actuelle, a dépassé la capacité des services de renseignements occidentaux de surveiller ses activités en ligne et d'y réagir.
- Internet n'est pas seulement un outil pour les terroristes. Il s'agit en quelque sorte du système nerveux central d'organisations comme al-Qaïda, un système indispensable à leur survie, tant comme organisations que comme mouvements, qui les aide à se régénérer.
- Toute stratégie visant à miner les réseaux terroristes mondiaux doit tenir compte d'Internet comme

d'un aspect essentiel de leurs communications, de leur organisation et de leur perpétuation.

***BBC News* : « Saudi dissident shuts down site »** – 28 août 2005 (http:news.bbc.co.uk/go/pr/ fr/-/2/hi/uk_news/4191396.stm)

- Reportage sur le site Web controversé de Muhammed al-Massari, où des images d'attentats suicide en Israël et en Irak et des messages de partisans d'al-Qaïda ont été affichés.
- L'article soulève la question de la liberté d'expression et des limites de la décence et de la sécurité dans le cybermonde.
- Le site a été fermé et des représentants du gouvernement ont réclamé l'expulsion d'al-Massari, une demande contestée par des groupes de défense de la liberté publique comme Amnistie Internationale.

Chronique du FBIS (FEA20051004010077) : « Analysis: Increasing Prolific Contributor Posts Threat to US Nuclear Reactor » – 5 octobre 2005 (article fourni par Greg Ohayon, du SCRC)

- Article sur les activités d'un dénommé « Ayaf » membre d'un forum en ligne et collaborateur prolifique du site Web de l'Organisation du renouveau islamique (ORI) (www.tajdeed.com.uk/forums).
- Bien qu'« Ayaf » se contentait auparavant d'afficher d'anciens articles et d'anciennes déclarations jihadistes ainsi que des informations personnelles à son propre sujet, le 3 octobre 2005, il a publié un nouveau type de message dans lequel il annonçait avoir communiqué directement avec une personne liée à al-Qaïda, transmettait à la division d'al-Qaïda aux États-Unis, dirigée par Abu-Azzam al-Amriki, l'ordre de détruire un réacteur nucléaire aux États-Unis et décrivait les secteurs de responsabilité géographiques des dirigeants d'al-Qaïda.
- L'article souligne l'importance de ce type de forum comme mode de transmission d'informations opérationnelles et de coordination des activités entre des cellules terroristes situées dans des régions géographiques différentes.
- Il fait également ressortir que l'augmentation du nombre de communications (dans ce cas-ci, une vague d'articles de forum et une forte participation aux discussions) pourrait signaler la coordination d'un attentat terroriste.
- Un autre aspect important est la capacité remarquable que l'on avait de changer l'emplacement du serveur du site Web lorsque les forces de l'ordre et le gouvernement tentaient de fermer le site. Le serveur, qui a occupé trois emplacements différents en moins de deux mois après les attentats à la bombe du 7 juillet à Londres, a été déplacé de Londres à Hong Kong, puis de là en Allemagne.

***The Middle East Media Research Institute* : Série de dépêches spéciales nº 1004, « On Islamic Websites: A Guide for Preparing Nuclear Weapons »** – 12 octobre 2005 (http://memri.org/bin/latestnews.cgi?ID=SD100405)

- Dépêche sur les sites Web islamistes qui contiennent des directives sur la fabrication d'armes nucléaires.
- Le 6 octobre 2005, dans le forum islamiste à l'adresse http://alfirdaws.org/forums/ showthread.php?t=5268&page=1&pp=10, un document intitulé *An Encyclopedia for the Preparation of Nuclear Weapons* a été mis en circulation parmi les membres.
- Le document d'environ 80 pages est divisé en neuf leçons rédigées « à des fins de recherche scientifique par Jihad Fighter No.1 », qui affirme avoir étudié la physique nucléaire et la technologie

ballistique en fréquentant divers forums scientifiques et jihadistes.

- Les leçons comprennent un historique de la science nucléaire ainsi que des explications sur la radioactivité naturelle, les qualités naturelles de certains matériaux, la masse critique, la composition des armes nucléaires et l'extraction du radium.
- Même si le document n'indique pas que des cellules terroristes sont en mesure de fabriquer une telle arme, l'auteur est d'avis que les moudjahidin ne peuvent atteindre l'équilibre stratégique militaire sans progrès scientifique et, surtout, démontre l'utilité des forums sur Internet pour communiquer des informations de base ainsi que pour enrichir les connaissances des réseaux terroristes par une mise en commun de leurs connaissances spécialisées.

***The Straits Times* : « Countering militant Islam in cyberspace »** – de Mafoot Simon, mardi 18 octobre 2005 (http://www.asiamedia.ucla.edu/article.asp?parentid=31719)

- Article avançant qu'Internet est devenu plus qu'un simple outil pour les terroristes. Il est maintenant indispensable à leurs opérations, notamment au recrutement de membres, à la collecte de fonds, à la promotion de l'idéologie et, de plus en plus, à la coordination des opérations tactiques et à l'entraînement des recrues.
- Internet est un média idéal pour le terroriste moderne, car il lui donne un caractère d'universalité tout en préservant son anonymat.
- Une tendance plus récente et inquiétante est la capacité des nombreux forums jihadistes de retenir l'attention des jeunes internautes musulmans qui veulent uniquement mieux comprendre leur religion, surtout au moyen des sermons en ligne. La bataille pour séduire les musulmans se livre maintenant dans le cyberespace, où les opinions modérées ou différentes sont dangereusement sous-représentées.
- L'auteur avance que le meilleur moyen de lutter contre l'attrait du terrorisme en ligne consiste à instruire et à sensibiliser la communauté musulmane, plus particulièrement les dirigeants musulmans laïcs locaux, sur l'usage d'Internet (pour qu'ils s'y sentent à l'aise). En effet, s'ils déplacent « leur » lutte sur le Web en intégrant leurs discussions et leurs forums à leurs propres sites Web, ils fourniront des solutions de rechange et des occasions de dialogue dans un média où les opinions extrémistes occupent une place de plus en plus dominante.

***The Times* : « Deported Jihadists resume UK activity by Internet »** – de Sean O'Neill et Yaakov Lappin, 23 octobre 2005 (http://www.timesonline.co.uk/article/0,,22989-1835824,00.html)

- Article sur les activités de l'imam radical exilé Omar Bakri Mohammad, plus particulièrement sur le fait qu'il continue de communiquer avec ses disciples par l'intermédiaire de sites Web et de salles de clavardage.
- Ces activités révèlent qu'al-Qaïda et les groupes qui y sont affiliés tentent d'utiliser Internet pour attirer une génération de recrues moins visible dans des pays occidentaux tels que le Royaume-Uni.
- Grâce au réseau Internet « Paltalk » très connu, dirigé par une entreprise à New York, des imams extrémistes comme Bakri continuent de joindre un vaste public.

***The Sunday Times* : « Al-Qaeda woos recruits with nuclear bomb website »** – de Uzi Mahnaimi et Tom Walker, 6 novembre 2005 (http://www.timesonline.co.uk/article/0,,2089-1859222,00.html)

- Article sur la publication dans un site Web sur al-Qaïda d'instructions détaillées en arabe sur la fabrication

des bombes nucléaires, des bombes « sales » et des bombes biologiques.

- Le site Web, qui a été consulté plus de 57 000 fois, a suscité des centaines de demandes de renseignements des lecteurs, ce qui soulève la préoccupation que le site pourrait accroître la popularité d'al-Qaïda auprès des recrues potentielles.
- Le document de 80 pages, divisé en neuf leçons, a alarmé les atomistes en raison de l'exactitude et du détail de ses instructions, qui vont bien au-delà des principes de base.
- Il indique qu'al-Qaïda est véritablement résolu à acquérir et à déployer des armes de destruction massive.
- On s'inquiète davantage de l'incidence que de telles publications pourraient avoir sur les jeunes musulmans vulnérables, qui pourraient interpréter la popularité du site comme un signe de la force et de l'attrait d'al-Qaïda.

***Washington Post* : « France's Youth Battles Also Waged on the Web »** – de Molly Moore et Daniel Williams, 10 novembre 2005 (http://www.washingtonpost.com/wpdyn/content/article/ 2005/11/09/AR2005110902134.html)

- Article sur le rôle de la messagerie textuelle et des carnets Web français dans l'organisation, la mobilisation et l'incitation à la violence des jeunes Français en banlieue de Paris et dans quelque 300 autres villes de la France.
- L'article montre comment Internet peut aggraver une crise en faussant le débat, en diffusant des images trompeuses de la réalité et en jetant de l'huile sur le feu grâce à la publication de messages haineux et à la promotion de la violence.
- On mentionne également la difficulté de surveiller et de régir le contenu des carnets Web et des forums en ligne.

***Weekend Australian* : « Militant website shows attack tactics »** – de correspondants à Jakarta, 19 novembre 2005 (http://www.theaustralian.news.com.au/common/story_page/ 0,5744,17294708%255E170 2,00.html)

- Article sur la façon dont la Jemaah Islamiyah utilise des sites Web pour donner des directives à ses militants sur des attentats, des cibles et des tactiques terroristes.
- Un site Web indique aux militants comment attaquer des étrangers à Jakarta, fournit les cartes de plusieurs lieux publics et donne des détails sur la valeur de ces lieux comme cibles ainsi que sur des voies de sortie utiles.

***New York Times* : « A T-Shirt-and-Dagger Operation »** – de Scott Shane, 23 novembre 2005 (http://www.globalsecurity.org/org/news/2005/051113-osint.htm)

- Article sur les mesures prises par l'appareil du renseignement américain pour intégrer l'analyse des renseignements de sources ouvertes au système de renseignement américain.
- Les renseignements de sources ouvertes sont un moyen économique de tenter de comprendre le militantisme islamiste qui anime al-Qaïda, car ils rassemblent non seulement les perspectives de la presse et de la télévision à l'étranger, mais aussi celles d'une vaste gamme de sources sur Internet et d'autres sources particulières (musique, slogans sur des t-shirts, etc.)
- L'article décrit cette nouvelle façon de recueillir une quantité infinie de renseignements grâce à la navigation et à la recherche en ligne.

***Associated Press* : « FBI: Internet-Based Attacks Unlikely »** – de Mark Sherman, 7 décembre 2005 (http://www.usatoday.com/tech/news/computersecurity/2005-12-07-fbi-terrorism-web_x.htm?csp=34)

- Dans cet article, une citation de Louis Reigel, directeur adjoint du FBI aux États-Unis, soutient qu'al-Qaïda et les réseaux terroristes qui y sont affiliés sont incapables de monter des cyberattaques pouvant endommager les infrastructures essentielles des États-Unis.
- Tout en reconnaissant que les groupes terroristes font preuve d'une maîtrise technique et d'une complexité croissantes, les experts du FBI croient qu'ils ne sont pas encore en mesure de monter une campagne cyberterroriste d'envergure.
- L'article mentionne aussi que les terroristes n'utilisent que rarement la stéganographie (dissimulation d'un message en format texte dans un autre type de fichier, généralement une image).

ARTICLES SCIENTIFIQUES, ARTICLES DE REVUES, RAPPORTS, FORUMS ÉLECTRONIQUES ET DOCUMENTS DE CONFÉRENCE (par ordre chronologique)

AIVD : *Annual Report 2004: General intelligence and security service* – 2004 (http://www.fas.org/irp/world/netherlands/aivd2004-eng.pdf)

- Rapport volumineux, produit par le Service général de renseignement et de sécurité des Pays-Bas, qui aborde de nombreux enjeux et faits nouveaux liés à la sécurité et au renseignement.
- Une partie du rapport porte exclusivement sur le terrorisme et fait ressortir non seulement les problèmes et événements les plus récents, mais aussi les activités de divers groupes précis et reconnaissables qui pourraient mener leurs activités aux Pays-Bas ou en Europe.
- Le rapport souligne l'importance du rôle d'Internet, particulièrement dans la radicalisation de certaines parties de la communauté musulmane au pays grâce à la dawa « virtuelle » (sermons radicaux en ligne) et de plus en plus grâce aux salles de clavardage sans surveillance. Les échanges animés de vues islamiques sur l'autoroute électronique (un processus autodirigé) sont de plus en plus fréquents par rapport à l'endoctrinement personnel effectué par les prédicateurs.
- Le rapport mentionne aussi brièvement les efforts déployés par l'AIVD pour surveiller les cas de cyberattaque ainsi que pour recueillir et réunir les données et les rapports sur ces cas.

United States Institute of Peace : « Special Report: www.terror.net - How Modern Terrorism Uses the Internet » – de Gabriel Weimann, rapport spécial n° 116, mars 2004 (www.usip.org)

- La source la plus directe et la plus utile à consulter pour comprendre comment les organisations terroristes contemporaines utilisent Internet.
- Le rapport explique le phénomène du terrorisme moderne et d'Internet. Il donne notamment un aperçu de la création d'Internet, de sa raison d'être initiale, de son évolution et de l'attrait qu'il exerce sur les organisations terroristes.
- Il donne également un aperçu utile de certains sites Web terroristes actuels classés par lieu géographique

et assortis d'une explication sur leur contenu et leur public cible.

- La majeure partie du rapport porte sur les différentes utilités d'Internet pour les terroristes, divisées en plusieurs catégories comprenant des analyses détaillées : guerre psychologique; publicité et propagande; exploration des données; collecte de fonds; recrutement et mobilisation; maillage; partage de l'information; planification et coordination.

Sommet international sur la démocratie, la sécurité et le terrorisme : « Madrid – Terrorism, the Internet and Democracy » – du 8 au 11 mars 2005 (http://english.safe-democracy.org/index.html – en anglais et en espagnol)

- Excellent site Web sur le sommet international sur la démocratie, la sécurité et le terrorisme tenu à Madrid en mars 2005.
- Il examine les multiples facettes du terrorisme, de même que leur incidence sur l'attitude et les réactions des démocraties occidentales en matière de sécurité.
- Un groupe de travail spécial analyse la relation entre le terrorisme et Internet ainsi que les répercussions des stratégies en matière de sécurité sur les institutions démocratiques.
- On soutient qu'Internet est une assise de la démocratie du XXIe siècle en raison de leurs valeurs fondamentales très semblables, l'ouverture et la liberté. Il avertit également qu'une réglementation et une restriction excessives de l'usage d'Internet dans les sociétés démocratiques pourraient menacer les valeurs mêmes qu'elles cherchent à protéger.
- On y fournit des conclusions et des recommandations, entre autres : accepter Internet comme une assise de la démocratie du XXIe siècle et l'adopter comme outil de lutte contre le terrorisme; reconnaître l'importance de l'infrastructure d'Internet et la consolider pour la protéger des attaques; augmenter l'accessibilité d'Internet dans le monde (combler le « fossé numérique »); protéger le droit à la liberté d'expression dans tous les forums; résister aux tentatives d'établir un système de gouvernance internationale d'Internet.
- Dans l'ensemble, le site Web est une excellente source d'informations sur les courants terroristes dans le monde et jette les bases d'un dialogue ouvert et éclairé sur la question.

***International Journal of Intelligence and Counter-Intelligence* : « The Intelligence Services' Struggle Against al-Qaeda Propaganda »** – de Javier Jordan, Manuel R. Torres et Nicola Harsburgh, volume 18, numéro 1, printemps 2005

- Article faisant ressortir l'attention que les campagnes antiterroristes doivent porter aux stratégies qui apportent un complément aux attentats terroristes et qui, en conséquence, font en sorte qu'un réseau terroriste survit ou disparaît, notamment des aspects de la propagande et de la gestion de la perception qui sont actuellement amplifiés et transmis à un vaste public grâce aux technologies de l'information et des télécommunications modernes.
- Les autorités et les experts doivent commencer à prêter davantage attention à la lutte qui fait rage sur Internet, la « guerre de l'information ».
- Les auteurs prétendent que même si l'idéologie radicale qui anime le groupe tire son origine d'une forme d'intolérance primitive et extrémiste, son organisation et ses méthodes témoignent d'une grande

adaptation aux nouvelles réalités de la mondialisation et de la révolution de l'information.

- Bien que la collecte de fonds, l'entraînement et l'acquisition d'armes et d'explosifs demeurent des activités fondamentales, de l'avis des auteurs, la guerre de l'information et de la propagande est le véritable pilier sur lequel reposent la structure et la continuité de l'organisation, d'où l'importance vitale d'un outil de communication moderne comme Internet.

- Une fois créé et diffusé le message du mouvement jihadiste mondial, qui favorise une compréhension universelle, il est plus probable que des alliances transnationales se forment entre des régions dispersées, toujours grâce à la révolution de l'information. Ainsi, les réseaux du mouvement s'organisent en nébuleuse (sans hiérarchie claire, donc impossible à décapiter), ce qui donne lieu à un « terrorisme franchisé », au maintien et à l'élargissement des appuis à l'échelle sociale, à la possibilité du terrorisme amateur et à la perpétuation du discours du jihad moderne.

OTAN : Atelier de recherche avancée mixte du STS-CNAD, du 8 au 11 avril 2005 : « Terrorism and the Use of Communications – Countering the Terrorist Information Cycle » – de Bruce Jones, président, 3 mai 2005

- Excellente source qui examine la nature et l'étendue actuelles des communications terroristes, de même que leurs composantes opérationnelles, techniques et culturelles étroitement reliées, l'image qu'en ont les gouvernements occidentaux, les réactions de ces derniers ainsi que les stratégies possibles de prévention, de contre-mesure, d'interdiction et de perturbation.

- Le document dresse la liste des constatations de l'atelier, qui portent notamment sur l'utilisation d'Internet pour la préparation, le conditionnement et le recrutement, la communication d'« ordres de combat », le partage d'informations techniques et tactiques et d'informations sur les cibles, les points faibles des forces armées et des forces de l'ordre et le manque de linguistes et de spécialistes de la technologie de l'information judiciaire compétents (surtout de personnes spécialisées dans ces deux domaines).

- Il contient également des conclusions et des recommandations concernant notamment : la nécessité de faire adopter des procédés judiciaires à l'échelle internationale; la collaboration et la coordination internationale des organismes d'application de la loi et des services de renseignements; la formation de professionnels occidentaux en linguistique et en technologie de l'information judiciaire et l'exploitation de leurs aptitudes; les approches et stratégies d'engagement directes et valables auprès de la population musulmane dans le monde; le piratage technique de sites indésirables; l'analyse de groupes qui utilisent Internet à des fins criminelles pour repérer les méthodes et les synergies applicables; une éducation efficace en matière de sécurité pour favoriser une couverture médiatique plus avisée des enjeux et des événements et pour sensibiliser le public.

Terrorism Research Centre : « Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy » – article de Dorothy E. Denning parrainé par l'Institut Nautilus, 6 juin 2005 (http://www.terrorism.com/modules.php?op=modload&name=News&file= article&sid=12110)

- Précieux article scientifique qui analyse l'utilisation stratégique d'Internet et son rôle dans la réalisation des objectifs liés à la politique étrangère.

- L'auteure examine les usages d'Internet et les classe dans trois grandes catégories qui se chevauchent : l'activisme, le cyberactivisme et le cyberterrorisme. Elle conclut que les groupes qui emploient des stratégies liées à la première catégorie sont plus susceptibles d'atteindre leurs objectifs

en matière de politique étrangère que ceux qui emploient les stratégies liées aux deux autres catégories.

- L'article offre un cadre de référence très important pour comprendre les diverses méthodes et tactiques que les groupes et les personnes utilisent pour tirer parti d'Internet, de même que pour comprendre la relation entre le terrorisme et Internet.

***Terrorism Focus* : « Al-Qaeda's Next Generation: Less Visible and More Lethal »** – de Michael Scheuer, volume 2, numéro 18, 4 octobre 2005 (http://jamestown.org/terrorism/news/ article.php?issue_id=3481)

- Article examinant la nouvelle génération d'agents d'al-Qaïda, qui s'adaptent mieux que leurs prédécesseurs aux outils modernes, plus particulièrement les outils de communication et les armes, qui en apprennent le maniement plus facilement et qui les utilisent avec plus d'habileté pour réaliser leurs objectifs.

- Leur ferveur intense est le produit d'un monde où Internet et la télévision par satellite constituent un important débouché pour la lutte des musulmans partout dans le monde, car ils donnent du courage en projetant une identité musulmane commune et la certitude du rôle que joue l'Occident (dirigé par les États-Unis) dans l'oppression de la cause musulmane.

- Leur professionnalisme s'explique par le fait que beaucoup d'entre eux proviennent de la classe moyenne ou de la bourgeoisie, ce qui leur a permis d'acquérir des aptitudes et des connaissances concernant la plupart des technologies de l'information et des communications actuelles.

- L'auteur croit que l'Occident ne comprend pas al-Qaïda comme il comprenait l'Union soviétique en tant qu'adversaire et qu'il doit vaincre ce malaise institutionnel s'il veut venir à bout du défi que représente la nouvelle génération de moudjahidin.

Jamestown Foundation : « Technology and Security Discussions of the Jihadist Forums: Producing a More Savvy Next Generation » – 11 octobre 2005

- Rapport de la Jamestown Foundation concernant les discussions sur la technologie et la sécurité dans les forums électroniques sur le jihad et l'utilisation de ces forums pour créer une nouvelle génération plus compétente de jihadistes.

- Le rapport examine l'importance des nouveaux forums en ligne comme voies de communication populaires où des personnes sans lien avec un groupe particulier peuvent afficher un document ou un manuel de leur cru que les cellules terroristes peuvent ensuite utiliser pour établir leurs procédures.

- Fait notable : l'accent mis sur le « savoir-faire ». La diffusion de directives de sécurité de base sur le piratage et l'utilisation de cellulaires augmente l'efficacité des jihadistes en herbe, qui commettent ainsi moins de bévues en matière de sécurité et laissent moins de pistes aux autorités et aux services de renseignements.

- Le rapport prend l'exemple de deux récents manuels affichés dans deux forums électroniques (www.minbarislam.com/forum et www.al-farouq/vb) où les documents de base conviviaux circulent rapidement auprès d'un grand nombre d'utilisateurs, ce qui en augmente la valeur.

- Il en résulte la possibilité que se crée une nouvelle génération de jihadistes en herbe ayant des aptitudes techniques et tactiques de plus en plus grandes ainsi que l'assurance et la volonté nécessaires pour mettre à l'essai leurs nouvelles habiletés.

Organisation pour la sécurité et la coopération en Europe : « Expert Workshop on Combating the Use of the Internet for Terrorist Purposes » – atelier présenté par le Bureau du représentant pour la liberté des médias et le Bureau des institutions démocratiques et des droits de l'homme, 13 et 14 octobre 2005 (http://www.osce.org/documents/odihr/2005/10/ 16705_en.pdf)

- Atelier qui reconnaît la menace que représentent l'augmentation du nombre de terroristes et l'utilisation accrue d'Internet pour diffuser des documents qui favorisent les actes de terrorisme, les virements de fonds, de même que la communication, la planification et la coordination d'activités et d'attentats.
- L'objectif de l'atelier et du document connexe consiste à aborder ces problèmes tout en faisant ressortir le danger qui menace certains droits importants en matière de vie privée, de liberté des médias et de liberté d'expression lorsque les autorités se mettent à surveiller et à régir la documentation publiée sur le Web, les virements bancaires et la correspondance privée sur Internet.

Jamestown Foundation : « An Online 'University' for Jihad » – de Stephen Ulph, *Terrorism Focus*, volume 2, numéro 19, 18 octobre 2005 (http://jamestown.org/terrorism/news/ article.php?articleid=2369807)

- Article soutenant que la présence d'al-al-Qaïda sur Internet s'est accentuée au point de devenir un phénomène culturel et militaire permanent.
- Un message affiché le 7 octobre par l'« émir adjoint » du Front islamique mondial de l'information dans un forum sur le jihad (www.al-farouq.com) annonçait la création d'une « université d'études sur le jihad d'al-Qaïda » et proclamait qu'al-Qaïda est une organisation, un État et une université.
- Selon l'auteur, le but est de tirer parti de l'infrastructure d'Internet pour créer une université décentralisée, sans frontières géographiques et omniprésente qui offre un entraînement militaire et enseigne des principes idéologiques et moraux stricts.
- Les soi-disant « diplômés » de cette université virtuelle ont étudié chacune de ses « matières » pour devenir des spécialistes du « jihad électronique », du « jihad des médias » et du « jihad spirituel et financier ».

Council on Foreign Relations : « Terrorism: Questions & Answers – How do terrorist organizations use the internet? » – article électronique consulté le 26 novembre 2005 (http://cfrterrorism.org/home/)

- Aperçu concis et utile de la façon dont les réseaux terroristes utilisent ou peuvent utiliser Internet pour soutenir ou mener des opérations.
- On reconnaît que le nombre de sites Web liés au terrorisme a fait un bond immense pendant la dernière décennie (de moins de 100 à plus de 4 000).
- Les terroristes se servent d'Internet pour donner des ordres, planifier des attentats et virer des fonds, protégés par de nombreux babillards électroniques et salles de clavardage.
- Les sites des terroristes sont aussi des lieux d'entraînement virtuels qui contiennent des tutoriels et des manuels sur des sujets divers, qui diffusent de la propagande et qui servent à collecter des fonds et à recruter de nouveaux membres.
- Internet peut également être le théâtre d'actes de cyberterrorisme contre des infrastructures énergétiques, de transport ou de sécurité essentielles.
- De plus, les services de renseignements peuvent se servir des sites Web des terroristes pour surveiller

leurs activités, leurs communications et leurs méthodes ainsi que pour recueillir de précieux indices sur les attentats à venir.

Intelligence and Terrorism Information Center at the Center for Special Studies : « The Palestinian Islam Jihad Internet infrastructure and its Internet Webhosts » – 28 décembre 2005 (http://www.intelligence.org.il/eng/eng_n/internet_e1205.htm)

- Évaluation de cas intéressants sur la présence d'une organisation terroriste précise dans Internet.
- Elle décrit cinq sites Web qui contiennent et diffusent des documents en faveur de la cause et de l'idéologie du jihad palestinien. Les descriptions comprennent une analyse du contenu, les noms des personnes qui appuient le site ou qui y publient des articles, des adresses URL, des adresses IP, ainsi que les noms et adresses des fournisseurs des services d'hébergement et des administrateurs du site, lorsque ces derniers sont connus.

The Jamestown Foundation : « Internet Mujahideen Intensify Research on US Economic Targets » – de Stephen Ulf, 18 janvier 2006 (http://www.jamestown.org/ news_details.php?news_id=155)

- Article sur l'intérêt persistant des réseaux terroristes pour les cibles économiques américaines, en particulier l'infrastructure énergétique aux États-Unis et dans d'autres pays, dans le cadre de leur grande stratégie consistant à « affaiblir jusqu'à la ruine ».
- Le message « Al-Qaeda's Battle is an Economic Battle, Not a Military One » d'Abu Musab al-Najdi, affiché en octobre dernier sur le forum Minbar Suriya al-Islami, soulignait cette stratégie et rajoutait aux cibles le Koweït, l'Arabie saoudite et le Venezuela (www.nnuu.org.vb). Le message était également assorti d'adresses URL menant à des informations, des cartes et des images portant sur des réseaux de distribution, des centres de transport et des dépôts d'approvisionnement en carburant militaire.
- Les experts sont préoccupés par la quantité d'informations de recherche circulées par de tels forums, qui demandent une plus grande participation des lecteurs du forum qui se spécialisent dans les domaines du génie pétrochimique, des pompes et des réseaux de distribution, de même que des livres ou des documents en format PDF sur ces sujets.
- L'article fait ressortir deux aspects majeurs de l'importance que revêt Internet pour le mouvement jihadiste mondial. Premièrement, il souligne la vitesse des communications et les moyens que les partisans du jihad dispersés dans le monde peuvent consacrer à un seul projet. Deuxièmement, il démontre l'ampleur dans laquelle le Web est devenu un milieu d'exploration des données qui donne instantanément accès, non seulement à des données de recherche scientifique, mais aussi à des informations sur les infrastructures sensibles des services publics et des réseaux de transport et de distribution, de même qu'aux perceptions des points faibles de ces infrastructures et de la menace qui pèse sur elles.