CONSERVATOIRE NATIONAL DES ARTS ET METIERS

‘‘Le financement du terrorisme et des opérations de déstabilisation psychologique.”

Module : Mémoire Sciences Criminelles – Criminologie

Module Leader : Dr Philippe Baumard

Etudiant : PAPADOPOULOS ANDREAS (Ecole de Guerre)

No (INE): 0G5DRRE1B04

No (Siscol): 100210321

Paris,31 Mai-2018

Table of Contents

List of Figures:

1. Introduction

C’est indisputable que le terrorisme a changé ou plutôt « évolué » au cours des dernières décennies, concernant les types d'attaques que les terroristes mènent aussi bien que la façon dont ils les financent. Nous en témoignons le processus de transition de la guerre traditionnelle où le champ de bataille est remplacé par le cyberespace, les opérations militaires par des cyber-opérations et tout cela dans le nouveau cadre de **cyber guerre**.

Au niveau du groupe, les organisations terroristes utilisent le parrainage d'États, le soutien de la diaspora, des organismes de bienfaisance, des financiers indépendants, des organisations de façade ou elles vendent leur formation et leur expertise à d'autres groupes et elles utilisent également le crime organisé pour se financer. Au niveau de la cellule, effectuer des opérations n’est pas tellement coûteux. Des délits mineurs ou même un travail à temps plein peuvent aider à couvrir les coûts d'une attaque terroriste.

La montée des formes de paiement qui sont indépendantes des monnaies gouvernementales émises et contrôlées et qui peuvent être échangées de manière hautement anonyme, instantanément transférées et utilisées pour des transactions légales et illégales représentent un nouveau moyen de blanchir de l'argent destiné à financer les opérations des organisations terroristes. Comprendre cette nouvelle forme de «monnaie» indépendant du gouvernement est important pour ceux qui sont impliqués dans le domaine du combat contre le terrorisme.

En découvrant ces réseaux qui fournissent un soutien monétaire et logistique, on pourrait perturber les réseaux terroristes. En plus de cela, le cyberespace est une technologie transformatrice que les terroristes exploitent pour propager la propagande et radicaliser de nouvelles recrues. Les groupes de cyber terroristes mènent une campagne médiatique moderne et sophistiquée centrée sur le réseautage social en ligne.

Notre choix d’étudier ce phénomène est basé sur le fait que notre société vit actuellement dans un état chaotique plein de terreur à cause du cyber terrorisme. Il nous semble qu’il ajoute un énorme chalenge à la science de la criminologie aussi bien

qu’à l’informatique. En effet c’est un problème qui fait couler beaucoup d’encre sans pour autant donner des réponses concrètes. D’ailleurs, c’est pour cette raison que ce phénomène a attiré notre attention pour le traiter.

Tout d’abord, en tant que citoyen actif et ensuite en tant que militaire, nous nous sommes posé des questions au sujet du cyber terrorisme concernant, d’un côté, les moyens dont les terroristes font usage pour accomplir leurs missions meurtrières et de l’autre côté, les raisons pour lesquelles les différents gouvernements, la société internationale et les peuples en général, ont échoué jusqu’à présent à confronter efficacement ces groupes terroristes. En fait, ces derniers, se trouvent toujours un pas en avance et le reste du monde les suit. Nous nous sommes, donc, plongé dans la recherche des réponses qui feront le sujet de notre mémoire.

Dès le départ, nous étions conscients de la complexité et de la difficulté que présente un tel sujet. C’est d’ailleurs pour cela que nous nous sommes tenus les pieds bien à terre sachant que nous ne pourrions ni découvrir la recette qui aurait éliminé le problème en question, ni produire une littérature scientifique toute neuve à ces propos. Néanmoins, le recueil des positions prises par d’autres chercheurs, souvent contradictoires et l’étude des cas variés mènent à des réflexions plus approfondies et à la meilleure compréhension de vraies dimensions du phénomène en question.

En effet, dans cet essai nous allons essayer de présenter une image plus claire et nette du **cyber terrorisme** qui peut être considéré comme le fléau de notre ère mais sans pour autant qu’il soit clairement défini. En fait, étant donné que le terme du terrorisme est défini différemment par chaque gouvernement ou encore des institutions du même pays selon leur législation, il est évident qu’il n’y ait pas de définition unique pour définir le cyber terrorisme.

Cet essai vise à expliquer les bases scientifiques de l'accès, des conditions et de l'utilisation du cyberespace par les terroristes dans la réalisation de toutes leurs activités cycliques, allant des appels à l'acceptation de l'idéologie jusqu'à l'accomplissement d'un acte terroriste.

Dans une première partie donc, nous allons étudier les différentes formes de financement des activités terroristes et par la suite nous allons mettre l'accent sur

l'utilisation du cyberespace dans la collecte des modèles de transfert de fonds de la source aux terroristes ainsi que sur leur manière d'utiliser ces fonds pour les activités cycliques nécessaires. En même temps, nous essaierons d'expliquer le paradoxe du développement des techniques et de la technologie et nous examinerons comment les terroristes utilisent Internet dans le cadre de leurs stratégies médiatiques plus générales. Ensuite, nous allons étudier les opérations terroristes qui visent à la déstabilisation psychologique des citoyens et faire des réflexions personnelles.

Dans cette première partie, nous allons, donc, présenter la question centrale, expliquer le titre et mettre en perspective la spécificité du sujet. De plus, nous allons formuler quelques hypothèses de départ concernant les résultats envisagés de cet essai.

Dans la deuxième partie, nous allons citer des références fondamentales et en faire une lecture critique afin que nous guidions le lecteur à suivre le chemin de notre raisonnement en employant une méthode historique. En plus, nous allons expliquer notre démarche méthodologique et justifier le choix de la méthodologie et de l'approche retenues. Par la suite, nous allons présenter les résultats des recherches d'autres chercheurs concernant la question soulevée. Enfin, nous allons essayer d'indiquer la contribution de ceux derniers à la meilleure compréhension du problème.

Dans la conclusion, nous indiquerons les perspectives et les limites de cette recherche et nous allons faire des réflexions sans prétendre pouvoir donner la réponse au problème du cyber terrorisme.

2. Méthodologie

2.1 Introduction

Pour effectuer une recherche, il est indispensable d'appliquer une méthodologie afin d'examiner la problématique en question. La méthodologie n'est qu'un outil qui conduit à la compréhension ainsi qu'à l'approfondissement du sujet. Il nous a paru que la méthodologie la plus appropriée pour mener notre enquête était celle de Veal 2001.

La méthodologie en question, propose les étapes qui sont citées ci-dessous dans le modèle circulaire du processus de recherche de [1]Veal (2011) :

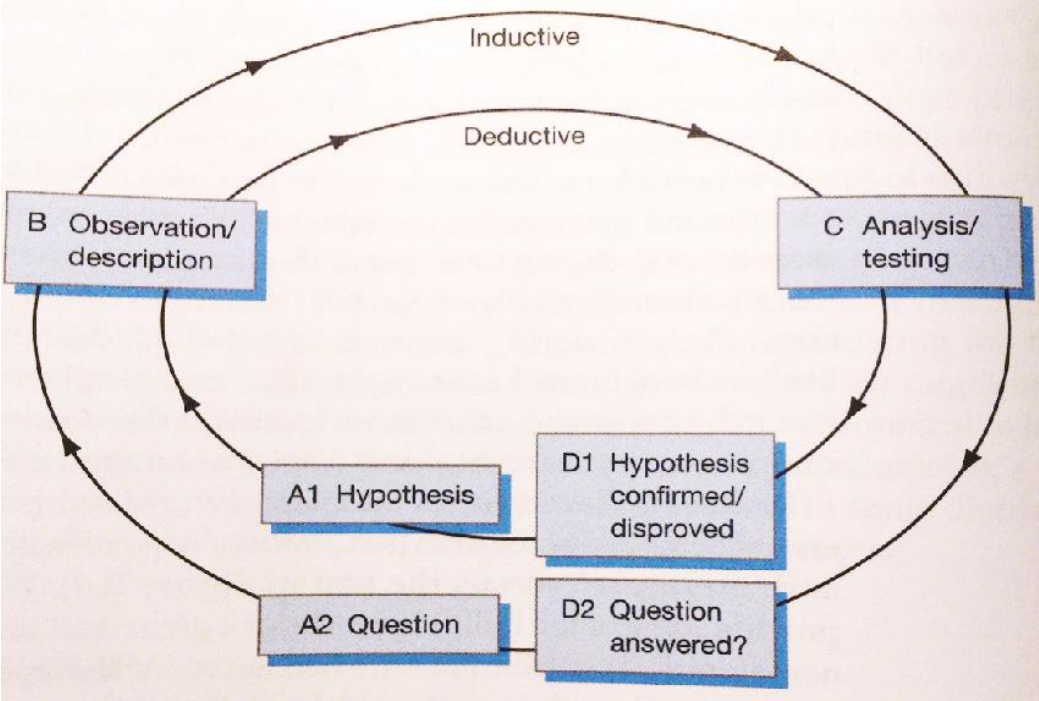

Figure 2. Circular model of the research process (Veal 2011:40)

Selon Veal, il y a deux méthodes différentes à appliquer dans une recherche : la Déductive et l'Inductive. Pour qu'une hypothèse puisse être vérifiée, la déduction est un moyen qui aide à équilibrer la perspective et les preuves existantes de la réflexion parue dans la littérature. Le processus de recherche déductif commence au point d'hypothèse A1 et fait des suggestions concernant la manière d'accomplir une tâche. Par la suite, il passe à l'étape B et donc, à la Description / Observation, qui est primordial afin que nous puissions découvrir la preuve autour de nous. Alors, d'un point de vue critique nous nous concentrons sur la manière de comprendre les résultats, les dispositions prises et les circonstances observées. L'étape C analyse / test, rejette ou approuve l'hypothèse D1. Alternativement, la méthode inductive commence par une description / observation B ou une question A2. Ensuite, elle passe à l'étape C, celle d'analyse / test qui conclut à l'échec ou le succès, c'est - à - dire à répondre ou pas à la question A2. Il est bien connu qu'avant la description et l'analyse c'est essentiel de rassembler les

[1] Veal, Anthony James, (2011). *Research methods for leisure and tourism: a practical guide.* Harlow: Financial Times Prentice Hall

informations et les preuves sur le sujet en question afin de pouvoir faire avancer les théories et les hypothèses qui sont en partie déductive et inductive. Pour cette recherche nous allons suivre l'approche inductive car elle est moins rigide. Pour les questions / observations auxquelles il faut répondre, les buts et objectifs doivent être utilisés.

Dans cette étude, nous allons aborder la question en examinant la littérature et en établissant un modèle théorique explicatif qui s'adresse à la question. L'examen et les définitions aident le lecteur à comprendre le fonctionnement du cyberterrorisme sur Internet. Bien que les spécialistes des sciences sociales aient beaucoup fait pour découvrir le fonctionnement interne de ces organisations clandestines, nous devons encore comprendre pleinement la relation entre l'État, les groupes criminels-terroristes et le développement politico-économique.

2.2 Développement d'instruments

Une définition qui est opérationnelle décrit un concept en ce qui concerne ses caractéristiques observables et mesurables. Ceci est fait en examinant comment les concepts peuvent être observés dans la pratique réelle ([2]Frey H. Christopher et al., 1999). L'objectif principal de cette étude était de faire ressortir les antécédents de la lutte contre la cyberterrorisme, non pas du point de vue des décideurs politiques ou du gouvernement, mais de la perception des cyberterroristes eux-mêmes. Cela a été fait avec l'utilisation de quatre principes principaux; l'effort requis pour commettre le cyberterrorisme, la quantité de risques encourus, les excuses qui peuvent être avancées et les avantages attendus de la perpétration du cyberterrorisme. Cette étude testera également les perceptions et les raisons des valeurs, en examinant certains attributs démographiques.

2.3 Base philosophique de l'étude

Les chiffres devraient augmenter au cours des prochaines années en raison du fait que les nations adoptent l'Internet et saisissent les opportunités offertes par ce secteur en

[2] Frey H. Christopher, Cullen**,** Alison C., (1999). "*Probabilistic Techniques in Exposure Assessment."* A Handbook for Dealing with Variability and Uncertainty in Models and Inputs. Springer Science & Business Media.

termes d'entrepreneuriat et de création d'entreprises. Bien que la croissance économique puisse être bien accueillie, il est important de garder à l'esprit que toute croissance générée par le commerce électronique comporte des risques associés aux cyberattaques. Une coopération étroite entre les gouvernements, les universités et les entreprises du monde entier a renforcé notre défense contre le cyberterrorisme en réponse à la hausse du taux de terrorisme. Comment le blanchiment d'argent et d'autres fraudes informatiques utilisant la plate-forme Internet peuvent-ils contribuer au financement du terrorisme et aux opérations de déstabilisation psychologique?

De même, cette recherche remarque le manque de sensibilisation et de cadre juridique, ainsi que d'autres facteurs qui ont contribué à une augmentation des Cyberterroristes. Ces activités sapent une économie déjà fragile, engendrant une énorme perte de revenus et une atmosphère de méfiance universelle. En outre, ils permettent aux terroristes de lancer des attaques et d'opérer dans un environnement cybernétique sûr, car les pays en développement n'ont pas d'infrastructure réglementaire en place pour les traiter.

En outre, cette étude indique que les internautes ont été victimes d'escroqueries et qu'une personne sur cinq est tombée dans le piège de courriels frauduleux ou de sites Web liés à ces activités douteuses. Les experts estiment que le cyberterrorisme est désormais la première menace stratégique, après avoir dépassé les chiffres pour les importations de drogues et l'immigration clandestine. De plus, les activités d'espionnage en ligne constituent une menace croissante. Plusieurs dizaines de milliards de dollars de secrets commerciaux, de nouvelles technologies et de propriété intellectuelle sont déversés chaque année sur les systèmes informatiques des organismes gouvernementaux, des sociétés et des instituts de recherche.

Internet change la réflexion sur notre futur. Le développement du commerce de détail est un bon exemple. De plus en plus de magasins ferment leurs portes alors que les ventes sur Internet continuent d'augmenter et que les nouvelles technologies sont au cœur des tendances de consommation. Pourtant les consommateurs continuent à exiger un excellent service. Ils veulent être impliqués, mais à distance, et d'une certaine façon, cela leur permet de contrôler la situation. Evidemment, ils nécessitent une certaine compréhension des avancées technologiques, ils achètent en ligne les produits

essentiels, mais ils veulent aussi se retrouver dans des environnements appropriés lorsqu'ils font des «achats uniques» et saisissent des «opportunités uniques». Il est donc essentiel que les nouvelles technologies surpassent ces tendances afin de garantir la satisfaction de ces clients virtuels.

3. Définition du sujet

Nous avons déjà mentionné la raison pour laquelle il est difficile et compliqué à définir le terme du Cyber terrorisme. Pourtant, il nous paraît indispensable de porter quelques clarifications qui pourraient contribuer à mieux comprendre le phénomène en question.

En premier lieu, il est important de distinguer les termes Cyber terrorisme, piratage et «hacktivisme». Le terme «piratage» désigne des activités menées en ligne, visant à révéler, manipuler ou exploiter des vulnérabilités des systèmes et d'autres logiciels. La plupart des pirates n'ont pas d'objectifs politiques et ils se concentrent sur la création de programmes qui exposent les failles de sécurité des logiciels. Leurs efforts dans ce sens ont parfois embarrassé les entreprises, mais ont également alerté le public et les professionnels de la sécurité sur les principales failles de sécurité logicielle. De plus, bien que les hackers soient connus pour endommager les systèmes, perturber le commerce électronique et forcer les sites Web hors ligne, la grande majorité des pirates n'ont pas les compétences et les connaissances nécessaires pour infliger des dommages sérieux, et ceux qui possèdent ces compétences ne s'intéressent pas à endommager gravement des logiciels. (Denning Dorothy, 2001).

Le « hacktivisme » est un terme inventé par des érudits pour décrire le piratage avec une composante d'activisme politique. Bien que l'hacktivisme soit politiquement motivé, il ne constitue pas un cyber terrorisme. Les hacktivistes veulent protester et perturber. Ils ne veulent pas tuer, mutiler ou terroriser. Cependant, l'hacktivisme met en évidence la menace du cyber terrorisme: les individus sans contrainte morale peuvent utiliser des méthodes similaires à celles développées par les hackers pour faire des ravages. La ligne entre le cyber terrorisme et le piratage ou le hacktivisme peut être floue, surtout si les groupes terroristes recrutent ou embauchent des hacktivistes ou si les hacktivistes décident d'intensifier leurs actions en attaquant les systèmes qui exploitent les éléments

critiques de l'infrastructure nationale, tels que les réseaux électriques et les services d'urgences.[3] (Weimann Gabriel, 2005a, 136-37).

4. Cyber terrorisme, technologie et Internet

Sûrement, les types de violence que l'on décrit généralement comme du cyber terrorisme existaient bien avant Internet mais, comme tout le monde le sait, Internet a été une technologie extrêmement transformatrice. Environ une personne sur quatre sur Terre dispose aujourd'hui d'un smartphone qui permet une connexion instantanée à Internet ([4]Statista 2017). Facebook compte à lui seul près de 1,5 milliard d'utilisateurs actifs, soit près de 20% de la population mondiale. Ce n'est donc pas une surprise qu'Internet soit adopté par les cybers terroristes pour les mêmes raisons que par d'autres organisations, notamment pour sa capacité à étendre sa portée et son influence (Weimann Gabriel, 2015). Si le cyber terrorisme est perçu comme une forme de violence communicative et que la diffusion de la propagande est donc au cœur de cyber criminalité, alors une présence en ligne est logiquement encore plus vitale pour les cybers terroristes que bien d'autres organisations. Des études récentes ont identifié des milliers de sites ouvertement jihadistes fonctionnant sur Internet aujourd'hui ([5]Denning Dorothy, 2011). L'État Islamique (IS) a été particulièrement actif et a réussi à recruter des combattants étrangers, notamment d'Europe et d'Amérique, en utilisant Twitter, YouTube, Diaspora et d'autres réseaux sociaux en ligne.

Internet offre des avantages évidents et uniques par rapport aux médias plus anciens tels que la radio et la télévision. Pratiquement n'importe qui peut créer un site Web facilement et à peu de frais pour publier de la littérature, des images, des vidéos et des logiciels. Le message peut être complètement contrôlé par l'auteur-éditeur et ne dépend pas des journalistes ou de l'approbation ou de la médiation du gouvernement (les stations de télévision sont exploitées par l'Etat dans de nombreux pays). Cependant, plus importante est l'opportunité présentée par les nouvelles technologies des médias pour l'interactivité bidirectionnelle à travers les forums, les forums de discussion, le

[3] Weimann Gabriel. (2005a)."Cyberterrorism: The Sum of All Fears?" *Studies in Conflict & Terrorism 28* (2): p. 136-37.
[4] Statista, (2017). "Nombre d'utilisateurs de Smartphone dans le monde de 2014 à 2020 (en millions)," Statista. Disponible à : http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[5] Dorothy Denning, (2011). «Terror's Web: Comment Internet transforme le terrorisme», dans Yvonne Jewkes et Majid Yar, éd., Handbook of Internet Crime (Abingdon: Routledge, 2011), p. 194-213.

courrier électronique, les textes. Les cyber terroristes peuvent se connecter directement avec des publics divers et ces publics, à leur tour, peuvent devenir des participants actifs à une conversation en cours. Un sens de communauté virtuelle peut donc être favorisé qui n'est souvent pas possible avec des formes, plus traditionnelles, de médias audiovisuels comme la radio et la télévision.

Les cybers terroristes reconnaissent qu'Internet est un outil puissant à utiliser délibérément et tactiquement pour faire avancer leurs objectifs stratégiques. Afin que nous puissions comprendre la propagande en ligne et la radicalisation, Internet devrait être examiné dans un contexte plus large, celui d'autres outils employés dans les stratégies médiatiques des terroristes.

5. Première Partie

5.1 Nouveau modus operandi - source de fonds

La structure modifiée des organisations du cyber terrorisme a contribué à trouver de nouvelles façons de financer leurs opérations. La nouvelle théorie prédit un financement indépendant des cellules. La direction centrale des organisations a perturbé le flux de fonds vers les cellules pour des raisons de sécurité. Dans une telle situation, les membres des cellules étaient obligés de fournir eux-mêmes des fonds. Afin de ne pas être identifiés et de ne pas attirer l'attention sur leur comportement, les membres de la cellule devaient s'engager dans la vie sociale ou mener des activités criminelles pour acquérir de l'argent. Ainsi, les membres ont commencé à être employés dans les entreprises ou même à ouvrir leurs propres entreprises. De cette manière, ils bénéficient de tous les avantages et produits de la mondialisation. Ils peuvent ouvrir un compte bancaire, obtenir des crédits, avoir des cartes de crédit, réaliser des transactions, etc. Les membres qui n'avaient pas un statut significatif dans les sociétés, ont mené des activités criminelles dans le même but ; obtenir des fonds.

Internet est un bon outil à l’aide duquel on peut gagner de l’argent de manière légale ou illégale. En outre, le vol d'identité, la falsification de signatures, le vol et l'abus de cartes de crédit font partie des moyens pour obtenir des sommes considérables.

5.2 Financement du cyber terrorisme

Le financement du cyber terrorisme - la capacité des terroristes à lever, déplacer, stocker et déployer des fonds et d'autres biens ou ressources, est fait à une plus petite échelle par rapport à la taille de l'économie criminelle et à la valeur illicite du blanchiment d'argent. Bien que les services répressifs tendent à privilégier les transactions de plus grande valeur associées au crime organisé, l'accent est mis sur le financement du cyber terrorisme en raison d'une meilleure compréhension du phénomène et de la croissance malheureuse de groupes tels que l'État Islamique. Si le financement du cyber terrorisme peut soutenir des activités terroristes telles que les attentats suicides, il peut également soutenir les aspects moins violents et moins évidents des opérations d'un groupe en payant les frais de subsistance, les déplacements, la formation, les activités de propagande, les frais d'organisation et d'indemnisation des familles des terroristes tués.

Le financement du cyber terrorisme, semblable au blanchiment d'argent, est un phénomène en constante évolution. Bien qu'il existe des similitudes entre les deux activités, il existe un certain nombre de différences fondamentales. La principale différence, bien sûr, c'est le fait qu'en ce qui concerne le blanchiment d'argent, tous les fonds soumis au processus de blanchiment sont sales dès le départ; ils sont le produit de crimes. Cependant, dans le financement du cyber terrorisme, si une partie de l'argent est sans aucun doute le produit de crimes, une part importante de celui-ci n'est pas réellement sale dès le départ, du moins pas à la suite d'une inspection occasionnelle. Naturellement, si les fonds sont considérés comme illicites, il est normal de supposer que les cyber terroristes auront recours à des activités de blanchiment d'argent alignées sur la criminalité pour financer leurs activités. C'est particulièrement le cas si un groupe de cyber terroristes n'est pas en train de commettre un crime non terroriste pour lever des fonds ([6]Simser Jeffrey, 2011). Par conséquent, en raison des caractéristiques associées au financement du terrorisme, le processus de financement du cyber terrorisme a été étiqueté de manière inoffensive «le blanchiment d'argent à l'envers»

[6] Simser Jeffrey, (2011). "Le financement du terrorisme et la menace pour les institutions financières", Journal of Money Laundering Control, Vol. 14 No. 4, pp. 334-345.

([7]Unger Brigitte, Daan van der Linde, 2013, p.88). La raison en est la légitimité des fonds impliqués au début du processus. Toutefois, reconnaître les fonds comme ceux qui financent le cyber terrorisme nécessite la connaissance de l'intention ultime. Par conséquent, pour soutenir le financement du terrorisme, une approche large et sophistiquée est nécessaire pour détecter les flux financiers dirigés vers les cellules terroristes partout dans le monde (Krieger et Meierrieks, 2011). Cependant, cela reste difficile, car le processus de financement du cyberterrorisme est souvent simple, se fondant sans effort dans des pratiques de routine formelles et légitimes.

Dans de nombreux cas, il est difficile et peut-être presque impossible de séparer le financement du cyber terrorisme et le financement non terroriste. La raison pour cela, comme déjà identifiée, est que les fonds généralement utilisés pour soutenir le terrorisme sont plus petits en valeur globale et impliquent des méthodes de transfert qui sont alignés à des montants plus faibles tels que l'utilisation de cartes prépayées.

Porté par une approche qui exploite des vulnérabilités similaires - soutenues par un haut niveau d'anonymat et de non-transparence dans l'exécution des transactions financières - le blanchiment d'argent et le financement cyber terroriste présentent, tous les deux, des menaces importantes et distinctes pour la sécurité nationale. Il est clair que les fonds blanchis sont plus faciles à associer à des activités illicites, car ils sont plus proches de l'infraction principale tandis que dans le cyber terrorisme, c'est à la fin du cycle que les fonds peuvent être liés au bénéficiaire prévu. Ce désalignement indique donc que même si les deux méthodes conservent leurs propres problèmes, le financement du cyber terrorisme reste beaucoup plus difficile à prévoir surtout dans le cas où les détails des individus, des entreprises, des organisations caritatives et des destinations ne sont pas connus ou alignés de manière officielle au cyber terrorisme. En outre, ceci indique les possibilités avantageuses qui existent pour que les cyber terroristes puissent contourner le contrôle formel ou le processus CFT (Combattre le financement du terrorisme). Cette approche contredit celle du blanchiment d'argent qui, en tant qu'activité, doit - à moins que les fonds ne soient auto-blanchis - passer par le processus de blanchiment d'argent en trois étapes dans son intégralité.

[7] Unger Brigitte, Daan van der Linde, (2013). Manuel de recherche sur le blanchiment d'argent, Edawrd Elgar Publishing, Londres. p. 88

5.3 Distinction entre financement du cyber terrorisme et blanchiment d'argent.

La consolidation des pratiques préventives et d'investigation en matière de lutte contre le blanchiment d'argent et le financement du terrorisme (AML / CFT) a conduit, en principe, à un alignement étroit des deux mesures recommandées par le Groupe d'Action Financière (FATF.GAFI.ORG). Malgré cela, il n'est pas toujours vrai que ces pratiques correspondent à la nécessité de convertir les produits du crime, permettant ainsi aux fonds de paraître légitimes. En réalité - comme le démontrera ce document - les fonds légitimes destinés au cyber terrorisme n'ont pas nécessairement besoin d'être blanchis. Au lieu de cela, il peut être nécessaire de déguiser le lien entre les petites sommes d'argent et les personnes soupçonnées d'activités criminelles initiales ou de conspiration cyber terroriste.

Ce que les pratiques de blanchiment d'argent et de cyber terrorisme permettent d'obtenir, même si l'objectif final de chaque pratique est nettement différent, c'est de créer une obscurité entourant le processus de financement, une pratique remarquablement moins complexe pour le financement du cyber terroriste. Par conséquence, le débat autour des différences entre AML et CFT se poursuit alors que les deux pratiques se déroulent en trois étapes, suggérant une «brouille de la ligne» (Laqueur Walter, 1999) entre le crime organisé et les organisations cyber terroristes. Selon Makarenko[8] (2004), cette question est mieux comprise lorsqu'on considère que chaque groupe peut traverser l'échelle en fonction de l'environnement dans lequel il opère. La raison en est que certains groupes criminels affichent des motivations politiques, tandis que d'autres groupes de cyber terroristes se concentrent sur les profits criminels à travers une façade alignée sur la rhétorique politique. Pour compliquer davantage la distinction entre les deux pratiques, le financement du cyber terrorisme commence souvent par des fonds légitimes provenant des envois de fonds des immigrants et des organisations caritatives, suggérant que les fonds peuvent passer par le système financier légitime ou être transférés directement à une organisation cyber terroriste.

[8] Makarenko Tamara, (2004). "Le continuum crime-terreur: traçage de l'interaction entre le crime organisé transnational et le terrorisme", Global Crime, Vol. 6, pp. 129-145.

5.4 Blanchiment d'argent

Le blanchiment d'argent est la pratique selon laquelle les actifs illicitement dérivés (et pas seulement l'argent) sont convertis en actifs apparents légitimes afin d'être dépensés ou transférés sans éveiller de soupçons. Des montants importants peuvent être impliqués, de même que de petites quantités, indiquant que le processus de blanchiment d'argent dépend fortement des caractéristiques sous-jacentes, telles que la méthode de blanchiment, l'expérience du blanchisseur, l'infraction principale et les risques associés à la détection. Pour que les activités de blanchiment d'argent soient réussites, elles doivent tout simplement masquer efficacement le lien entre les fonds et l'activité criminelle initiale.

Comme indiqué, le processus formel derrière le blanchiment d'argent consiste en trois étapes consécutives : le placement, l'empilage et l'intégration. Chaque étape facilite une caractéristique particulière pour permettre aux fonds, autrefois illicitement dérivés et corrompus, de paraître légitimes. Cependant, il est également reconnu que dans certaines circonstances, les criminels peuvent auto-blanchir des fonds illicites, leur permettant de contourner ou de participer au processus «officiel» de blanchiment d'argent pour acheter de petits articles tels que de la nourriture, du carburant et d'autres articles non suspicieux. ".

Le blanchiment d'argent tire profit d'activités illégales telles que la drogue, le mazoutage, la fraude et la cybercriminalité. Les sommes qui apparaissent sur un compte (placement), consistent en de nombreuses transactions financières dans le but de cacher leur propre provenance et évidemment empêcher les autorités à les retracer. Les sources illégales (layering-empilage) sont inévitablement déguisées afin que personne ne puisse soupçonner que c'est une obtention de richesse illégale découlant de transaction avec des fonds illicites (intégration) ([9]Harowitz Richard, 2010).

L'introduction de nouvelles méthodes de paiement, d'environnements virtuels et la facilité avec laquelle l'anonymat peut être maintenu sur Internet ont également modifié la portée des possibilités de blanchiment d'argent disponibles. Les méthodes disponibles offrent maintenant de nouvelles façons de déplacer facilement des sommes d'argent

[9] Harowitz Richard (2010). "The global anti money laundering regime: a short review." Cayman Island.

importantes (Pearce Rohan, 2012, Jacobson Michael, 2010, GAFI, 2008, Irwin Angela[10] et al., 2014). Bien que le blanchiment de fonds à travers le scénario virtuel puisse prendre plus de temps, il est parfois impossible pour des sommes plus considérables, et les coûts peuvent être significativement plus élevés que dans le monde réel.

5.5 Types de financement du cyber terrorisme (renforcement des capacités dans la lutte contre le cyber terrorisme)

Comme les temps ont changé, les groupes du cyber terrorisme se sont adaptés à ces changements. Au niveau du groupe, les organisations cyber terroristes ont utilisé le parrainage d'État, le soutien de la diaspora, des organisations caritatives, des financiers indépendants, des organisations de façade ou elles vendent leur formation et leur expertise à d'autres groupes et au crime organisé pour se financer. Le financement de grandes organisations cyber terroristes demande de grosses sommes. Comme pour n'importe quelle multinationale, il y a des coûts d'exploitation associés au simple fait de pouvoir «garder les portes ouvertes». Cependant, au niveau de la cellule, effectuer des opérations ne coûte pas autant. Des délits mineurs ou même un emploi à temps plein peuvent aider à couvrir les coûts d'achat d'articles en vente libre et qui sont utilisés pour fabriquer certains engins explosifs. La section suivante présente brièvement de différentes méthodes de financement au niveau du groupe et de la cellule, ainsi qu'un aperçu de la façon dont les groupes de cyber terroristes utilisent le crime organisé pour financer leurs opérations.

Le cyber terrorisme parrainé par l'État a diminué au cours des dernières décennies, bien qu'il se produise encore. Par exemple, Le renseignement interservices pakistanais (ISI) a été lié à divers groupes terroristes et cyber terroristes pakistanais, dont Jaish-e-Mohammad, Harakat-ul-Jihad. Islami Bangladesh (HuJI-B), et d'autres groupes, ainsi qu'aux plusieurs attentats terroristes et cyber terroristes (Kania Rick, 2011). Au passé, l'Iran a été accusé d'avoir envoyé des roquettes Kassam à Hamas à l'aide du groupe

[10] Irwin Angela, Slay Jill, Choo Kim-kwang Raymond, et Lui Lin, (2014). "Le blanchiment d'argent et le financement du terrorisme dans les environnements virtuels: une étude de faisabilité", Journal of Money Laundering Control, Vol. 17 No. 1, pp. 50-75, doi: 10.1108 / JMLC-06-2013-0019.

terroriste Hezbollah ([11]Esposito Michaelle, 2003). La Syrie a également été liée au Hezbollah en tant que sponsor du cyber terrorisme, y compris des informations liées à l'attaque du Hezbollah qui a tué l'ancien Premier ministre libanais Rafic Hariri. De plus elle a été accusée d'avoir fourni refuge à divers autres groupes terroristes (PKK) qui y ont trouvé refuge dans les années 1980 et 1990 (Fletcher Holly, 2008). Les financiers indépendants, tels qu'Oussama ben Laden lui-même, qui sont en mesure de gérer de grandes quantités d'argent à l'appui des objectifs et des opérations cyber terroristes, ont également été utilisés. En mai 2012, par exemple, Abdul Baqi Bari a été désigné par les États-Unis comme terroriste mondial à cause de l'utilisation de ses entreprises en Afghanistan et au Pakistan pour financer les opérations des talibans et d'Al-Qaïda (Roggio Bill, 2012).

Certains groupes collectent des fonds auprès des communautés expatriées, en utilisant différentes méthodes. Les grandes communautés tamoules étaient une ressource pour les Tigres de libération de Tamoul Eelam (LTTE), de la même manière que les communautés kurdes finançaient le Parti des travailleurs du Kurdistan (PKK). Dans certains cas, les dons proviennent de ces communautés volontairement, dans d'autres cas, le soutien est obtenu par les terroristes, en les menaçant. Cependant, ils ont attiré plus d'attention aux États-Unis plus particulièrement, après les attentats du 11 septembre. De nombreuses organisations caritatives, telles que le World Tamil Movement (WTM), la Holy Land Foundation, et l'IIRO (International Islamic Relief Organization), connue aussi sous le nom d'Organisation Islamique Internationale de Secours en Arabie Saoudite (IIROSA), qui est une organisation caritative basée en Arabie Saoudite et fondée par la Ligue islamique mondiale en 1978, elles ont tous été liées au financement de groupes terroristes ([12]Sécurité publique Canada, 2012).

Dans d'autres exemples, des groupes ont vendu de la formation et des connaissances afin d'obtenir des fonds. En 2001, par exemple, James Monaghan, Niall Connolly et Martin McCauley ont été arrêtés en Colombie après avoir passé 18 mois à former des membres des Forces armées révolutionnaires de Colombie (FARC). Tous les trois

[11] Michele K. Esposito, (2003). Rapport trimestriel sur les conflits et la diplomatie, Journal of Palestine Studies 33 (1) (automne 2003), pp. 116-138, disponible à : http://www.palestine-studies.org/files/pdf/jps/5663.pdf

[12] Sécurité publique Canada, (2012). "Entités actuellement listées", disponible à : http://www.securitepublique.gc.ca/prg/ns/le/cle-fra.aspx;

avaient été chargés de former les membres des FARC à utiliser des armes de l'IRA. Mortiers, (Pogatchnik Shawn, 2005). Dans plusieurs cas, des groupes terroristes, tels que les Taliban en Afghanistan et au Pakistan, ont autorisé des membres d'autres groupes terroristes à participer à des camps d'entraînement. Non seulement certains groupes vendent des connaissances, mais ils transmettent aussi des tactiques. Al Shabaab, un groupe lié à al-Qaïda opérant en Somalie, a formé des membres du groupe terroriste nigérian Boko Haram, alors que des rapports récents ont lié les deux groupes et Al-Qaïda au Maghreb Islamique (AQMI), alléguant qu'ils partagent la formation, les explosifs et les fonds (Smith David, 2012). En outre, en juillet, deux Nigérians ont été arrêtés à Abuja (Nigeria) d'avoir reçu de l'argent d'Al-Qaïda dans la péninsule arabique (AQAP - Yémen) pour avoir recruté des membres de l'AQAP en provenance du Nigeria (BBC 2012).

Une fois que l'argent est recueilli pour les groupes du cyber terroriste, il peut être déplacé de plusieurs façons. L'argent peut être transféré légalement à travers le système bancaire. Un groupe cyber terroriste peut également blanchir l'argent par le biais du système bancaire. La Banque de Crédit et de Commerce International (BCCI) est un exemple précoce de la façon dont les banques commerciales ont été utilisées pour blanchir de l'argent pour des groupes de cyber terroristes tels qu'Abu Nidal (Fritz Sara, et al., 1991). Certains groupes utilisent des systèmes informels de transfert d'argent tels que Hawala, ou le Black Market Peso Exchange (BMPE). Les groupes sont également en mesure de transférer de l'argent à travers des organisations caritatives ou des sociétés écrans. Des groupes ont employé des courriers pour transférer de grosses sommes d'argent en espèce, d'un pays à l'autre ou d'un groupe à l'autre. D'autres groupes ont échangé des marchandises telles que l'or, les diamants ou d'autres pierres précieuses pour transférer des fonds. Les groupes de cyber terroristes ont également échangé des produits tels que l'échange de drogues contre des armes.

Les groupes de cyber terroristes qui opèrent au niveau de la cellule n'ont pas de gros frais généraux et peuvent subvenir à leurs besoins sans avoir besoin d'une telle somme d'argent. Dans de nombreux cas, les petits groupes au niveau cellulaire peuvent être soutenus par des activités criminelles mineures, y compris le vol ou la fraude. Dans certains cas, le simple fait d'occuper un emploi légitime peut fournir suffisamment

d'argent pour vivre tout en préparant une attaque terroriste. On en a un premier exemple dans les attentats qui ont eu lieu à Londres le 7 juillet 2005. Comme les bombes étaient fabriquées avec des produits en vente libre, le coût n'était pas très élevé. Selon un rapport de la Chambre des Communes sur les attentats du 7/7, les attentats à bombe, qui ont fait 52 morts et plus de 770 blessés, avaient coûté moins de £ 8,000 livres sterling à planifier et à exécuter ([13]UK House of Commons 2006).

Le 7 juillet 2005, trois explosions ont eu lieu dans le réseau de transport de Londres près de 9h et une quatrième a eu lieu peu après 9h45. Quatre hommes - Shehzad Tanweer, Mohammad Sidique Khan, Hasib Hussain et Jermaine Lindsay - étaient les kamikazes qui ont mené ces attaques. Pour mener à bien l'opération, Khan et Tanweer sont allés au Pakistan et à leur retour, ils ont quitté leur emploi pour avoir le temps à planifier les attaques. Khan avait reçu une formation sur les explosifs et les armes dans un camp d'entraînement à Malakand, au Pakistan, en juillet 2003 (Silber Mitchell, et al., 2007). Les dépenses pour ces attentats comprenaient le voyage au Pakistan, la location d'un appartement au 18, rue Alexandra Grove à Leeds, le voyage au Royaume-Uni, la location d'un véhicule et l'achat de matériel de fabrication de bombes. Les enquêteurs ont découvert que le kamikaze Jermaine Lindsay avait fait des achats dans les semaines précédentes les attaques et il avait payé par chèques qui ont rebondi. On pense cependant que Mohammad Sidique Khan a financé la plus grande partie de l'opération. Il travaillait à plein temps, il a donc pu obtenir plusieurs cartes de crédit et un prêt bancaire personnel. Les bombes ont été fabriquées en utilisant des matériaux disponibles dans le commerce et étaient donc faciles à obtenir et pas très coûteux.

5.6 Sources de financement des activités cyber terroristes

L'attitude pragmatique du crime organisé et des membres de la diaspora a créé des fonds et des ressources nécessaires à la mise en œuvre des activités du cyber terroriste. Les organisations terroristes utilisent très souvent des méthodes

[13] U.K. House of Commons (2006), Report of the Official Account of the Bombings in London on 7th July 2005. disponible à: https://www.gov.uk/government/publications/report-of-the-official-account-of-the-bombings-in-london-on-7th-july-2005

traditionnelles de financement de leurs activités (trafic, contrefaçon, trafic de drogue, extorsion, vols, enlèvements et métaux précieux) ([14]Ljupco Arnaudovski, 2002).

Comme vous pouvez le voir, au-dessus de l'action affichée tout se déroule dans la zone informelle (illégale) où le crime organisé règne. L'objectif est de couvrir les fonds provenant d'activités criminelles et d'éviter le secteur financier. Ce type de financement des organisations terroristes présente un risque «faible», car les fonds ne sont pas enregistrés dans le système financier, où les institutions financières et les forces de l'ordre peuvent les localiser, geler et confisquer, et où les acteurs peuvent être retracés et portés en justice, bloquant le processus de financement.

Ce phénomène est la base de la "loi Gudhartoviot" selon laquelle on reconnaît des opportunités de faire basculer les modes de financement qui sont strictement réglementés, avec ceux qui ne le sont pas. Dans le cas d'Al-Qaïda, cela signifie l'introduction de différentes méthodes dans le réseau terroriste qui entre d'autres, ils comprennent des diamants et d'autres pierres précieuses et fausses, la cybercriminalité, etc. (Gendron Angela, 2007).

Le caractère international du cyber terrorisme présente une mobilité et une flexibilité dans la recherche de nouvelles méthodes d'action qui restent inconnus aux autorités qui, en fait, ont un problème à trouver une méthode fiable pour la suppression précoce du financement du terrorisme.

Cependant, comme décrit ci-dessus, le processus de changement des structures internes des organisations terroristes entraîne des changements dans la manière traditionnelle d'acquérir des biens. Ceci a été nécessaire car la communauté internationale a renforcé la lutte contre le terrorisme sous tous ses aspects, en adoptant de nombreuses lois, décisions, conventions, directives, etc., et en renforçant les capacités institutionnelles, en échangeant des informations, etc. Mais la dernière décennie a été une décennie de révolution technologique. Tous les produits du développement de la technologie paraissaient utiles pour faciliter notre vie et améliorer sa qualité. Personne n'aurait pu imaginer que les mêmes produits pouvaient être utilisés

[14] Arnaudovski Ljupco, (2002). "Interdiscipline et interdépendance du terrorisme et du crime organisé" Annuaire de la Faculté de sécurité, Université "St. Kliment Ohridski", Skopje, Centre pour le personnel éducatif dans le domaine de la sécurité-Skopje, Skopje, 2002, p. 92

à d'autres fins, contre l'humanité par les terroristes. À titre d'exemple, nous indiquons les cartes de crédit qui sont bénéfiques pour tous les citoyens. Au moment du lancement de ce nouveau système de paiement, tout le monde parlait d'une grande découverte mais personne n'aurait pu prédire que ces cartes de crédit pourraient être volées, abusées, falsifiées, etc.

5.7 Opérations cyber terroristes de déstabilisation psychologique

Les racines de la notion de cyber terrorisme remontent au début des années 1990, lorsque la croissance rapide de l'utilisation d'Internet et le débat sur la «société de l'information» émergente ont suscité plusieurs études sur les risques potentiels de la dépendance d'États de cette technologie de pointe. Dans l'avenir prochain, le terroriste peut être capable de faire plus de dégâts avec un clavier qu'avec une bombe. En même temps, le terme prototypique « Pearl Harbor électronique » a été inventé, reliant la menace d'une attaque informatique à un traumatisme historique américain.

Le principal danger du cyber terrorisme est sa capacité à exposer rapidement de grandes communautés qui sont en ligne à une quantité substantielle de contenu multimédia engageant. Les experts sont de plus en plus préoccupés par le potentiel de ces cybercommunautés à des fins illégales. Le cyber terrorisme a complètement changé le rôle de la stratégie culturelle. La guerre n'a pas de règles. Dans le cyber terrorisme, le crime organisé et la nouvelle guerre non conventionnelle, les pièces de l'échiquier communiquent entre elles et en même temps elles ont le pouvoir d'agir de façon autonome. Les États, en tant que maître d'échecs, tentent de contrôler et de gérer leurs 16 pièces d'échecs, mais l'adversaire (tous les acteurs illégaux contemporains) parvient encore à agir facilement et efficacement. Néanmoins, le maître est en arrière-plan, permettant aux 16 pièces de penser et d'agir pour eux-mêmes et de communiquer entre eux en permanence.

Les forces psychologiques, politiques et économiques se sont combinées pour promouvoir la terreur du cyber terrorisme. D'un point de vue psychologique, deux des plus grandes craintes contemporaines, sont combinées dans le terme «cyber terrorisme». La peur de la victimisation aléatoire et violente se confond bien avec la méfiance et la peur pure de la technologie informatique. Une menace inconnue est

perçue comme plus menaçante qu'une menace connue. Bien que le cyber terrorisme n'entraîne pas une menace directe de violence, son impact psychologique sur les sociétés anxieuses peut être aussi puissant que l'effet des bombes terroristes. De plus, les forces les plus destructrices qui s'opposent à la compréhension de la menace réelle du cyber terrorisme sont la peur de l'inconnu et le manque d'information ou, pire, l'diffusion de trop de désinformation.

À ne pas négliger le fait qu'il y a aussi une dimension politique à la nouvelle focalisation sur le cyber terrorisme. Les débats sur la sécurité nationale, y compris la sécurité du cyberespace, attirent toujours des acteurs politiques avec des programmes qui vont au-delà de la question spécifique et donc, le débat sur le cyber terrorisme ne fait pas exception à cette tendance.

La lutte contre le cyber terrorisme est devenue non seulement une question hautement politisée, mais aussi une question économiquement enrichissante. Toute une industrie a émergé pour faire face à la menace du cyber terrorisme: des « think tanks » ont lancé des projets élaborés et ont publié des livres blancs alarmants sur le sujet, des experts ont témoigné devant le Congrès des dangers du cyber terrorisme et des sociétés privées ont déployé à la hâte des consultants et des logiciels de sécurité pour protéger des cibles publiques et privées. Les cybers terroristes utilisent la prédication des clercs radicaux pour promouvoir l'enrôlement de nouveaux membres, légitimer leur cause militante et justifier leurs actes violents.

5.8 Trolling

De nombreuses organisations terroristes mondiales comme l'Etat Islamique (ISIS) essaient de plus en plus de recruter des jeunes occidentaux. Selon les experts américains, environ 1000 combattants étrangers rejoignent ISIS chaque mois. Certaines de ces recrues viennent de pays occidentaux. Cependant, les principales zones identifiées comme soutenant le pouvoir des groupes terroristes sont liées aux «tactiques

psychologiques telles que la terreur des populations, les récits religieux et sectaires et les contrôles économiques» ([15]Schmittdec Eric, 2014).

En 1982, Schmid et de Graaf ont souligné que «un acte de terrorisme est en réalité un acte de communication. Pour le terroriste, ce qui compte c'est le message passé et non pas la victime ». De plus, la communication et le terrorisme vont de pair car la communication est l'oxygène des actes terroristes ([16]Schmid P. Alex et al., 1982). De même, Freedman et Thussu pensent que les médias sont au cœur du terrorisme parce qu'ils sont «de plus en plus considérés comme des agents actifs dans la conceptualisation effective des événements terroristes» (Freedman Des et al., 2012). Comme indiqué ci-dessus, ISIS exploite pleinement de diverses plates-formes médiatiques afin de diffuser des messages effrayants et de créer un impact efficace sur leurs destinataires.

À notre époque, les médias sociaux jouent un rôle important dans la vie quotidienne. En fait, les médias sociaux peuvent contribuer à unifier et parfois radicaliser le public par rapport aux questions politiques et sociales. Les motivations psychologiques qui conduisent certaines personnes à rejoindre des groupes extrémistes sont diverses. C'est pourquoi ces personnes peuvent être catégorisées à : «des vengeurs qui ont besoin d'un exutoire pour leur frustration, des demandeurs d'état qui ont besoin de reconnaissance, des demandeurs d'identité qui ont besoin d'appartenir à un groupe et des amateurs de sensations fortes ayant besoin d'aventure » (Venhaus John, 2010).

En ce qui concerne le « Trolling » et le « Flaming » il y a un problème conceptuel dans la définition de ces deux termes car ces tactiques ont le même but et appliquent les mêmes méthodes. Il est donc, impossible parfois de distinguer l'une de l'autre. En fait, elles ont l'intention de perturber une conversation en cours, et toutes les deux peuvent mener à des arguments aggravés» ([17]Herring Susan, et al., 2002). L'anonymat relatif des utilisateurs en ligne favorise leur application sur des plates-formes différentes.

---

[15] Schmittdec Eric, (2014). "In Battle to Defang ISIS, U.S. Targets Its Psychology," The New York Times, December 28, 2014, Disponible à: http://www.nytimes.com/2014/12/29/us/politics/in-battle-todefang-isis-us-targets-its-psychology-.html?_r=0

[16] Alex P. Schmid and Danny De Graaf, (1982). Violence as Communication: Insurgent Terrorism and the Western News Media (London: Sage, 1982), p. 14.

[17] Susan Herring, Kirk Job-Sluder, Rebecca Scheckler et Sasha Barab, (2002). "À la recherche de la sécurité en ligne: gérer la pêche à la traîne dans un forum féministe", The Information Society 18, no. 5 (2002): p. 371 à 384, p. 372.

La littérature sur ces deux types de comportements antisociaux est plutôt liée aux études et rapports sur les pratiques de protection de l'enfance. En général, il y a souvent un sentiment de panique morale, de risque et d'anxiété publique en ce qui concerne l'exposition et l'utilisation d'Internet par les enfants (David Matthew et al., 2011). L'utilisation des médias sociaux pourrait avoir des effets négatifs sur le bien-être de certains adolescents, notamment «E-Crime 2.0», qui comprend «les infractions qui exploitent les moyens par lesquels les utilisateurs des nouvelles technologies de communication deviennent publiquement visibles et disponibles ». Certains des effets néfastes des médias sociaux qui ont été signalés dans des recherches antérieures sur les adolescents et les enfants comprennent« l'isolement social, la dépression et la cyber intimidation »([18]Best Paul et al., 2014).

En ce qui concerne le Trolling, l'une des premières études qui l'a examiné a été menée par Donath sur les groupes User net (Donath Judith, 1999). Hardaker fournit également plusieurs définitions et le classe en différents types selon quatre caractéristiques principales: l'agression, la tromperie, la perturbation et le succès. En relation avec cette étude, il y a deux catégories qui sont plus pertinentes : La première est connue comme l'impolitesse contrariée / frustrée et elle fait référence à l'intention malveillante d'un message. Pourtant son intention est frustrée ou contrecarrée par le destinataire soit parce qu'il n'est pas offensé, donc aucune action n'est prise (frustrée), soit parce qu'il est contré par le message. Par exemple, "sarcasme, mépris ou amusement" (contrarié). La seconde est appelée l'impolitesse véritable, malveillante ou stratégique et atteint son but en offensant le (s) receveur (s) (Hardaker Clair, 2010).

Dans tous les cas, le trolling cherche à créer un argument, à inciter les autres à une discussion interminable ou à détourner une discussion. En d'autres termes, il est conçu comme une distraction par rapport à la discussion principale du forum ou de la plate-forme en détournant l'attention sur un autre problème qui n'est pas pertinent pour la plupart des participants.

Comme pour le trolling ainsi que pour le flaming, il n'y a pas d'accord sur une définition unifiée. Il s'agit généralement d'une communication agressive ou hostile qui se produit

[18] Paul Best, Roger Manktelow et Brian Taylor, (2014). «La communication en ligne, les médias sociaux et le bien-être des adolescents: un examen narratif systématique», Revue des services à l'enfance et à la jeunesse 41 (2014): p. 27-36.

via des canaux informatiques. En effet, le flaming est similaire au trolling mais beaucoup plus agressif car il contient des insultes, de l'obscénité et des jurons, surtout s'il s'agit d'un sujet religieux.

Les sympathisants de l'ISIS exploitent ce qu'on appelle des «comptes disséminateurs» sur les médias sociaux, en particulier Twitter, qui «apportent un soutien moral et politique à ceux qui sont dans le conflit». «Une fois le contenu produit et diffusé, c'est souvent le réseau de distribution des médias moudjahidin, plutôt que le producteur d'origine, qui assure la disponibilité continue du contenu» ([19]Fisher Ali, 2015). Ce modèle suggère que les sympathisants se rassemblent comme un essaim d'abeilles qui se réorganisent constamment et qui sont prêts à s'engager et à attaquer à tout moment.

6. Deuxième Partie

6.1 Typologies de terrorisme et financement de terrorisme

Il y a beaucoup de différentes catégories de terrorisme. Ces catégories permettent de différencier les groupes terroristes selon des critères spécifiques liés à un domaine spécifique. Sur la base des stratégies que les terroristes utilisent pour financer leurs activités, le terrorisme peut être divisé en sept groupes ([20]Vittori Jodi, 2011):

(i). Terrorisme parrainé par l'État,

(ii).Terrorisme parrainant un État,

(iii). État de coquille,

(iv). Franchise,

(v). Soutien groupé,

(vi). Société transnationale et

(vii). Loup solitaire

[19] Ali Fisher, (2015). "Comment les réseaux djihadistes maintiennent une présence en ligne persistante", Perspectives on Terrorism 9, no. 3 (2015): p. 4.

[20] Vittori Jodi, (2011). Financement du terrorisme et ressourcement, Palgrave Macmillan, New York, NY.

(i). Un groupe parrainé par l'État reçoit des soutiens importants d'un État qui cherche des objectifs politiques ou idéologiques particuliers. L'État peut trouver de nombreuses façons afin de soutenir les terroristes, notamment en leur fournissant de faux documents et passeports, leur permettant de voyager en toute sécurité à l'intérieur du pays ou vers d'autres pays, en leur fournissant un sanctuaire et des armes. L'autonomie des groupes dans cette catégorie dépend de leur degré d'intégration dans le commandement et le contrôle d'un État particulier (Vittori Jodi, 2011). Les terroristes peuvent recevoir le soutien des États tant que cette aide ne perturbe pas leur indépendance. Cependant, les promoteurs de l'État peuvent imposer des exigences à ces groupes afin de les orienter dans une direction spécifique. Dans un tel cas, c'est-à-dire des «groupes dirigés par l'État» (Deatherage Robert, 2008), les groupes existent aussi longtemps qu'ils valent la peine pour les États promoteurs.

(ii). Un groupe terroriste parrainant un État est un groupe capable de fournir des facilités à un État sponsor en échange d'un soutien de la part de cet État (Vittori Jodi, 2011). Par exemple, le gouvernement du Soudan a laissé Al-Qaïda organiser des camps d'entraînement au Soudan en échange d'argent et d'infrastructures (Byman Daniel, 2005). C’est considéré que ces groupes terroristes doivent avoir atteint un niveau élevé de capacité pour attirer l'attention des promoteurs de l'État (Vittori Jodi, 2011).

(iii). Dans le cas des «États de coquilles», les terroristes prennent le contrôle d'une zone géographique et l'exploitent pour le sanctuaire et leurs besoins (Napoleoni Loretta, 2005). Une zone peut être aussi petite que quelques quartiers ou aussi grande qu'une vaste zone dans un pays. L'exemple de ce type de terrorisme est le narco terrorisme.

(iv). Dans la catégorie des franchises, les groupes terroristes reçoivent une grande partie de leur soutien d'une source, mais leurs ressources sont suffisamment diversifiées pour rester indépendantes (Vittori Jodi, 2011). Dans ce cas, si les sponsors arrêtent de soutenir, bien que les groupes terroristes puissent s'affaiblir, ils ne sont pas menacés d'extinction. Par exemple, on prétend que le Hamas et le Hezbollah sont des franchisés iraniens, dont ils reçoivent une grande partie de leur soutien, mais ils

maintiennent également leur propre réseau d'organisations caritatives, de sociétés écrans et de réseaux criminels pour soutenir leurs activités (Levitt Matthew, 2007).

(v). Dans la catégorie «soutien groupé», les terroristes ne comptent pas sur un ou plusieurs sponsors, mais ils reçoivent un certain nombre de ressources tangibles et intangibles de la part de nombreux contributeurs non étatiques (Vittori Jodi, 2011). Le phénomène de soutien de la diaspora, selon lequel les terroristes reçoivent le soutien de donateurs dispersés mais de la même ethnie ou de la même nationalité, est l'exemple frappant de cette catégorie. Beaucoup de petites contributions de différents contributeurs donnent aux groupes terroristes plus d'autonomie qu'un groupe terroriste sponsorisé par l'Etat. Cependant, ils ne reçoivent de soutien que dans la mesure où leurs actions satisfont leurs supporteurs (Vittori Jodi, 2011).

(vi). Le modèle des sociétés transnationales, largement utilisé pour décrire Al-Qaïda, permet aux groupes terroristes d'agir à l'échelle mondiale sans identification nationale spécifique. Ces groupes, utilisant la mondialisation, sont très sophistiqués et complexes en termes de ressources, de membres et d'opérations géographiques (Cronin Audrey Kurth, 2002-2003). Les groupes de ce modèle sont des experts qui utilisent des systèmes financiers formels et informels, des sociétés écrans, des organismes de bienfaisance, du blanchiment d'argent et d'autres activités criminelles. Ils ont également un haut niveau d'autonomie, car ils ont accès à diverses ressources financières.

(vi). Le terrorisme des loups solitaires est l'exemple de groupes terroristes qui ne sont pas essentiellement impliqués dans des activités collectives organisées ([21]Spaaij Ramon, 2012). Les groupes terroristes de loups solitaires sont des individus ou des petits groupes qui sont identifiables par une idéologie ou un grief particulier, et qui mènent des actions à l'appui de leur conviction radicale. Contrairement à d'autres types, les groupes de terroristes de loups solitaires sont de petite taille avec peu d'exigences financières et des capacités limitées. Ils sont autonomes, libres de choisir leurs cibles et leurs tactiques. Le terrorisme sous cette forme n'est pas coûteux, mais les causes peuvent être importantes. On prétend qu'il existe une tendance considérable qui indique la fréquence croissante des attaques de loups solitaires par des individus ayant peu ou

[21] Spaaij Ramon,F.J. (2012). Comprendre le terrorisme des loups solitaires: modèles, motivations et prévention dans le monde, Springer, Dordrecht.

pas de liens avec des organisations formelles ([22]Michael George, 2012, p.1). Les attentats terroristes en France en mars 2012 (Nimmo Kurt, 2012), en Norvège en juillet 2012 (Spaaij Ramon, 2012) et en Allemagne en mars 2011 (FoxNews.com, 2011) sont des exemples récents de terrorisme des loups solitaires.

6.2 Processus de changement de la structure organisationnelle des organisations terroristes.

"Le gagnant n'est pas celui qui est le plus fort; Le gagnant est celui qui est variable dans son environnement. "(Darwin)

Après les événements du 11 septembre 2001, la communauté internationale a renforcé la lutte contre le terrorisme sous tous ses aspects, en adoptant de nombreuses lois, décisions, conventions, directives, etc., et en renforçant les capacités institutionnelles, l'échange d'informations etc. Cette dynamique d'activités a suscité l'inquiétude de la plus puissante organisation cyber terroriste Al-Qaïda, selon laquelle, les terroristes se sont retrouvés à un carrefour où ils devraient choisir soit continuer sur la même voie, soit en prendre une nouvelle.

Cependant, le processus rapide de la mondialisation et la circulation des biens, des personnes, des services et des capitaux ainsi que le développement de la technologie permettent aux organisations de cyber terroristes de se doter de l'appareil nécessaire pour survivre.

En effet, d'une structure strictement conventionnelle - hiérarchique considérée comme la plus efficace, mais pas la plus sûre, Al-Qaïda et d'autres organisations terroristes affiliées, ont changé à une structure organisationnelle dans la structure où la sécurité et la sûreté était la prioritaires, ([23]Peresin Anita, 2007). En voici la raison pour laquelle Al-Qaïda était et l'est toujours indestructible.

Pourquoi est-il important de mentionner ces changements et comment ils influencent la modification des sources de financement? Dans une structure strictement

[22] Michael George, (2012). La terreur des loups solitaires et la montée de la résistance sans chef, Vanderbilt University Press, Nashville, TN. p.1

[23] Peresin Anita, (2007). "Paradigma novog terorizma informacijskoga doba" Politicka Misao Vol. XLIV, (2007), br. 2, p. 93-112.

conventionnelle - hiérarchique, les organisations terroristes ont un département spécial chargé de fournir des fonds et un soutien logistique. Les sources de leur financement proviennent souvent du trafic de drogues, d'armes, de vols, d'enlèvements, etc.

Par contre, les nouvelles organisations utilisent de plus en plus le système financier légal, bien qu'il y ait quelques exceptions, où la plupart de membres des cellules s'autofinancent. Le transfert de fonds a lieu via le système bancaire financier et, dans certains cas, le transfert rapide d'argent via Western Union est utilisé ([24]HM Treasury 2007). Ces transactions sont très difficiles à identifier lorsqu'il s'agit de suspicion. Il faut une coordination opportune entre les cellules de renseignement financier et les autorités d'enquête afin de faire le lien avec les activités opérationnelles et l'analyse des données financières (GAFI 2008). À notre avis, ce qui est primordial c'est que ces autorités effectuent le profilage des individus sur la base de l'analyse financière. Nous en sommes certain qu'elles constateront des transactions illogiques et artificielles qui s'écartent du normal.

6.3 Le crime organisé comme méthode de financement

Les groupes terroristes ont commencé à se diversifier afin d'utiliser des méthodes de financement communes aux groupes criminels transnationaux. Bien que les tactiques du crime organisé servent depuis longtemps à financer certains groupes, comme les Forces des Armées Révolutionnaires de Colombie (FARC), elles sont également devenues un mode de financement répandu pour d'autres groupes. Divers types de tactiques de criminalité organisée comme le trafic de drogue, le trafic d'armes, le trafic d'êtres humains et la traite des êtres humains, la contrefaçon de produits, l'extorsion, la fraude et d'autres types d'activités criminelles ont été utilisés par diverses organisations terroristes. En 2011, par exemple, au moins 30 vols de banque au Nigeria ont été attribués au groupe terroriste nigérian Boko Haram (thisdaylive 2011). Après l'arrestation d'Abu Qaqa, dirigeant de Boko Haram, il a révélé que lorsque le groupe manque de fonds, ils se tournent vers les vols de banque pour pouvoir continuer leurs opérations (onlinenigeria 2012). Le mouvement des fonds, dans le but de financer des

[24] HM Treasury (2007), Le défi financier de la criminalité et du terrorisme, HM Treasury, Londres, disponible à : http://webarchive.nationalarchives.gov.uk/+/http:/www.hm-treasury.gov.uk/media/C/B/financialchallenge_crime_280207.pdf

activités d'organisations terroristes, dans le cyberespace, peut être souligné par plusieurs études de cas. Ce ne sont pas les seuls moyens par lesquels les groupes obtiennent des financements, mais ces études de cas sont censées à mettre l'accent sur certaines des tactiques utilisées par les groupes terroristes dans le cyberespace. La section suivante donnera plusieurs exemples de ce type concernant le financement de groupes terroristes dans et hors du cyberespace.

L'enlèvement est une tactique qui a été utilisée par plusieurs groupes terroristes. Dans de nombreux cas, il y a des motivations financières, alors que dans d'autres cas, il y a des motivations politiques. Un exemple fondamental d'un groupe terroriste qui utilise cette tactique est Al-Qaïda au Maghreb islamique (AQMI), anciennement connu sous le nom de Groupe Salafiste pour l'Appel et le Combat (GSPC). En tant que GSPC, leur zone d'opération était limitée en Algérie; Cependant, au cours des dernières années, leurs opérations se sont étendues à de nombreux pays d'Afrique. Les enlèvements sont devenus la principale source de revenus d'AQMI, le groupe terroriste ayant gagné environ 65 millions de dollars en rançons depuis 2005 (Knaup Horand, 2012). Même si on tient compte qu'AQMI a déjà acheté des otages à d'autres groupes, on estime qu'il a gagné environ 130 millions de dollars des Occidentaux kidnappés (Nydailynews 2012).

Le 22 janvier 2009, par exemple, quatre Européens ont été kidnappés par des rebelles touaregs près de la frontière entre le Niger et le Mali et ils ont été vendus par la suite, à des membres d'AQMI au Mali (Pidd Helen, 2012). L'un des otages, Edwin Dyer, était un ressortissant britannique. AQMI a tenté de négocier avec le gouvernement britannique afin de l’échanger avec Abou Qatada, un Jordanien soupçonné d'être le lien européen d'Al-Qaïda et qui était détenu à Londres. Les Britanniques allaient l'expulser en Jordanie pour son implication présumée dans des attaques en Jordanie en 1998 (BBC 2012). Après que cette demande a été refusée, le groupe a exigé 10 millions d'euros (près de 12,5 millions de dollars américains) pour le retour de Dyer et d'un otage suisse. Le 31 mai 2009, Dyer a été tué dans le nord du Mali selon une déclaration d'AQMI (Gardham Duncan, 2009). Le groupe a alors tenté de négocier avec la Grande-Bretagne pour le retour du corps de Dyer (Gorman George, 2010).

Dans un exemple plus récent, l'ingénieur allemand Edgar Fritz Raupach a été kidnappé le 26 janvier 2012 lors d'un raid à Kano, au Nigeria, mené par le groupe terroriste Boko

Haram (Gambrell J. 2012). Ce n'est pas évident qu'AQMI ait procédé à l'enlèvement, mais en mars 2012, il a publié une déclaration et une vidéo montrant Raupach suppliant le gouvernement allemand de l'aider à sauver sa vie (BBC 2012). Le groupe a demandé la libération de Filiz Gelowicz, qui avait été arrêté et condamné pour avoir apporté son soutien à des terroristes qui avaient organisé un complot visant à tuer des militaires et des citoyens américains en Allemagne. Raupach a été blessé par balle par des ravisseurs, lorsque les forces de sécurité nigérianes ont mené un raid à Kano lors d'une tentative de sauvetage ratée (Gambrell Jon, 2012).

Un autre exemple de la façon dont les groupes cyber terroristes utilisent le crime organisé pour se financer, a eu lieu aux États-Unis en 2000. L'affaire implique plusieurs agents utilisant la contrebande de cigarettes comme moyen d'obtenir des fonds pour le Hezbollah. La cellule, prétendument dirigée par Mohamad Youssef Hammoud, a acheté de grandes quantités de cigarettes en Caroline du Nord, où la taxe par paquet était de 0,03 dollars à l'époque, a forgé des timbres fiscaux et les a transportés au Michigan où la taxe était de 1,50 $ par paquet, ([25]Grand Jury Acte d'accusation 2000). Cela a donné au groupe un profit de 1,47 $ par paquet de cigarettes. Hammoud et ses co-accusés ont été condamnés pour le soutien matériel au Hezbollah, la contrebande de cigarettes, le blanchiment d'argent, le racket et la fraude en matière d'immigration. En 2002, Hammoud a été condamné à 155 ans de prison, qui ont été réduits à 30 ans en janvier 2011 (ICE press 2011).

6.4 Les cyber terroristes dans le cyberespace

La monnaie virtuelle fait référence à une forme de représentation numérique de la valeur qui peut être échangée par des moyens numériques (Réseau de lutte contre la criminalité financière du Département de la trésorerie, 2013). Par rapport à la définition traditionnelle de la monnaie, consistant à échanger des unités ou des jetons en tant que moyen de valeur dans un pays, généralement représenté par des pièces physiques ou du papier ayant cours légal dans une juridiction particulière, la monnaie virtuelle se déplace entre plusieurs juridictions. La conception traditionnelle de la monnaie, celle des

[25] Grand Jury Acte d'accusation, (2000). U.S. c. Mohamad Youssef Hammoud, et al, Dossier 3: 00CR-147-MU (Cour de district des États-Unis pour la Division de loterie du District de l'Ouest de la Caroline du Nord, 31 juillet 2000), disponible à : http://fl1.findlaw.com/news.findlaw.com/wp/docs/terrorism/ushammoud32801ind.pdf

unités tactiles ou des jetons d'échange, est qualifiée de monnaie «réelle» et comporte l'aspect d'être soutenue et légitimée par le gouvernement respectif de chaque juridiction. La valeur d'une telle monnaie est affectée par les gouvernements.

En revanche, les monnaies virtuelles n'ont pas cette dépendance, mais leur valeur est plutôt liée à l'acceptation des individus. Une monnaie virtuelle n'est ni émise par une juridiction ni garantie, et "elle ne fonctionne que par un accord au sein de la communauté des utilisateurs de la monnaie virtuelle elle-même" ([26]Financial Action Task Force, 2014, p.4). Ainsi, bien que certaines monnaies virtuelles telles que le dollar Linden et les pièces Avination Care puissent être converties en monnaie réelle, cela peut ne pas toujours être le cas. De nombreuses devises dites «fermées» et ne peuvent être converties que dans un seul sens. Elles ne peuvent pas être échangées contre des devises du monde réel (Financial Action Task Force, 2014).

Le terme crypto-monnaie fait référence à une monnaie virtuelle mathématique, décentralisée, convertible (ou «ouverte»), dont les processus sont protégés par une cryptographie et présentent une valeur équivalente en monnaie réelle (Financial Action Task Force, 2014). Le concept de crypto-monnaie a été introduit pour la première fois en 1983 par Chaum qui a proposé un système bancaire numéraire, composé de pièces aveuglément signées, créant ainsi des «paiements irrécupérables» ([27]Chaum David, 1982, p.200). Ces signatures aveugles empêchent les institutions financières de relier les transactions aux utilisateurs, offrant ainsi une forme d'insignifiance (Bonneau Joseph et al., 2015). Depuis la naissance de ce concept, de multiples variations ont été développées, établissant des systèmes qui permettent un anonymat et une efficacité accrus durant le processus de transaction ([28]Camenisch Jan et al., 2005).

Par conséquence, on craint que les crypto-monnaies deviennent de plus en plus attrayantes pour les organisations criminelles et les cyber terroristes (Meiklejohn Sarah, 2013). La capacité des crypto-monnaies à éviter les contrôles et les réglementations

[26] Groupe d'action financière (2014). "Monnaies virtuelles - définitions clés et risques potentiels de LBC / FT", Groupe d'action financière, disponible à : www.fatfgafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[27] Chaum, David, (1982). Signature aveugle pour les paiements introuvables, Advances in Cryptology-Eurocrupt 82, Plenum Press, New York, NY, pp. 199-203.

[28] Jan Camenisch, Susan Hohenberger, Anna Lysyanskaya, (2005). "Compact e- cash", *Advances in Cryptology – EUROCRYPT*, Springer, Berlin Heidelberg, pp. 302-321.

des devises par les institutions financières lors de la réalisation de transactions, crée une méthode attrayante de transfert anonyme des fonds. Les produits de la criminalité, le financement d'activités illicites, l'achat de matériel illicite et la possibilité accrue de fraude ont tous été un effet secondaire confirmé du contournement des contrôles réglementaires ([29]Middlebrook Stephen T., Hughes, Sarah Jane, 2014). Ainsi, les crypto-monnaies exposent «les utilisateurs aux risques que les régimes réglementaires visent à atténuer et entravent les efforts des autorités et des banques chargées de combattre la fraude, le blanchiment d'argent et l'évasion fiscale» ([30]Pflaum Isaac et Hateley Emmeline, 2014, p.134).

L'attention générale portée à l'utilisation abusive des crypto monnaies pour compléter les transactions illicites a été récemment mise en évidence suite aux informations recueillies concernant la saisie des actifs du prétendu fondateur de la «Route de la Soie» (Silk Road), Ross William Ulbricht. Le FBI a confirmé qu'une somme équivalente à 33,6 millions de dollars américains était stockée sur un portefeuille Bitcoin affilié au site Web illicite (Federal Bureau of Investigation, 2013). Bien que le site internet prétendument entretenu par Ulbericht ait été fermé à la suite de l'enquête, des sites similaires comme "Alpha Bay" fonctionnent encore sur Internet. Ces formes de marché attirent de plus en plus les criminels et les cyber terroristes, en particulier ceux qui recherchent un environnement moins risqué, car l'adoption de ce processus réduit le risque «d'échanges violents entre acheteurs et vendeurs» ([31]Martin James, 2014, p.353). De plus, il réduit davantage l'effet déstabilisateur que les opérations d'application de la loi ont sur la distribution illicite des marchés (Bouchard Martin, 2007). Comme l'a observé Bouchard (2007), l'impact d'un choc externe sur un marché illicite, tel que l'exposition d'un concessionnaire sur « la route de la soie » est minime, en raison du rôle négligeable des acteurs par rapport à la taille du marché.

L'attrait de ces sites est encore accru par leur capacité à accroître l'efficacité, l'immédiateté et la rentabilité sur un marché criminel mondial (Serious Organized Crime

[29] Middlebrook Stephen T., Hughes, Sarah Jane, (2014). "Réglementer les cryptomonnaies aux États-Unis: problèmes actuels et orientations futures", William Mitchell Law Review, vol. 40, pp. 813-848.

[30] Pflaum Isaac et Hateley Emmeline, (2014). "Un peu de problème: la régulation nationale et extraterritoriale de la monnaie virtuelle à l'ère de la désintermédiation financière", Georgetown Journal of International Law, vol. 45 No. 4, pp. 134.

[31] Martin James, (2014). "Perdu sur la route de la soie: la distribution de drogue en ligne et le" Cryptomarket "", Criminology and Criminal Justice, Vol. 14 No. 3, pp. 351-367.

Agency, 2006). Ainsi, en adoptant des crypto-monnaies sur ces sites Web illicites, les transactions de matériel illicite comportent moins de risques pour l'acheteur que les transactions traditionnelles effectuées par l'intermédiaire d'institutions financières tierces.

6.5 Terrorisme et cybercriminalité

La proportion de la cybercriminalité qui peut être attribuée directement ou indirectement aux terroristes est difficile à déterminer. Cependant, il existe des liens entre les groupes terroristes et les criminels qui permettent aux réseaux terroristes de se développer à l'échelle internationale en tirant parti des ressources informatiques, des activités de blanchiment d'argent ou des routes de transit exploitées par des criminels. Par exemple, les attentats au Royaume-Uni en 2005 montrent que des groupes de terroristes sont déjà secrètement actifs dans des pays dotés de grands réseaux de communication et d'infrastructures informatisées. De plus, ils ont à leur disposition un grand nombre de travailleurs hautement qualifiés. Les responsables de la police de Londres pensent que les terroristes ont obtenu des explosifs de haute qualité pour les attentats de 2005 contre le Royaume-Uni, des groupes criminels basés en Europe de l'Est (Rollie Lal, 2005).

Un procès récent au Royaume-Uni a révélé un lien important entre les groupes terroristes islamiques et la cybercriminalité. En juin 2007, trois résidents britanniques, Tariq al-Daour, Waseem Mughal et Younes Tsouli, ont plaidé coupables et ont été condamnés d'avoir utilisé Internet pour inciter au meurtre. Ces trois hommes avaient utilisé des cartes de crédit volées dans les boutiques en ligne pour acheter des articles nécessaires pour leurs camarades djihadistes. Des articles tels que des lunettes de vision nocturne, des tentes, des GPS par satellite, des centaines de téléphones portables prépayés et plus de 250 billets d'avion. Pour effectuer tous ces achats, ils ont utilisé 110 cartes de crédit volées. Encore, 72 autres cartes de crédit volées ont été utilisées pour enregistrer plus de 180 domaines Internet sur 95 sociétés d'hébergement Web différentes. Le groupe a également blanchi l'argent facturé à plus de 130 cartes de crédit volées par le biais de sites de jeux en ligne. Au total, le trio a facturé plus de 3,5 millions de dollars à partir d'une base de données contenant 37 000 numéros de cartes

de crédit volés, y compris les noms et adresses des titulaires de compte, leurs dates de naissance, leurs créditeurs et leurs limites de crédits ([32]Krebs Brian, 2007).

Les cybercriminels concluent des alliances avec des trafiquants de drogue en Afghanistan, au Moyen-Orient et ailleurs, où des fonds illicites ou d'autres activités lucratives comme le vol de cartes de crédit servent à soutenir des groupes terroristes ([33]Bergen Peter, 2006). Les trafiquants de drogue sont parmi les utilisateurs les plus répandus du cryptage pour la messagerie Internet et sont capables d'engager des informaticiens de haut niveau pour éviter l'application de la loi, coordonner les expéditions de médicaments et blanchir de l'argent. Les régions possédant d'importants marchés de narcotiques, telles que l'Europe occidentale et l'Amérique du Nord, possèdent également une infrastructure technologique optimale et des nœuds commerciaux ouverts qui répondent de plus en plus aux besoins transnationaux des groupes criminels et terroristes (Curtis Glenn et al., 2002). Des fonctionnaires de l'Agence américaine de lutte contre la drogue (DEA) ont signalé en 2003 que 14 des 36 groupes figurant sur la liste des organisations terroristes étrangères du Département d'État américain étaient également impliqués dans le trafic de drogue. Un rapport publié en 2002 par la Division Fédérale de la Recherche à la Bibliothèque du Congrès révélait une «implication croissante des groupes terroristes et extrémistes islamiques dans le trafic de drogue» et une coopération limitée entre différents groupes terroristes impliquant le trafic de drogue et le trafic d'armes (LaVerle Berry et al., 2002). Par conséquent, les responsables de la DEA devraient soutenir que la guerre contre la drogue et la guerre contre le terrorisme doivent être liées (Eddy Mark, 2003).

Lors d'une audition du Sénat en mars 2002, des représentants du Département d'État ont également indiqué que certains groupes terroristes utilisaient le trafic de drogue comme moyen d'obtenir du financement tout en affaiblissant leurs ennemis (en exploitant leur désir de drogues) en Occident (Beers Rand et al., 2002).

La culture de pavot en Afghanistan fournit de la résine pour produire plus de 90% de l'héroïne mondiale, soutenant un trafic de drogue estimé à 3,1 milliards de dollars. Les

[32] Brian Krebs, (2007). "Trois ont travaillé sur le Web pour aider les terroristes", The Washington Post, 6 juillet 2007, p. D01.

[33] Peter Bergen, (2006). “The Taliban, Regrouped and Rearmed,” *The Washington Post*, September 10, 2006, p. B1. Helen Cooper, “NATO Chief Says More Troops Are Needed in Afghanistan,” *The New York Times*, September 22, 2006, p. 10.

rapports indiquent que les revenues du trafic de drogue en Afghanistan sont utilisées pour financer des groupes terroristes et insurgés qui opèrent dans ce pays. Par la suite, des rapports de renseignement américains en 2007 démontrent que "Al-Qaïda en Afghanistan" a été revitalisé et a restauré ses niveaux d'opération d'avant le 11 septembre 2001, et il est actuellement dans une meilleure position pour attaquer les pays occidentaux, ([34]Lee Matthew et al., 2007).

Les trafiquants de drogue ont les moyens financiers d'embaucher des informaticiens capables d'utiliser des technologies qui rendent les messages Internet difficiles ou impossibles à déchiffrer et qui permettent aux organisations terroristes de transcender les frontières et d'opérer sur le plan international avec moins de risque de détection. De nombreux spécialistes techniques hautement qualifiés, disponibles à la location, viennent des pays de l'ex-Union soviétique et du sous-continent indien (Shelly Louise, 2004). Certains de ces spécialistes techniques ne travailleraient pas volontiers pour des organisations criminelles ou terroristes, mais pourraient être induits en erreur ou ne pas être conscients des objectifs politiques de leurs employeurs. D'autres encore accepteraient de fournir de l'aide parce que les emplois légitimes bien rémunérés sont rares dans leur région.

6.6 Groupes terroristes liés aux pirates.

Les liens entre les pirates informatiques et les cyber terroristes ou les pays qui parrainent le cyber terrorisme sont difficiles à confirmer. L'appartenance aux groupes de pirates informatiques les plus qualifiés est parfois très exclusive et limitée aux individus qui développent, démontrent et partagent uniquement les uns avec les autres, leur ensemble d'outils de hackers sophistiqués, le plus étroitement surveillé. Ces groupes de hackers exclusifs ne recherchent pas l'attention parce que le maintien du secret leur permet de fonctionner plus efficacement. Certains groupes de pirates peuvent aussi avoir des intérêts politiques supranationaux, religieux ou idéologiques sociopolitiques,

[34] Matthew Lee et Katherine Shrader, (2007). Al-Qaïda a été reconstruite, avertit l'agence américaine Intel, Associated Press, 12 juillet 2007, disponible à : http://news.yahoo.com/s/ap/20070712/ap_on_go_pr_wh/us_terror_threat_32;_ylt=AuURr2eP8AhBrfHyTOdw714Gw_IE.
Associated Press, «La récolte de pavot en Afghanistan pourrait rapporter plus que le record de 2006, selon l'ONU», International Herald Tribune, 25 juin 2007 , disponible à :http://www.iht.com/articles/ap/2007/06/25/asia/AS-GEN-Afghan-Drugs.php

alors que d'autres groupes de pirates peuvent être motivés par le profit ou être liés au crime organisé et être disposés à vendre leurs services, quels que soient les intérêts politiques impliqués.

Les informations sur les vulnérabilités informatiques sont désormais disponibles en ligne sur le «marché noir» des hackers. Par exemple, une liste de 5 000 adresses d'ordinateurs qui ont déjà été infectés par des logiciels espions et qui attendent d'être contrôlés à distance dans le cadre d'un «réseau de robots» automatisé, peut être obtenue pour environ 150 à 500 dollars. Les prix des informations sur les vulnérabilités informatiques pour lesquelles il n'existe pas encore de logiciel correctif, se situent entre 1 000 et 5 000 dollars. Les acheteurs de cette information sont souvent des groupes criminels organisés, divers gouvernements étrangers et des entreprises qui font du spam (Francis Bob, 2005).

6.7 Pourquoi les terroristes utilisent l'espace cybernétique

Avant de clarifier pourquoi les terroristes utilisent le cyberespace dans la réalisation des activités du cyber terroriste, nous devons définir les étapes à travers lesquelles un processus terroriste a lieu.

Selon la recherche d'experts dans le domaine du cyber terrorisme, il est généralement établi que le terrorisme se compose de plusieurs étapes nécessaires pour effectuer un acte cyber terroriste. Toutes ces phases s'appliquent au cyber terrorisme collectif, alors que le cyber terrorisme individuel évite habituellement, la première phase qui est la diffusion de l'idéologie ([35]Perisa Ivona, 2012).

Connaissant et tenant compte de ces phases à travers lesquelles passe un processus cyber terroriste, nous pouvons créer une stratégie d'action contre le cyber terrorisme.

Devrait-on appliquer une stratégie préventive afin d’empêcher le cyber terrorisme ou devrait-on prendre des actions militaires selon la situation présentée? En tout cas, pour affronter efficacement ce phénomène, les Etats doivent avoir les capacités nécessaires.

[35] Ivona Pastor Perisa, (2012). "Formes organisationnelles de l'organisation terroriste moderne", Polemos 15 (2012) 2: p. 139-156.

En déterminant les différentes étapes du déroulement d'un cycle cyber terroriste et en prenant en considération les possibilités offertes par le cyberespace, nous pouvons conclure que le cyberespace peut être utilisé pour la réalisation des activités suivantes:

- Appel à l'idéologie

- Recrutement

- La mise en réseau

- La communication

- Collection de fonds financiers

- Méthode de transfert de fonds financiers

- Utilisation de fonds financiers

- Éducation et formation

- Organisation et réalisation des attaques terroristes et cyber-attaques. ([36]Wilson Clay et al 2007).

Les organisations de cyber terroristes utilisent de plus en plus le cyberespace pour mener leurs attaques terroristes. Les cyber terroristes utilisent Internet et le réseau de communication mondial pour recruter des membres, recueillir des renseignements, lever des fonds légalement ou illégalement, organiser et coordonner leurs activités, fournir des documents de voyage et distribuer illégalement du matériel de propagande. Par exemple certains terroristes afghans, comme Oussama ben Laden autrefois, possèdent des ordinateurs, du matériel de communication et des lecteurs pour stocker de grandes quantités de données utiles pour leurs opérations. L'organisation terroriste du Moyen-Orient, le Hamas, a utilisé le messager Internet (chat) et le courrier électronique pour planifier et coordonner les opérations à Gaza, en Cisjordanie et au Liban. Le deuxième groupe du Moyen-Orient, le Hezbollah a géré plusieurs sites Web à des fins de

[36] John Rollins et Clay Wilson, (2007). Capacités terroristes pour la cyberattaque: Aperçu et questions de politique (Rapport CRS RL33123). Disponible à : https://fas.org/sgp/crs/terror/RL33123.pdf

propagande, pour décrire les attaques contre Israël et diffuser des nouvelles et des informations (Wilson Clay et al 2007).

Pour effectuer des attaques cyber terroristes, les pirates informatiques doivent disposer d'informations pertinentes, mais comme chaque développeur n'est pas pirate, aucun pirate n'a besoin de connaître la programmation informatique. La plupart des développeurs créent des « vers » informatiques que la planification ultérieure pousse vers un objectif spécifique lequel doit répondre aux caractéristiques d'une attaque terroriste. Dans ce cas, l'attaque est qualifiée d'un acte cyber terroriste.

En 2003, un « ver » informatique (Slammer) a été inséré et a provoqué un ralentissement du contrôle du système énergétique aux États-Unis. Il en est résulté que huit États américains et deux provinces canadiennes et alors, près de 50 millions de personnes sont restés sans électricité. En août 2006, l'un des quatre e-mails de l'OTAN a été exposé à une série d'attaques DOS par un dispositif. Ce dernier a été détecté par les dispositifs de surveillance et l'attaque a été bloquée et donc le serveur reconfiguré (Rollins John et al., 2007).

Le cas qui a provoqué une panique mondiale s'est produit fin 2008 lorsqu'un groupe de hackers appelé "équipe de sécurité Grecque" a fait irruption dans les ordinateurs du CERN - le Centre européen pour la recherche nucléaire – et a pris le contrôle de l'un des détecteurs du grand collisionneur de hadrons (LHC) - le plus grand accélérateur de particules. Les hackers, une fois dans le système, ont mis en place une fausse page sur le site du CERN, se moquant des experts en charge du système informatique. Les représentants du CERN ont indiqué que cela ne causait aucun dommage. Pourtant, le fait que les détecteurs et l'équipement général soient exposés à une menace électronique est au moins désagréable.

6.8 Le terrorisme dans le cyberespace

L'anonymat offert par Internet est très attrayant pour les terroristes modernes. En raison de leurs croyances et de leurs valeurs extrémistes, les terroristes ont besoin de l'anonymat pour exister et opérer dans des environnements sociaux qui peuvent ne pas correspondre à leurs opinions idéologiques particulières ou à leurs activités. Internet

offre cet anonymat, en plus d'un accès facile et universel avec les options d'envoi de messages, d'envoi d'e-mails ou de téléchargement ou d'informations. Une fois ces objectifs atteints, Internet permet aux terroristes de disparaître dans le noir. Par conséquence, les terroristes sont devenus de plus en plus sophistiqués en exploitant des plateformes en ligne pour des communications anonymes. Par exemple, les terroristes peuvent utiliser un simple compte de courrier électronique en ligne pour la "mort" (dead dropping) électronique des communications. Cela se réfère à la création d'un brouillon de message, qui reste non envoyé et laisse donc un minimum de traces électroniques, mais auquel n'importe quel terminal Internet du monde entier peut accéder par plusieurs personnes ayant le mot de passe approprié. Cette pratique permet aux messages d'atteindre un public large mais anonyme, et d'être édités et supprimés avec peu de preuves comme s’ils n’aient jamais existé.

Les technologies émergentes ont rendu la communication en ligne plus facile et moins coûteuse pour les terroristes et de plus en plus difficile pour les autorités de surveiller ces communications. Courriels, salons de discussion, téléphones mobiles, communications par SMS (Short Message Service), communications VoIP (Voice-over-Internet Protocol), médias sociaux, partage de vidéos en ligne, mondes virtuels et sites de micro-blogs ne sont pas seulement des plateformes idéales pour les terroristes, mais elles leurs permettent aussi de se cacher facilement. A part les nombreuses plates-formes, les appareils de communication alternatifs prolifèrent des conversations, vidéos ou images qui peuvent être placés sur les téléphones mobiles, ordinateurs portables et tablettes, médias sociaux, sites Web, appareils électroniques grand public, tels que lecteurs de musique portables ou appareils de jeux. Tout cela peut être obtenu sans fournir aucune information d'abonné. Une abondance de mesures et de technologies plus sophistiquées augmente également la difficulté d'identifier l'auteur, le destinataire ou le contenu des communications en ligne des terroristes. Ceux-ci incluent des outils de chiffrement et des logiciels d'anonymisation qui sont facilement disponibles en ligne à télécharger.

Ces avantages ne sont pas passés inaperçus par les organisations terroristes, quelle que soit leur orientation spécifique. Les islamistes et les marxistes, les nationalistes et les séparatistes, les fondamentalistes et les extrémistes, les racistes et les anarchistes

trouvent tout cela séduisant. Aujourd'hui, toutes les organisations terroristes actives tiennent des sites Web et beaucoup d'entre elles gèrent plus d'un site Web et utilisent plusieurs langues.

L'utilisation variée du cyberespace par les cyber terroristes, peut être classé en deux catégories: la communicative et l'instrumentale. L'utilisation communicative comprend la diffusion de la propagande, le lancement de campagnes de guerre psychologique, la sécurisation des communications internes et la radicalisation des recrues (Weimann Gabriel, 2006a, 2006b). L'utilisation instrumentale inclue l'enseignement en ligne et la formation de terroristes, et l'établissement de «camps d'entraînement virtuels» pour les futurs assaillants (Weimann Gabriel, 2005a, 2006b, 2007a, 2007b, 2008b, 2009d). Les terroristes font davantage usage des plateformes en ligne ayant comme objectif: (1) la guerre psychologique, (2) la propagande, (3) l'endoctrinement en ligne, (4) le recrutement et la mobilisation, (5) l'exploration de données, (6) l'entraînement virtuel, (7) le cyber planning et la coordination, et (8) la collecte de fonds.

6.9 Cybercriminalité: menaces, tendances, outils et infrastructure.

Les technologies de l'information et de la communication, Internet en particulier, qui relient des ordinateurs à des distances diverses dans le monde entier, offrent une excellente opportunité pour les organisations ou leurs membres. Les avantages d'Internet sont nombreux pour l'organisation et la communication et le partage des données, des services, etc. Mais, en même temps, le recours à Internet et aux technologies de l'information et de la communication rend ces groupes vulnérables aux menaces connues sous le nom de cybercriminalité.

Selon le Comité d'experts de MONEYVAL pour la lutte contre le blanchiment d'argent et le financement du terrorisme au sein du Conseil de l'Europe, la cybercriminalité ou le cyber crime est composé de:

- Infractions contre les données et systèmes informatiques: ceci inclut en particulier les "infractions C.I.A." contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes et comprenant:

L’accès illégal, par exemple, par le biais du «piratage», de la tromperie ou d'autres moyens,

L'interception illégale de données informatiques

L'interférence des données, y compris l'endommagement, la suppression, la détérioration, l'altération ou la suppression des données informatiques,

L'interférence du système, y compris l'entrave grave au fonctionnement d'un système informatique, par exemple, par des attaques par déni de service contre des infrastructures critiques,

L'utilisation abusive de dispositifs, qui se réfère, par exemple, à la production, à la vente ou à la mise à disposition d'autres programmes ou d'autres dispositifs ou outils pour commettre des «délits C.I.A.»,

Les infractions commises à l’aide des données et des systèmes informatiques: cela inclut des infractions telles que la fraude et la pornographie ou des infractions liées aux droits de propriété intellectuelle qui ont un impact différent si elles sont commises par des systèmes informatiques,

La falsification et la fraude informatiques,

Les infractions liées au contenu, notamment la pornographie enfantine et l'exploitation et les abus sexuels d'enfants, le racisme et la xénophobie, ainsi que la sollicitation et l'incitation au crime, la fourniture d'instructions et l'offre pour commettre des crimes tels que le meurtre, le viol, la torture, le sabotage et le terrorisme. Cette catégorie comprend également le cyber-harcèlement, la cyber intimidation, la diffamation et la diffusion de fausses informations par Internet et les jeux d'argent sur Internet,

Iles infractions liées à la violation du droit d'auteur et d’autres droits concernant la reproduction et l'utilisation non autorisées de programmes informatiques, audio / vidéo et d’autres formes d'œuvres numériques ou de bases de données et de livres (comité MONEYVAL).

Le fait que les cyber crimes économiques puissent inclure une composante destinée à être utilisée dans les systèmes informatiques, fait du cyber terrorisme un sujet très vaste

et important. Déjà, le cyber terrorisme est un phénomène transfrontalier par sa nature. Son but est d'obtenir des avantages économiques à travers diverses formes de fraude et de criminalité économique et organisée. Certaines formes de ce type de cyber terrorisme sont nouvelles et représentent de nouveaux crimes encore inexploitées par les forces de l'ordre. Dans ce monde, il existe une «économie souterraine numérique» qui ne cesse de croître et qui comprend le crime organisé, les experts informatiques (IT), les pirates informatiques, les «mules d'argent» et d'autres personnes dont les services peuvent être loués. Cette économie souterraine est désignée pour fournir l'outil et les services nécessaires et faciliter la perpétration du cyber terrorisme ou pour assurer la couverture des traces des produits de la criminalité.

Les groupes de cyber terroristes n'ont pas nécessairement besoin de développer leur propre expertise sur Internet, car ces compétences ou services peuvent être recrutés pour répondre à leurs besoins, créant ainsi, une sorte de connexion de réseau transactionnelle entre les «petits délinquants» et le crime organisé, situé dans différentes parties du monde. Évidemment, ceci suggère de grandes quantités de flux d'argent criminel sur Internet.

6.10 Capacités terroristes pour Cyber attaque.

Certains experts estiment que des cyber attaques avancées ou structurées contre plusieurs systèmes et réseaux, y compris la surveillance ciblée et le test de nouveaux outils de piratage sophistiqués, pourraient nécessiter deux à quatre ans de préparation, alors qu'une cyber attaque coordonnée complexe, causant une perturbation massive des systèmes intégrés et hétérogènes nécessitent 6 à 10 ans de préparation, ([37]Denning Dorothy, 2004). Ce fait qui démontre que les hackers consacrent beaucoup de temps à une planification détaillée avant de lancer une cyber attaque, a également été décrit comme une «marque de fabrique» des précédentes attaques terroristes physiques et des attentats à la bombe lancés par Al-Qaïda.

[37] Dorothy Denning, (2004). «Niveaux de cyberterrorisme: Terroristes et Internet», disponible à : http://www.cs.georgetown.edu/~denning/infosec/Denning-Cyberterror-SRI.ppt, présentation, et Zack Phillips, «Homeland Tech Shop Wants pour lancer des idées de cybersécurité », CQ Homeland Security, 14 septembre 2004 disponible à : http://homeland.cq.com/hs/display.do?docid=1330150&sourcetype=31&binderName=news-all

Il est difficile de déterminer le niveau d'intérêt ou les capacités des groupes terroristes internationaux à lancer une cyber attaque efficace. Un rapport publié en 1999 par le Centre pour l'étude du terrorisme et de la guerre irrégulière à la Naval Postgraduate School concluait que les cyber attaques seraient probablement utilisées par des groupes de cyber terroristes dans le but de compléter les attaques terroristes physiques traditionnelles (Centre of Study Terrorism).

Certains observateurs ont déclaré qu'Al Qaïda ne considère pas la cyber attaque comme importante pour atteindre ses objectifs, préférant les attaques qui infligent des pertes humaines ([38]Swartz John, 2004). D'autres observateurs estiment que les groupes les plus susceptibles d'envisager et d'utiliser la cyber attaque et le cyber terrorisme sont les groupes terroristes opérant dans les sociétés postindustrielles (comme l'Europe et les États-Unis) plutôt que les groupes terroristes internationaux opérant dans les régions en développement concernant la technologie à pointe.

Cependant, d'autres sources signalent qu'Al-Qaïda a pris des mesures pour améliorer le secret organisationnel grâce à une utilisation plus active et sophistiquée de la technologie. Les preuves suggèrent que les terroristes d'Al Qaïda ont largement utilisé Internet pour planifier leurs opérations du 11 septembre 2001 ([39]Kaplan David, 2003). Au cours des dernières années, des groupes d'Al-Qaïda ont utilisé de nouveaux services téléphoniques sur Internet pour communiquer avec d'autres cellules terroristes à l'étranger. Khalid Shaikh Mohammed, l'un des cerveaux de l'attaque contre le World Trade Center, a utilisé un logiciel spécial de discussion sur Internet pour communiquer avec au moins deux pirates de l'air. Ramzi Yousef, condamné à la réclusion à perpétuité pour l'attentat à la bombe contre le World Trade Center (WTC), avait suivi une formation d'ingénieur électricien et prévoyait d'utiliser des systèmes électroniques sophistiqués pour faire exploser des bombes sur 12 avions américains partant d'Asie pour les États-Unis. Il a également utilisé un cryptage sophistiqué pour protéger ses données et empêcher les forces de l'ordre de décoder ses plans en cas où il serait capturé (Windrem Robert, 2003).

---

[38] John Swartz, (2004). «L'impact du cyberterrorisme, la défense sous surveillance», USA Today, 3 août 2004, p. 2B.

[39] David Kaplan, (2003). “Playing Offense: The Inside Story of How U.S. Terrorist Hunters Are Going after Al Qaeda,” *U.S. News & World Report*, June 2, 2003, pp. 19-29.

Des mesures de sécurité physique actuellement plus strictes et largement appliquées aux États-Unis pourraient encourager les groupes de cyber terroristes à explorer les cyber attaques afin de réduire le risque de détection de leurs opérations (Enders Walter, 2004). Cependant, d'autres observateurs de la sécurité estiment que les organisations terroristes pourraient être réticentes à lancer une cyber attaque, car cela entraînerait moins de drames immédiats et aurait un impact psychologique plus faible qu'une attaque à la bombe plus conventionnelle. Ces observateurs estiment qu'à moins qu'une cyber attaque puisse entraîner des dommages physiques ou des effusions de sang, elle ne sera jamais prise en compte comme l'est une attaque terroriste nucléaire, biologique ou chimique (Lewis James, 2002).

6.11 Stratégie de communication d'ISIS

Les groupes cyber terroristes utilisent une stratégie de communication basée sur la mise en évidence de certains appels. Haroro J. Ingram a identifié trois stratégies médiatiques suivies par ISIS: «l'utilisation d'une approche multidimensionnelle et multiplateforme qui cible simultanément aussi bien « les amis que les ennemis » pour améliorer la portée, la pertinence et la résonance de ses messages, la synchronisation du récit et de l'action pour maximiser les «effets» opérationnels et stratégiques sur le terrain et la place centrale de la «marque» de l'État islamique dans toute sa campagne» ([40]Haroro J. Ingram, 2014).

D'autre part, ISIS publie également des images qui montrent son côté charitable, comme son aide aux personnes âgées ou l'organisation de la vie dans les villes qu'il contrôle. Certains montrent également des combattants se détendre, nager, manger et jouer avec des chats. James Farwell affirme que ces «images plus chaleureuses visent à communiquer le message que, bien que strictement islamique, ISIS est synonyme de la promotion du bien-être des gens, pas de l'assassinat des citoyens» ([41]Farwell P. James, 2014). Pourtant, ce n'est pas le seul message que l'ISIS veut communiquer, car l'intention principale derrière la publication de ces images positives est de donner l'impression au monde extérieur ainsi qu'aux personnes qu'il contrôle que le groupe est

[40] Haroro J. Ingram, (2014). "Trois Traits de la Guerre d'Information de l'Etat Islamique", The RUSI Journal 159, no. 6 (2014): p. 4.

[41] James P. Farwell, (2014). "La stratégie médiatique de l'Etat islamique", Survival 56, no. 6 (2014): p. 50.

fort et résilient puisqu'il n'est pas affecté par les opérations militaires en cours contre ses combattants.

Enfin, et surtout, ISIS utilise la propagande et la désinformation pour diffuser son idéologie au plus grand nombre possible de personnes et dans différentes langues. Le président Obama a révélé certaines des stratégies d'ISIS dans un discours prononcé en février 2015: «Les vidéos de haute qualité, les magazines en ligne, les médias sociaux, les comptes Twitter des terroristes, tout est conçu pour cibler les jeunes en ligne, dans le cyberespace». (Kathy Gilsinan, 2015). Le New York Times décrit avec justesse la stratégie médiatique de l'ISIS comme Jihad 3.0 en raison de sa campagne médiatique très sophistiquée qui utilise la «propagande multidimensionnelle», avec des tournages de haute technologie à l'aide d'équipement de montage (Arabiya Al, 2014). Le terme est dérivé à l'origine de Web 3.0, développé à partir du Web 2.0. En effet, ISIS utilise pleinement des technologies différentes qui ne se limitent pas aux médias sociaux, en particulier Twitter, mais s'étendent aux jeux vidéo, au piratage par son armée des califats, aux applications et au Dark Web.

D'autres plates-formes médiatiques sont activement exploitées par ISIS. En avril 2014, ISIS "a présenté une application Android, appelée ***L'aube de Glad Tidings***, qui exploite les comptes des utilisateurs de Twitter pour partager des tweets liés à ISIS." ISIS a récemment déménagé sur un autre réseau social appelé "Diaspora". Ainsi qu'à d'autres réseaux et sites Web moins connus comme Friendica, Quitter, Justpaste, Ask.fm, Soundcloud et Mixlr après que ses comptes Twitter aient été bloqués. En termes d'influence en ligne, il semble que ISIS dispose d'un large réseau de partisans et / ou de sympathisants qui existent non seulement dans la région du Moyen-Orient mais aussi en Amérique du Nord et en Europe ([42]Berger James et al., 2015).

Il est important de noter ici que les images et vidéos de décapitation et de destruction choquantes qui sont diffusées par ISIS visent à sensibiliser le groupe et ses activités aux techniques de publicité de choc utilisées par certaines sociétés commerciales qui sont bien documentées dans des recherches scientifiques antérieures. Il s'agit d'une

[42] Berger M. James et Jonathon Morgan, (2015). "Le recensement Twitter d'ISIS: Définir et décrire la population des partisans d'ISIS sur Twitter", The Brookings Project sur les relations des Etats-Unis avec le monde islamique 3, no. 20, p. 2, (2015), http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf

autre stratégie persuasive, car ISIS tente de se définir comme un groupe sauvage qui défend l'islam contre les infidèles. À cet égard, les sites de réseaux sociaux sont principalement utilisés pour attirer l'attention et attirer des victimes potentielles, après quoi d'autres technologies de communication sont utilisées, notamment les services mobiles comme Viber, Surespot, WhatsApp, FaceTime, Kik, Skype et Telegram ([43]Jaffer Nabeelah, 2015). En bref, les différentes plateformes utilisées et les stratégies médiatiques suivies par ISIS qui semblent se compléter, indiquent que ce groupe mène un nouveau Jihad qui va au-delà de ce que propose le Web 2.0, le rendant beaucoup plus efficace que les organisations terroristes traditionnelles comme Al-Qaïda.

En octobre 2014, trois adolescentes de Denver, au Colorado, avaient été disparues de l'école secondaire (Brumfield Ben, 2014). Les autorités allemandes les ont interceptées à l'aéroport de Francfort et les ont renvoyées aux États-Unis où elles ont été interrogées par des agents du Federal Bureau of Investigation (FBI). Les filles étaient soupçonnées de se rendre en Turquie puis en Syrie pour rejoindre des extrémistes islamiques, bien que les détails de l'affaire aient été scellés en raison de leur âge (15 à 17 ans). Tous les trois avaient parcouru des sites Web extrémistes pour rechercher comment se rendre en Syrie. Plus tôt dans l'année, Shannon Conley, 19 ans, avait été arrêtée à l'aéroport international de Denver en route vers la Syrie via Francfort et la Turquie. Chargée de conspiration pour aider l'État islamique (IS, État islamique d'Iraq et al Sham [ISIS], également connu sous le nom de Daesh) en Syrie, elle a avoué qu'elle avait été «radicalisée» ([44]Baker Beall C. et al., 2015) par un Tunisien militante qu'elle avait rencontré en ligne et qu'elle avait l'intention de marier. Conley a dit que sa connaissance de l'Islam était basée uniquement sur sa propre recherche en ligne (Awan Akin, 2015).

De même, des histoires alarmantes de radicalisation sont régulièrement répétées dans les médias et au-delà. En effet, selon certains des rapports les plus hystériques, plus de citoyens britanniques ont rejoint ISIS en Irak et en Syrie que enrôlé dans la Réserve de l'armée américaine en 2013 (plusieurs centaines comparé à 170), (McTague Tom, 2014). Des rapports comme ceux-ci sont invariablement accompagnés de deux types

[43] Nabeelah Jaffer, (2015). "The Secret World of ISIS Brides: 'U dnt hav 2 pay 4 ANYTHING if u r wife of a martyr,'" The Guardian, June 24, 2015, disponible à:http://www.theguardian.com/world/2015/jun/24/isis-brides-secret-world-jihad-western-women-syria

[44] Christopher Baker-Beall, Charlotte Heath-Kelly, and Lee Jarvis, eds.,(2015). "Counter-Radicalisation: Critical Perspectives" (Abingdon: Routledge: 2015), pp. 1–13.

de questions ([45]Crenshaw Martha, 1981). La première est une question de causalité directe: ***Pourquoi les jeunes hommes et femmes veulent-ils quitter une vie souvent confortable pour rejoindre des extrémistes violents dans des pays lointains?*** La deuxième, c'est une question de causes favorables: ***Quelle est l'importance de l'influence d'Internet dans ce processus? Quel rôle joue-t-elle en encourageant ou en facilitant les efforts pour participer à des campagnes telles que celles menées par Al-Qaïda ou l'EI?***

6.12 Stratégies de propagande en ligne

Ayman al-Zawahiri, actuel chef d'Al-Qaïda et ancien député d'Oussama ben Laden, a déclaré: «Nous [Al-Qaïda] sommes en bataille, dont plus de la moitié de se déroule sur le champ de bataille des médias. Nous sommes dans une bataille médiatique dans une course pour le cœur et l'esprit de notre peuple » (Lieberman Joseph et al., 2008). Al-Qaïda a su adapter sa stratégie médiatique à l'évolution des circonstances et des technologies au fil des ans. Initialement, Al-Qaïda se concentrait sur la propagande, principalement des vidéos et des brochures, en interne à ses propres membres, contribuant à la construction d'un culte de la personnalité autour d'Oussama Ben Laden ([46]Torres Manuel et al., 2006). Au cours des années 1990, Al-Qaïda a commencé à étendre sa portée à travers l'Occident avec des interviews de Ben Laden données à d'éminents journalistes occidentaux tels que Robert Fisk. En même temps, Al-Qaïda s'est efforcé de renforcer son soutien dans le monde musulman, notamment par l'intermédiaire de la chaîne de télévision Al-Jazira, principalement par le biais d'interviews de Ben Laden ou de son adjoint, Ayman al-Zawahiri.

En 2001, la stratégie médiatique d'Al-Qaïda s'est concentrée sur les attaques et les enlèvements, à commencer par un long enregistrement vidéo de l'attaque contre les États-Unis. Ayant attiré l'attention grâce à l'attentat du 11 septembre, Al-Qaïda a déplacé sa propagande au niveau international. Un exemple de son nouvel objectif a été le tournage de l'enlèvement et de l'assassinat du journaliste américain Daniel Pearl en 2002. Avant le 11 septembre, Al-Qaïda avait un site Web qui était seulement en arabe.

[45] Martha Crenshaw, (1981). "The Causes of Terrorism", Comparative Politics 13 (4) (1981), pp. 379-399.

[46] Manuel Torres, Javier Jordán et Nicola Horsburgh, (2006). "Analyse et évolution de la propagande du mouvement djihadiste mondial", Terrorisme et violence politique 18 (3) (2006), pp. 399-421.

Après le 11 septembre, Al-Qaïda a élargi sa campagne de propagande par l'intermédiaire de son site Internet (al_nida.com) créant une division spéciale de production de médias, al-Sahab, pour des cassettes audiovisuelles et des CD distribués par les chaînes de télévision arabes et un nombre croissant de sites djihadistes en différentes langues.

Une grande partie de la propagande visait le courant dominant musulman parce qu'un objectif central de la stratégie de propagande d'Al-Qaïda était de gagner le soutien de la Oumma musulmane. Cependant, Al-Qaïda a reconnu la nécessité d'engager son ennemi sur plusieurs fronts simultanément. Sa propagande visait donc à maximiser l'impact du terrorisme pour infliger des dommages à «l'ennemi lointain» des États-Unis et de ses alliés, et à mobiliser les musulmans occidentaux contre leurs propres gouvernements (Gendron Angela, 2007). Internet a servi de canal principal pour la distribution de matériel de propagande, complété par les chaînes de radio et de télévision par satellite et les médias imprimés. À son tour, Al-Qaïda comptait de plus en plus sur les jeunes adultes ayant des compétences technologiques pour améliorer la qualité du matériel de propagande distribué sur Internet et sur les sites de réseautage social, ainsi que des médias comme Al-Furquan, As-Sahab Media al-Jihad.

Bien qu'EI (État Islamique) tire ses origines de Ben Laden, il s'est scindé décisivement d'Al-Qaïda en février 2014 et son chef actuel est Abu Bakr al-Baghdadi ([47]Stern Jessica et al., 2014). L'idéologie et la stratégie de propagande de l'EI diffèrent de celles d'Al-Qaïda. Bien que la relation entre la politique et la religion soit toujours complexe, ([48]Gunning Jeroen et al., 2011) l'EI a exprimé le désir de revenir à une lecture particulière de l'Islam primitif et de la «Méthodologie Prophétique» se référant à la prophétie et à l'exemple de Mahomet. Suivant, donc, la doctrine « takfiri », l'EI s'engage à purifier le monde en tuant un grand nombre de personnes. En se concentrant sur l'ennemi occidental, EI est plus préoccupé par l'application de la charia dans le califat et l'expansion du territoire local, bien que les récentes attaques coordonnées du 13

[47] Jessica Stern et J. M. Berger, (2014). "ISIS: l'état de terreur" (Londres: William Collins, 2015); Patrick Cockburn, «La montée de l'État islamique: ISIS et la nouvelle révolution sunnite» (Londres: Verso, 2014).

[48] Jeroen Gunning et Richard Jackson, (2011). "Qu'est-ce donc" religieux "au sujet du" terrorisme religieux "?" Critical Studies on Terrorism 4 (3) (2011), pp. 369-388.

novembre 2015 à Paris suggèrent une expansion de leur agenda sur la scène internationale.

La stratégie de propagande d'EI est moderne et sophistiquée, ce qui inclut non seulement l'utilisation intensive des réseaux sociaux en ligne, mais aussi la production de vidéos et de publications de haute qualité. Un exemple très médiatisé est la vidéo de la décapitation du journaliste américain James Foley en août 2014. Le New York Post a publié une image graphique en première page et les captures d'écran de la vidéo ont été largement diffusées sur Twitter. La plupart des médias et des journalistes ont refusé de partager la vidéo ou les photos graphiques, mais EI était conscient que les médias sociaux étaient un moyen facile afin de contourner les contrôles utilisés par les médias pour arrêter la propagation de la propagande.

ISIS publie des rapports annuels sur ses progrès complets avec des illustrations de haute qualité et des infographies. Les rapports sont remplis de métriques d'attaque, une approche qui imite les sociétés modernes, orientées métriques. L'effet est de «communiquer l'efficacité organisationnelle à des parties extérieures, telles que les donateurs, les groupes Al-Qaïda et les adversaires», selon un rapport de l'Institut pour l'étude de la guerre (Bilger Alex, 2014).

La campagne de propagande sophistiquée d'ISIS dépend largement des réseaux sociaux. Des milliers de followers sur Twitter ont installé une application personnalisée appelée Dawn of Glad Tidings qui permet à ISIS d'envoyer des tweets centralisés à travers leurs comptes. Diffusés simultanément, les messages submergent les médias sociaux et étendent la présence en ligne d'ISIS beaucoup plus loin que la normale. En plus des comptes Twitter centralisés, les comptes provinciaux publient des flux en direct sur les opérations ISIS locales. En outre, un fan club en ligne de milliers de partisans de l'ISIS retweet ses hashtags et traduit des messages de l'arabe à des langues occidentales.

Tout ce qui est fait avec la stratégie de propagande d'ISIS a un effet combiné pour construire la «marque». L'ISIS a des avantages supplémentaires par rapport à Al-Qaïda: plus de moyens financiers, d’armes et d’expérience de combat ainsi que l'aide d'un nombre croissant de recrues occidentales qui apportent des compétences

technologiques et des compétences langagières surtout en anglais. ISIS semble également utiliser délibérément l'anglais dans les messages et certaines vidéos, y compris dans le vidéo d'exécution de James Foley dans la vidéo.

Alors que les médias ont tendance à se concentrer sur la barbarie de l'EI, sa stratégie de propagande a été décrite comme étant plus large, englobant cinq récits supplémentaires: (1) la miséricorde (par opposition à la brutalité); (2) la victimisation, par exemple les dommages collatéraux imputés à l'ennemi; (3) les gains de guerre ou militaires; (4) l'appartenance (faire appel à des recrues particulièrement étrangères offrant l'amitié, la sécurité et le sentiment d'appartenance); et (5) l'utopisme, c'est-à-dire non seulement parler du califat mais l'adopter ([49]Winter Charlie, 2015, p. 6). En d'autres termes, la propagande d'EI vise à attirer un large public, et pas seulement des combattants sanguinaires, ce qui aide à expliquer son succès de recrutement.

6.13 Stratégies de radicalisation en ligne

Un rapport du Comité sénatorial américain pour la sécurité intérieure et les affaires gouvernementales sur l'extrémisme islamiste violent et Internet (le sénateur Lieberman 2009) soutient que la campagne Internet d'Al Qaïda affecte le téléspectateur de différentes manières à travers différentes étapes de la radicalisation. Au cours de la première étape de la pré-radicalisation et de l'auto-identification, un individu peut être intéressé à en apprendre davantage sur l'idéologie. Les sites Web les mèneront directement aux pages d'enrôlement du groupe avec des articles sur les croyances religieuses et les idéologies fondamentales. La deuxième étape est celle de l'endoctrinement lorsque les individus, ayant accepté les idéologies et les croyances fondamentales, cherchent des moyens pour participer et promouvoir les objectifs de l'organisation. À l'étape suivante, celle de la jihadisation, Internet permet aux individus de se connecter avec d'autres recrues et membres d'organisations afin de planifier et de mener leurs propres attaques.

Dans le mouvement vers ce qui a été appelé Al Qaïda 2.0, (Post Jerrold, 2007), il se peut qu'Al Qaïda ne dépende pas d'Internet pour le recrutement autant qu'elle dépend

[49] Charlie Winter, (2015). The Virtual “Caliphate”: Understanding Islamic State’s Propaganda Strategy (London: The Quilliam Foundation, 2015). p. 6

de la tendance des individus à rechercher les sites Web et à contacter l'organisation, ou en d'autres termes, se radicaliser et s'auto endoctriner, ([50]White Jeremy, 2012). Le processus de recrutement d'Al-Qaïda via Internet suit une stratégie ascendante selon laquelle les sympathisants, prédisposés à être affectés par la propagande, s'endoctrinent peut-être en s'exposant à plusieurs reprises à ces sites et vidéos.

L'EI est censé opérer l'une des campagnes de médias sociaux les plus sophistiquées. C'est très visible et bien financé. Selon les informations, l'EI bénéficie également de sa richesse considérable, gagnant 3 millions de livres par jour grâce à la contrebande de pétrole, à l'extorsion, au vol et à la traite des êtres humains. Il est délibérément orienté vers les étrangers. Par exemple, l'EI a produit une vidéo de 20 minutes à la fin du mois de Ramadan en août 2014 qui mettait en évidence les variantes du même message répété des moudjahidin: britannique, finlandais, indonésien, marocain, belge, américain et sud-africain. Les messages importants du EI sont généralement publiés simultanément en anglais, en français et en allemand, puis traduits dans d'autres langues, telles que le russe, l'indonésien et l'ourdou. Selon Thomas Hegghammer dans une interview avec BillMoyers.com, "Les combattants étrangers sont surreprésentés, semble-t-il, parmi les auteurs des pires actes de l'Etat Islamique. Donc, ils aident à radicaliser le conflit - le rendre plus brutal. Ils rendent probablement le conflit encore plus difficile, car les gens qui viennent en tant que combattants étrangers sont, en moyenne, plus idéologiques que les rebelles syriens. "

La doctrine exige que les croyants résident dans le califat s'il est possible. Le nombre exact de combattants étrangers est presque impossible à estimer en raison des dangers que cela représente pour les journalistes et les agents de renseignement. Les estimations open-source ont largement varié. La majorité des combattants viennent du Moyen-Orient et d'Afrique du Nord, en particulier de la Tunisie et de l'Arabie Saoudite. Le reste vient d'autres endroits, y compris les anciennes républiques soviétiques, les Amériques et l'Australie. Les estimations du gouvernement sur le nombre d'Américains ont rejoint ISIS varient de 30 à 100. Les estimations pour le Royaume-Uni sont également difficiles mais généralement plus élevées (par exemple, des reportages ont

[50] Jeremy White, (2012). "L'endoctrinement virtuel et le Digihad: l'évolution de la stratégie médiatique d'Al-Qaïda" Small Wars Journal, 19 novembre 2012. Disponible à : http://smallwarsjournal.com/jrnl/art/virtual-indoctrination-and-the-digihad

cité 500 citoyens britanniques affiliés à l'EI en Syrie et en Irak). Des combattants français et allemands ont également été observés en grand nombre sur les médias sociaux, suggérant peut-être plus de 550 combattants venus d'Allemagne et plus de 1000 de France ([51] Stern Jessica et al., 2015).

Un combattant étranger djihadiste typique est un homme âgé de 18 à 29 ans, selon le groupe Soufan, bien qu'il existe de nombreuses exceptions (des plus jeunes mais aussi des plus âgés). Au-delà de l'âge et du sexe, il n'y a pas de profil fiable de qui est le plus susceptible de devenir un combattant étranger. Après quatre décennies de recherche sur la radicalisation, aucune voie socio-économique ou religieuse commune vers la violence n'a été trouvée, et le terme lui-même est caractérisé par une contestation considérable.

La radicalisation n'a pas été limitée aux hommes. L'EI a présenté des femmes parmi leurs partisans les plus visibles en ligne. Aqsa Mahmood était l'une des nombreuses femmes travaillant pour recruter des étrangers afin de rejoindre l'EI. Elle a choisi de quitter une vie adolescente typique et apparemment heureuse à Glasgow, en Écosse. Elle a documenté sa transformation et son attirance pour le radicalisme sur Tumblr. Etant en Syrie, elle a continué à utiliser Twitter et Tumblr pour encourager les autres à suivre son exemple. La même propagande et les récits extrémistes attirant des combattants étrangers ont également été adaptés au public féminin, soulignant la cause «musulmane», un nouvel état «utopique» et la volonté des djihadistes à devenir des martyres accomplissant leur devoir envers Dieu. Certaines femmes sont attirées par une vision romantique de devenir l'épouse d'un djihadiste combattant pour la cause ultime (le califat), et beaucoup de filles étrangères sont mariées à des combattants étrangers (Stern Jessica et al., 2015).

La stratégie médiatique d'EI a été à la fois innovante et opportuniste. EI a apparemment continué l'exemple des groupes terroristes ultraviolents antérieurs qui ont fini par aliéner des partisans. L'EI a conçu une nouvelle campagne médiatique mêlant récits de violence brutale et idéalisme utopique. En outre, la stratégie de recrutement de l'EI

[51] Jessica Stern et J. M. Berger, (2015). " ISIS and the Foreign-Fighter Phenomenon. Why do people travel abroad to take part in somebody else's violent conflict? The Atlantic 8 Mar 2015. Disponible à : https://www.theatlantic.com/international/archive/2015/03/isis-and-the-foreign-fighter-problem/387166/

diffère de l'approche d'Al Qaïda consistant à attirer les combattants d'abord et à les radicaliser plus tard. EI cherche des recrues qui sont plus loin sur la voie de la radicalisation idéologique ou plus enclins par la disposition personnelle à la violence. Lorsque ces combattants pré radicalisés et leurs familles arrivent en Irak ou en Syrie, ils sont exposés à un environnement rempli de violence et de mort.

6.14 La Propagande

L'une des principales utilisations de la communication en ligne par les terroristes est la dissémination de la propagande ([52]Minei et Matusitz 2012, Weimann Gabriel, 2012). Cela prend généralement la forme de communications multimédias fournissant des explications idéologiques, politiques ou religieuses, des justifications ou la promotion d'activités terroristes. Ces communications peuvent inclure des messages en ligne, des vidéos en streaming, des messages sur les réseaux sociaux et même des jeux vidéo développés par des organisations terroristes. Internet a considérablement élargi les possibilités pour les terroristes d'obtenir de la publicité. Jusqu'à l'avènement d'Internet, les espoirs des terroristes de gagner de la publicité pour leurs causes et leurs activités dépendaient de l'attention de la télévision, de la radio ou des réseaux de médias imprimés. Ces médias traditionnels ont des «seuils de sélection» - des processus de sélection éditoriale en plusieurs étapes - que les terroristes ne peuvent souvent pas atteindre. Bien sûr, ces seuils n'existent pas sur les propres sites web des terroristes. De nombreux terroristes ont maintenant un contrôle direct sur le contenu de leur message, ce qui leur donne l'occasion de façonner leur perception par différents publics cibles et leur permet de manipuler leur propre image en plus de celle de leurs ennemis ([53]Zanini Michele et Edwards Sean, 2001, p. 42).

Selon un rapport publié en 2012 par le Bureau contre la drogue et le crime des Nations Unies (ONUDC), «la menace fondamentale que représente la propagande terroriste est

[52] Minei, Elizabeth et Jonathan Matusitz. (2011). "Les messages cyberterroristes et leurs effets sur les cibles: une analyse qualitative." Journal of Human Behaviour in the Social Environment 21 (8): p. 995-1019.
- 2012. "Le cyberespace comme nouvelle arène pour la propagande terroriste: un examen mis à jour." Poiesis & Praxis 9 (1-2): p. 163-76.

[53] Zanini Michele et Sean J. A. Edwards. (2001). «Le réseautage de la terreur à l'ère de l'information», dans Réseaux et réseaux: l'avenir de la terreur, de la criminalité et de la militance, sous la direction de John Arquilla et David Ronfeldt, 29- 60. Santa Monica, CA: RAND Corporation.

liée à la manière dont elle est utilisée et à l'intention avec laquelle elle est diffusée. La propagande terroriste distribuée via Internet couvre une gamme d'objectifs et de publics. Il peut être adapté, entre autres, à des publics ciblés allant des partisans potentiels ou réels aux adversaires d'une organisation ou d'une conviction extrémiste partagée, aux victimes directes ou indirectes d'actes de terrorisme ou à la communauté internationale ou à un sous-ensemble » (UNODC 2012, p. 4).

La plupart des propagandistes terroristes en ligne ne célèbrent pas leurs activités violentes. Au lieu de cela, quels que soient les agendas, les motivations et l'emplacement des terroristes, les messages terroristes mettent l'accent sur deux questions: les restrictions imposées à la liberté d'expression et le sort des camarades prisonniers politiques ([54]Weimann Gabriel, 2005c). Ces questions résonnent puissamment avec leurs propres partisans et sont également conçues pour susciter la sympathie du public occidental, qui chérit sa liberté d'expression, et désapprouver les mesures visant à faire taire l'opposition politique. Les publics ennemis, eux aussi, peuvent être la cible de ces plaintes dans la mesure où les terroristes, en insistant sur le caractère antidémocratique des mesures prises à leur encontre, tentent de créer un sentiment de malaise et de honte parmi leurs adversaires. La protestation des terroristes contre le musellement est particulièrement adaptée à Internet, qui est pour de nombreux utilisateurs le symbole d'une communication libre et non censurée.

6.15 Indoctrination en Ligne

Les terroristes modernes ont fait d'Internet un instrument de radicalisation et d'endoctrinement. Un bon nombre des attaques terroristes récentes en Europe, en Afrique du Nord et au Moyen-Orient ont été perpétrées par des personnes qui avaient été endoctrinées sur Internet. Le recrutement, la radicalisation et l'incitation au terrorisme doivent être considérés comme des points tout au long d'un continuum ([55]UNDOC 2012, p. 6). La radicalisation se réfère principalement au processus d'endoctrinement qui accompagne souvent la transformation des recrues en individus

[54] --.2005c."Terrorist Dot Com: Using the Internet for Terrorist Recruitment and Mobilization." In The Making of a Terrorist: Recruitment, Training, and Root Causes, edited by James J. F. Forest, 53-65. Westport, a: Praeger.

[55] United Nations Office on Drugs and Crime (UNODC). (2012). The Use of the Internet for Terrorist Purposes. New York: United Nations.

déterminés à agir avec violence sur la base d'idéologies extrémistes. Les groupes terroristes peuvent utiliser une variété de plateformes en ligne pour endoctriner des recrues potentielles, allant des courriels personnels et des discussions en ligne aux vidéos séduisantes et aux médias sociaux.

En plus de l'endoctrinement, il y a aussi un processus connu sous le nom «d'auto-radicalisation en ligne». C'est un nouveau type de terroriste : l'extrémiste qui cultive ses opinions en ligne. L'attentat à la bombe du marathon de Boston, le 15 avril 2013, a impliqué deux frères, Dzhokhar et Tamerlan Tsarnaev, qui ont utilisé deux bombes à pression pour tuer trois personnes et blesser environ 264 autres. Selon les interrogateurs du Federal Bureau of Investigation (FBI), les frères Tsarnaev ont été motivés par des croyances extrémistes islamiques exprimées par des messages en ligne sur l'islam radical (Weimann Gabriel, 2014b). Il paraît que les dernières années, les frères s'étaient intéressés à l'extrémisme islamique. Une vidéo sur leur chaîne YouTube, par exemple, mettait en vedette le religieux radical Feiz Mohammad, qui vit en Australie. Tamerlan Tsarnaev avait téléchargé une quantité importante de matériel djihadiste sur Internet, y compris un livre sur les "mécréants" avec une préface du religieux radical Anwar al-Awlaki. En outre, il avait téléchargé le premier volume du magazine en ligne *Inspire*, un produit d'Al-Qaïda, qui proposait des instructions détaillées pour la construction de bombes avec des autocuiseurs, des éclats d'obus et de la poudre explosive à partir de feux d'artifice. Dzhokhar semble avoir été influencé par son frère aîné Tamerlan, mais lui aussi, apparemment, s'était radicalisé en ligne et il a avoué dans une note que les bombardements étaient censés servir de rétribution pour les guerres menées par les Américains en Irak et en Afghanistan. Les sites Web islamiques radicaux utilisent souvent les opérations militaires américaines dans les pays islamiques pour justifier la violence terroriste ([56]Siddiqui et Kaleem 2013).

6.16 Recrutement et Mobilisation

L'Internet et la technologie de pointe fournissent des outils puissants pour le recrutement et la mobilisation des membres du groupe grâce à des communications

[56] Siddiqui Sabrina et Jaweed Kaleem. (2013). "Les musulmans se concentrent sur l'extrémisme en ligne, la radicalisation après les attentats de Boston." Huffington Post, 4 juin.http://www.huffingtonpost.com/2013/06/04/muslims-online-extremism-radicalization-boston_n_3380159.html.

intégrées. En plus de chercher des convertis en utilisant toute la panoplie de technologies de sites Web (audio, vidéo numérique) pour améliorer la présentation de leur message, les organisations terroristes capturent des informations sur les utilisateurs qui naviguent sur leurs sites Web. Les utilisateurs qui paraissent les plus intéressés par la cause de l'organisation ou paraissent bien adaptés à l'exécution de son travail sont alors contactés. Les recruteurs peuvent également utiliser une technologie Internet plus interactive pour parcourir les forums de discussion en ligne, Facebook, Twitter et d'autres plateformes, à la recherche de personnes réceptives, en particulier des jeunes. La portée de ces points de vente en ligne fournit aux organisations terroristes et aux sympathisants un bassin mondial de recrues potentielles. Les forums virtuels offrent aux recrues la possibilité de se renseigner sur les organisations terroristes et de leur apporter leur soutien, et ils encouragent l'engagement dans des actions directes (Denning Dorothy, 2010, [57]Gerwehr et Daly 2006, Weimann Gabriel, 2007a).

Les efforts antiterroristes mondiaux ont conduit de nombreux groupes terroristes, y compris Al-Qaïda, à appeler leurs fidèles en Occident à mener des attaques individuelles à une échelle plus petite, principalement en leur fournissant une éducation en ligne pour leur apprendre à le faire. "Je recommande fortement à tous les frères et sœurs venant d'Occident d'envisager d'attaquer l'Amérique dans sa propre arrière-cour", écrit Samir Khan, un Américain qui a rejoint la branche Yémen d'Al-Qaïda et est devenu un fervent défenseur du terrorisme « fais-le toi-même » avant qu'il ne soit tué pendant une grève des drones en Amérique en Septembre 2011 (Shane Scott, 2013). Dernièrement, les propagandistes d'Al-Qaïda ont "fait un effort particulier pour recruter des personnes seules qui cherchaient une cause", a déclaré Jerrold Post, un ancien psychiatre de la Central Intelligence Agency (CIA) américaine et actuellement à l'université George Washington et qui est l'auteur de *L'esprit du Terroriste: La Psychologie du Terrorisme de l'IRA à Al-Qaïda* (cité dans Cobb Tyrus, 2013). Dans cet œuvre il y a, entre d'autres, des références sur le major Nidal Hasan, le psychiatre de l'armée qui a été accusé d'avoir tué 13 personnes lors du tir de Fort Hood en 2009. Hasan a été présenté comme un exemple à suivre dans une vidéo en deux parties publiée par le groupe d'al-Qaïda au Pakistan en juin 2011. Cette vidéo, intitulée "Vous

[57] Gerwehr, Scott et Sara Daly. (2006). "Al-Qaïda: sélection et recrutement terroristes". Dans le manuel de la sécurité intérieure de McGraw-Hill, édité par David Kamien, 73-89. New York, McGraw-Hill.

n'êtes que responsable de vous-même", a exhorté les musulmans occidentaux à effectuer des attaques sans attendre les commandes de l'étranger.

La communication terroriste axée sur le recrutement est souvent conçue pour attirer les groupes vulnérables et marginalisés de la société. Souvent, cette propagande de recrutement et de radicalisation capitalise sur les sentiments d'injustice, d'aliénation ou d'humiliation d'un individu ([58]Commission européenne 2008, Weimann Gabriel, 2008b). Comme on l'a déjà noté, les terroristes sont devenus plus sophistiqués avec l'utilisation du «narrowcasting» ou de la propagande ciblant des sous-populations spécifiques selon des facteurs démographiques (tels que l'âge ou le sexe) et des circonstances sociales ou économiques (Weimann Gabriel, 2008b, 2008f, 2009b).

Le cyberespace peut constituer une plate-forme idéale pour le recrutement d'enfants et de jeunes, car ceux derniers représentent une forte proportion d'utilisateurs. La propagande diffusée via Internet dans le but de recruter des mineurs peut prendre la forme de dessins animés, de clips musicaux populaires ou de jeux informatiques. Ces contenus mélangent souvent des dessins animés et des histoires d'enfants avec des messages promouvant et glorifiant des actes terroristes, tels que des attentats suicides. De même, certaines organisations terroristes ont conçu des jeux vidéo en ligne à utiliser comme outils de recrutement et de formation. De tels jeux peuvent promouvoir l'utilisation de violence, récompensant les succès virtuels (Weimann Gabriel, 2008b). Par exemple, Al-Qaïda au Maghreb Islamique (AQMI) change sa stratégie pour cibler les enfants à un âge précoce afin de les attirer vers son idéologie radicale. Pour atteindre ce but, dès mars 2013, le groupe a commencé à utiliser de nouvelles méthodes jugées plus susceptibles d'attirer l'attention des enfants, comme les jeux vidéo qui incluent une stratégie claire pour montrer la capacité du groupe de gagner des guerres contre les forces internationales. Sur son site Internet, AQMI a publié un jeu vidéo appelé "Muslim Mali" dans lequel les joueurs opèrent un avion militaire portant le drapeau noir d'AQMI pour attaquer et détruire des avions français au Sahara, où des combats font rage contre les terroristes du nord du Mali. Le site web dit que le jeu

[58] Commission européenne. (2008). «Processus de radicalisation conduisant à des actes de terrorisme», Groupe d'experts sur la radicalisation violente, Commission européenne, http://www.clingendael.nl/sites/default/files/20080500_cscp_report_vries.pdf.

affiche le message "Félicitations, vous êtes devenus des martyres!" au lieu de "Game Over" quand un joueur perd sa vie.

6.17 Mines de Données

Internet est une vaste source d'informations sur tous les sujets. En fait, il peut être considéré comme une vaste bibliothèque numérique. À lui seul, le World Wide Web offre des milliards de pages d'informations, en grande partie gratuites, et qui dans leur majorité, intéressent les organisations terroristes. Les terroristes peuvent utiliser Internet pour collecter des informations susceptibles d'être utiles à leur cause ou aux opérations futures. Ils peuvent apprendre une grande variété de détails sur les cibles potentielles, telles que les installations de transport, les centrales nucléaires, les bâtiments publics, les aéroports et les ports. Ils peuvent acquérir des images satellites, des cartes et des plans de ces cibles, et ils peuvent même découvrir les mesures antiterroristes prises. Dans son livre Black Ice: *La menace invisible du cyber terrorisme*, Dan Verton[59] (2003, p. 184) soutient que «les cellules d'Al-Qaïda fonctionnent maintenant à l'aide de grandes bases de données contenant des détails de cibles potentielles aux États-Unis. Les logiciels modernes leur permettent d'étudier les faiblesses structurelles des installations et de prédire l'effet d'échec en cascade en attaquant certains systèmes». Selon l'ancien secrétaire de la Défense, Donald Rumsfeld, le 15 janvier 2003, un manuel de formation d'Al-Qaïda retrouvé en Afghanistan communiquait à ses lecteurs que «en utilisant des sources publiques ouvertement et sans recourir à des moyens illégaux, il est possible de rassembler au moins 80% de toutes les informations sur l'ennemi». (cité dans [60]Thomas Timothy, 2003).

Outre les informations fournies par et au sujet des forces armées, la disponibilité des informations sur Internet concernant l'emplacement et le fonctionnement des réacteurs nucléaires et des installations connexes a été particulièrement préoccupante pour les autorités après le 11 septembre. Roy Zimmerman, directeur du Bureau de la Sécurité Nucléaire et de l'Affrontement des Incidents de la Nuclear Regulatory Commission (NRC), a déclaré que les attentats du 11 septembre mettaient en évidence la nécessité

[59] Verton, Dan. (2003). "Black Ice: la menace invisible du cyber terrorisme." New York: McGraw-Hill Osborne Media. p. 184

[60] Thomas, Timothée. (2003) "Al-Qaïda et Internet: le danger de la cyber-planification". Paramètres (ressort): p. 112-23. http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/03spring/thomas.pdf.

de protéger les informations sensibles. Dans les jours qui ont suivi les attaques, le NRC a mis son site Web hors ligne et, lorsqu'il a été restauré plusieurs semaines plus tard, il a été vidé de plus d'un millier de documents sensibles (Ahlers Mike, 2004). Les mesures prises par le NRC n'étaient pas exceptionnelles. Selon un rapport produit par Center for Effective Government, ex OMB Watch, depuis le 11 septembre 2001, des milliers de documents et d'énormes quantités de données ont été retirés des sites gouvernementaux américains[61]. Quand les forces américaines en Afghanistan ont découvert des dessins des barrages américains dans les ordinateurs d'al-Qaïda, le Army Corps of Engineers a cessé d'afficher des dessins de projets d'ingénierie dans le cadre de sollicitations contractuelles.

Récemment, on s'est inquiété de la disponibilité des images satellites de Google Earth sur Internet. Les images, mises à jour tous les 18 mois par Google Earth, sont un patchwork de photographies aériennes et satellitaires, dont la netteté relative varie. Pendant une brève période, des photos de la Maison Blanche et des bâtiments adjacents fournis par le United States Geological Survey à Google Earth apparaissaient avec certains détails obscurs, car le gouvernement avait décidé que montrer des endroits comme les plateformes d'atterrissage des hélicoptères sur les toits, représentait un risque pour la sécurité (Hafner, Katie et Saritha Rai, 2005).

Les terroristes utilisent les services de Google Earth: des images détaillées des bases militaires britanniques ont été trouvées dans les maisons des insurgés irakiens. Les terroristes du Hamas de Gaza ont utilisé Google Earth pour viser leurs roquettes vers des villes israéliennes et les terroristes qui ont attaqué divers endroits dans le sud de Mumbai, en Inde, en novembre 2008, ont utilisé des cartes numériques de Google Earth pour se repérer (Harding Thomas, 2007, Schneier Bruce, 2009). Les enquêtes de la police de Mumbai, y compris l'interrogatoire d'un terroriste capturé, suggèrent que les terroristes étaient hautement qualifiés et utilisaient des technologies telles que les téléphones satellites et les systèmes de positionnement global (GPS) associés aux images satellites de Google Earth. Dans la tentative planifiée de terroristes de faire

[61] Le Centre for Effective Government a été fondé sous le nom d'OMB Watch en 1983, ayant pour objectif principal de rendre le travail des agences exécutives plus transparent et ouvert aux contributions des citoyens. Le rapport est cité dans Declan McCullagh (2003).

exploser des réservoirs à l'aéroport international John F. Kennedy de New York en 2007, les dossiers judiciaires indiquent que les traceurs ont utilisé Google Earth pour obtenir des photographies aériennes détaillées de leur cible (Buckley, Cara et William K. Rashbaum, 2007). Le programme est considéré comme supérieur aux cartes car il est plus à jour et donne des emplacements précis pour les cibles potentielles.

Enfin, des incidents tels que les révélations «Wikileaks» de 2011, qui ont fui plus de 250000 câbles diplomatiques, fournissent des évaluations gouvernementales sur l'état des organisations terroristes, leurs plans et intentions et révèlent ainsi l'étendue de leurs connaissances. En août 2013, une fuite concernant un complot d'Al-Qaïda visant à attaquer les ambassades américaines au Moyen-Orient a apparemment miné les renseignements américains en incitant les terroristes à changer leurs méthodes de communication. Citant des responsables et des experts américains, le New York Times a rapporté le 29 septembre 2013 que les détails du complot d'Al-Qaïda en août avaient "causé plus de dommages immédiats aux efforts antiterroristes américains" que les documents divulgués par Edward Snowden, ancien agent de l'Agence Nationale de Sécurité. ([62]Schmitt et Schmidt, 2013).

6. 18 Formation Virtuelle

Internet est devenu un outil précieux pour les organisations terroristes, non seulement pour l'endoctrinement, la propagande et le recrutement, mais aussi comme lieu de camp d'entraînement virtuel pour l'application pratique du terrorisme. Des milliers de nouvelles pages de manuels terroristes, d'instructions et de rhétorique sont publiées chaque mois sur Internet. Certains experts ont qualifié l'Internet d '«université terroriste», où les terroristes peuvent apprendre de nouvelles techniques et acquérir des compétences pour les rendre plus efficaces dans leurs méthodes d'attaque (Groupe de travail de l'ONU sur la lutte contre le terrorisme 2011, p. 20). Les attaques continues contre les camps d'Al-Qaïda en Afghanistan et ailleurs ont forcé le groupe terroriste à déplacer sa base d'opérations et ses camps d'entraînement dans le cyberespace. "Il n'est pas nécessaire ... de vous joindre à un camp d'entraînement militaire, ou de voyager dans

[62] Schmitt, Eric et Michael S. Schmidt. (2013). "La fuite de complot de Qaeda a troublé l'intelligence des Etats-Unis." New York Times, le 29 septembre. http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html.

un autre pays ... vous pouvez apprendre seul, ou avec d'autres frères, suivant le programme de préparation", a annoncé le chef d'Al-Qaïda Abu Hajir al-Muqrin en 2004.

Alors que les attaques contre Al-Qaïda et d'autres groupes terroristes s'intensifient, leur dépendance à Internet pour lancer des campagnes d'instruction et de formation semble s'être considérablement étendue et devenir plus sophistiquée. De plus, les «cours» en ligne sont devenus plus développés et technologiquement avancés.

Des magazines en ligne (tels qu'Al-Qaïda Inspire) et de nombreux sites web terroristes fournissent également des formations et des idées d'attaques terroristes. Le développement et la disponibilité généralisée d'Internet ont rendu possible la création de «camps d'entraînement virtuels» facilement accessibles ([63]Amble John Curtis, 2012 , Weimann Gabriel, 2009a). Les documents en ligne facilement disponibles comprennent le "Manuel des Poisons Mujahideen", un manuel instructif qui contient diverses "recettes" pour les poisons faits maison et les gaz toxiques. Des informations similaires sur la prise d'otages, la fabrication de bombes et la tactique de guérilla sont également disponibles dans une grande variété d'autres sources telles que "Anarchist Cookbook" et "Sabotage Handbook". L'Encyclopédie du Jihad de 600 pages est aussi largement disponible en ligne et comprend des chapitres tels que «comment tuer», «engins explosifs», «fabrication de détonateurs» et «assassinat avec des mines».

La facilité d'accès et l'anonymat qu'offre le cyberespace ont éliminé la nécessité de s'entraîner dans des camps d'entraînement sur les tactiques spécifiques utilisées par les terroristes dans de nombreuses zones de conflit. La première instruction en ligne d'Al-Qaïda a pris la forme d'un magazine coloré en ligne appelé Al Battar Training Camp. Al Battar tire son nom de «l'épée des prophètes», une arme qui appartenait autrefois au prophète Mahomet. Au début de 2004, Al-Qaïda a publié en ligne le premier numéro d'Al Battar. L'introduction indique:

« En raison du fait que beaucoup de jeunes de l'Islam ne savent pas encore porter les armes, sans parler de les utiliser, et parce que les agents de la Croix entravent les Musulmans et les empêchent de planifier [le djihad] pour la gloire d’Allah - vos frères,

[63] Amble, John Curtis. (2012). "Combattre le terrorisme dans le nouvel environnement médiatique." Etudes sur les conflits et le terrorisme 35 (5): p. 339-53.

les moudjahidin de la péninsule arabique ont décidé de publier ce livret pour aider le frère moudjahid au lieu de son isolement, à faire les exercices et agir selon les connaissances militaires qui y sont incluses ... L'idée de base est de propager la culture militaire parmi la jeunesse dans le but de combler le vide que les ennemis de la religion ont cherché à développer depuis longtemps ».

Plus tard, la formation en ligne a été favorisée: « O frère Mujahid, afin de rejoindre les grands camps d'entraînement, vous n'avez pas à voyager vers d'autres pays. Seul, à votre domicile ou avec un groupe de vos frères, vous pouvez aussi commencer à exécuter le programme de formation ».

En novembre 2008, le Groupe de renseignement sur les Entités terroristes internationales ([64]SITE) a signalé que le bataillon des médias jihadiste al-Nusra groupe, avait compilé en un seul fichier une collection de manuels d'explosifs totalisant plus de mille pages et avait posté le fichier sur les forums jihadistes. Cette collection, intitulée «L'Encyclopédie des armes et des explosifs, première partie», comprend des manuels fréquemment distribués sur des forums jihadistes, tels que ceux rédigés par l'expert en explosifs Abdullah Dhu al-Bajadin et distribués par le Centre islamique des médias. Ces manuels fournissent des instructions pour une gamme de composés et d'équipements dans ce domaine, y compris les téléphones portables pour la détonation à distance, les explosifs chimiques, les détonateurs et le placement de ces matériaux pour atteindre une cible spécifique (SITE Monitoring Service 2008).

L'utilisation de nouvelles technologies pour lancer des attaques terroristes est un sujet fréquemment abordé dans ces forums et forums de discussion. Ainsi, des vidéos contenant des instructions pour préparer des explosifs, optimisées pour être visionnées sur des téléphones mobiles, ont été postées sur le forum jihadiste al-Fallujah, le 27 octobre 2008. Les vidéos comprennent la série d'explosifs «Cours pour la destruction de la Croix» qui ont attiré beaucoup d'attention par les jihadistes quand il a été publié sur al-Ekhlaas, un forum affilié à al-Qaïda. Le format de téléphone mobile par laquelle des groupes affiliés à Al-Qaïda, tels que l'État islamique d'Iraq, AQMI, et la Fondation As-

[64] SITE Monitoring Service. 2005. "Salafi Group for Call and Combat Issues Fatwa Calling for Jihad Against Foreigners in Algeria:' March 11. http://ent.siteintelgroup.com/Jihadist-News/salafi-group-for-call-and-com-bat-issues-fatwa-calling-for-jihad-against-foreingners-in-algeria.html.

Sahab (le nuage) pour la publication des médias islamiques est standardisé pour la distribution de vidéos. Ceux derniers comprennent environ 19 heures de séquences. Les quinze de ces leçons se concentrent sur des matériaux particuliers, tels que le TNT, l'acide picrique, l'acide de sodium et le nitrate d'ammonium. Les 10 autres vidéos comportent des séminaires sur des substances sensibles et semi-sensibles et des détonateurs, montrant un individu dirigeant le cours à l'aide d'un tableau blanc, d'illustrations et d'objets divers. Les forums jihadistes organisent des discussions sur l'utilisation des plates-formes modernes en ligne, telles que Twitter, Facebook, YouTube et autres.

Enfin, le manuel de formation en ligne le plus populaire est le magazine *Inspire* ultramoderne. *Inspire* est un magazine en ligne en anglais publié par Al-Qaïda dans la péninsule arabique (AQAP). De nombreux extrémistes islamistes nationaux et internationaux ont été influencés par le magazine et, dans certains cas, ont utilisé ses instructions de fabrication de bombes pour mener des attaques. Le magazine est un outil de marque important pour toutes les filiales, franchises et sociétés affiliées d'Al-Qaïda ([65]Merriam Lisa, 2011). Le magazine promeut le «djihad open source», une tactique nécessaire puisque la direction d'Al-Qaïda avait disparu au cours des 10 années qui ont suivi le 11 septembre. Ses dirigeants morts ou en prison, al-Qaïda a dû envisager de nouvelles façons d'attaquer ses ennemis. Cela a provoqué un changement par rapport aux attaques terroristes traditionnelles d'Al-Qaïda et aux attaques simples par des individus utilisant des armes communes. Le numéro de l'été 2010 recommandait de fabriquer une bombe à pression en utilisant des matériaux de tous les jours («Comment faire une bombe dans la cuisine de votre mère»), une méthode utilisée par les bombardiers du Marathon de Boston en 2013. Le onzième numéro d'Inspire, publié en ligne en juin 2013, a consacré la quasi-totalité de ses quarante pages à la glorification de ce qu'il appelle le «BBB»: les «Bombardements Bénits de Boston». Un article, «Inspiré par *Inspire*», est illustré par un iPad enflammé avec une copie du magazine sur son écran. La principale conclusion tirée du numéro de juin 2013 est que les éditeurs sont très heureux que des copies de leur magazine aient été trouvées chez les frères Tsarnaev.

---

[65] Merriam, Lisa. (2011). "La marque Al-Qaïda est morte la semaine dernière." Forbes, 6 octobre. http://www.forbes.com/sites/realspin/2011/10/06/the-al-qaeda-brand-died-last-week/.

6.19 Cyber Planning et Coordination

Les terroristes utilisent Internet non seulement pour apprendre à fabriquer des bombes, mais ils l'utilisent également pour planifier et coordonner des attaques spécifiques. Les membres d'Al-Qaïda comptaient beaucoup sur Internet pour la planification et la coordination des attentats du 11 septembre. De nombreux messages qui avaient été postés dans une zone protégée par mot de passe d'un site Web ont été trouvés par des fonctionnaires fédéraux sur l'ordinateur d'un terroriste d'Al-Qaïda, Abou Zubaydah, qui a orchestré les attentats du 11 septembre. Pour préserver leur anonymat, les terroristes d'Al-Qaïda ont utilisé Internet dans des lieux publics et envoyé des messages par courrier électronique public. Certains des pirates de l'air du 11 septembre ont communiqué entre eux à l'aide de comptes de messagerie Web gratuits ([66]Weimann Gabriel, 2006d). Beaucoup de méthodes plus sophistiquées existent pour assurer l'anonymat en ligne, y compris l'utilisation du nombre croissant de services d'anonymisation gratuits tels que le réseau Invisible Internet Project (I2P) et le projet Tor, qui utilisent une variété de technologies de cryptage pour masquer les adresses IP (Internet Protocol). Ces services d'anonymisation utilisent un serveur proxy qui sert d'intermédiaire et de bouclier de confidentialité entre le client et le reste de l'Internet. En effet, le proxy agit de la part de l'utilisateur d'origine pour protéger toute information personnelle afin que celle-ci ne soit pas partagée avec des points de destination sur Internet au-delà du proxy. De cette manière, les usagers peuvent «spoof» ou modifier leur adresse IP. Ces services de proxy sont augmentés et plus sophistiqués ces dernières années. Ils utilisent souvent une approche de réseau « peer-to-peer » afin d'empêcher que l'identité de l'utilisateur reste dans un site central qui pourrait la divulguer.

Les militants du Hamas au Moyen-Orient, par exemple, utilisent les salles de conversation pour planifier des opérations et les agents échangent des courriels pour coordonner les actions à Gaza, en Cisjordanie, au Liban et en Israël. Les instructions sous forme de cartes, de photographies, de directions et de détails techniques sur l'utilisation des explosifs sont souvent déguisées par le moyen de la stéganographie, qui

[66] --. 2006d. “Virtual Training Camps: Terrorist Use of the Internet? In Teaching Terror: Strategic and Tactical Learning in the Terrorist World, edited by James Forest, 110-32. Boulder, CO: Rowman & Littlefield.

consiste à cacher des messages dans des fichiers graphiques. Cependant, parfois les instructions sont livrées cachées dans des codes les plus simples. Le message final de Mohammed Atta aux 18 autres terroristes qui ont perpétré les attentats du 11 septembre avait été le suivant: "Le semestre commence dans trois semaines. Nous avons obtenu 19 confirmations pour des études à la faculté de droit, à la faculté d'urbanisme, à la faculté des beaux-arts et à la faculté d'ingénierie » (cité dans [67]Fouda et Fielding 2003, p. 140). La référence aux différentes facultés était apparemment le code des bâtiments visés à être attaqués.

Les terroristes compétents ont adapté les technologies de communication nouvelles et avancées à leur réseau, notamment deux technologies émergentes: les technologies informatiques mobiles et le «cloud computing». La plupart des téléphones mobiles offrent maintenant un accès facile à Internet et une large disponibilité du module de non-identification de l'abonné. Dans de nombreux pays, les cartes (SIM) permettent aux utilisateurs de passer des appels téléphoniques, d'envoyer des messages (texto) et de surfer sur Internet sans devoir fournir aucune forme d'identification. De plus, la grande disponibilité des ressources informatiques en nuage, qui stockent des informations sur un réseau en ligne accessible et partagé, permet aux terroristes d'héberger et de stocker leur matériel de propagande, leurs manuels et tout leur contenu numérique en ligne sans crainte d'identification ou de représailles. Lors de l'attaque terroriste de 2008 à Mumbai, les attaquants ont utilisé les technologies de communication les plus avancées. Celles-ci comprenaient des appareils GPS portatifs pour planifier et perpétrer l'attaque ainsi que des images satellite Google Earth. Les terroristes avaient reçu des mises à jour en direct de leurs collaborateurs sur leurs téléphones mobiles concernant l'emplacement des otages, en particulier des étrangers ([68]Groupe de travail de l'ONU sur la lutte contre le terrorisme 2011, p. 32).

[67] Fouda, Yosri et Nick Fielding. (2003). "Les cerveaux de la terreur: la vérité derrière l'attaque terroriste la plus dévastatrice que le monde ait jamais vue." New York: Arcade.

[68] Groupe de travail de l'ONU sur la lutte contre le terrorisme. (2011). Contrer l'utilisation d'Internet à des fins terroristes: aspects juridiques et techniques. New York: Nations Unies.

6.20 Relever des Fonds

Internet est probablement la méthode la plus simple, la plus facile à utiliser et la moins coûteuse pour solliciter des dons et des contributions. Les terroristes utilisent une variété de techniques pour collecter des fonds en ligne pour leurs activités. Suite à une tendance commerciale populaire, beaucoup se sont tournés vers le commerce électronique, vendant des CD, des DVD, des T-shirts et des livres comme moyen de collecte de fonds. Une approche encore plus simple consiste à «accepter des dons». De nombreuses organisations terroristes ont ajouté des liens vers leurs sites qui conseillent les visiteurs sur la façon de faire un don électronique par virement bancaire. Grâce à Internet, un groupe terroriste ou ses partisans peuvent demander des dons pour soutenir directement leurs actions ou peuvent, comme c'est souvent le cas, déguiser ses sollicitations en un soutien à la charité. De nombreuses organisations terroristes créent également des «organisations caritatives» à travers lesquelles elles sollicitent des fonds, promettant d'utiliser l'argent pour nourrir et vêtir les pauvres, même si leur véritable intention est de financer des actes de violence (Vaccani Matteo, 2010). Plusieurs organisations terroristes ont utilisé des applications de réseautage social comme la nouvelle méthode de collecte de fonds pour leurs activités. Souvent, les dons sont présentés comme un devoir religieux et un substitut pour rejoindre le jihad en tant que véritable guerrier.

Presque tous les groupes ont utilisé Internet pour solliciter des dons. Les groupes terroristes islamistes, notamment le Hamas, Lashkar-e-Taiba et le Hezbollah, ont aussi utilisé largement Internet pour mobiliser et transférer les fonds nécessaires à leurs activités (Jacobson Michael, 2010b). Le Hezbollah avait l'habitude de lancer des appels directs pour des dons pour la "subsistance de l'Intifada" sur le site web de son satellite de langue anglaise Al-Manar. Le site Web donnait des détails sur le compte bancaire auquel les donateurs pouvaient envoyer de l'argent. La plupart des sites liés au Hezbollah, au Jihad islamique palestinien et au Hamas sollicitent ouvertement des dons pour soutenir les familles des kamikazes. Le site Web du *Global Jihad Fund* demandait que des dons soient envoyés sur des comptes bancaires au Pakistan "pour faciliter la croissance de divers mouvements de jihad dans le monde entier, en leur fournissant des fonds suffisants pour acheter des armes et former leurs individus". En plus de

fournir de l'aide humanitaire, ces organisations poursuivent un programme secret de soutien financier et matériel aux groupes militants. Des chefs terroristes comme Oussama ben Laden, Ayman al-Zawahiri et d'autres, ont lancé un certain nombre d'appels pour collecter de l'argent à travers des discours en ligne, des déclarations et des vidéos postées. Les dirigeants jihadistes affirment souvent que l'apport d'argent est similaire à l'engagement physique au jihad. Le site Internet anglophone du groupe Harakat ul-Mujahideen, basé au Pakistan, a déclaré: "Allah vous donne l'opportunité de participer à la lutte pour les droits des musulmans, le jihad. Même si vous ne pouvez pas participer physiquement au jihad, vous pouvez nous aider par le biais d'une aide financière. "

Les groupes terroristes utilisent aussi l'activité criminelle via Internet pour collecter des fonds. Selon un rapport antiterroriste des Nations Unies publié en 2011, «les organisations terroristes utilisent les produits de la cybercriminalité traditionnelle, comme la fraude par carte de crédit en ligne, le vol d'identité et la fraude en matière de télécommunications pour financer leurs opérations» (Force antiterroriste des Nations Unies 2011, p. 34). Les terroristes utilisent également les escroqueries pour séduire des personnes innocentes en fournissant leurs détails de carte de crédit. Il existe de nombreux exemples de cette tendance croissante. La cellule qui a exécuté l'attentat à la bombe de Madrid en 2004 et a tué près de deux cents personnes, a partiellement financé l'attaque en vendant du haschich. Les terroristes qui ont perpétré les attentats du 7 juillet 2005 contre le réseau de transport londonien ont également été autofinancés, en partie à cause de la fraude par carte de crédit. La Jemaah Islamiyah, affiliée à al-Qaïda, a financé les attentats à la bombe de Bali en 2002, en partie par le biais de vols dans des bijouteries. Les principaux leaders terroristes ont spécifiquement encouragé leurs partisans à poursuivre cette voie. Par exemple, l'imam Samudra, un ancien membre de la Jemaah Islamiyah condamné pour son rôle dans les attentats de Bali en 2002, a écrit un livre dont un chapitre intitulé "Hacking, Why Not?" Dans ce chapitre Samudra a exhorté les autres jihadistes à utiliser la fraude par carte de crédit, le blanchiment d'argent et il a même conduit ses lecteurs vers des sites Web spécifiques

qui aideraient les individus à démarrer et à discuter dans des salles où ils pourraient trouver des «mentors» de piratage ([69]Jacobson Michael, 2010a).

Le terrorisme est entré dans le cyberespace dans les années 1990 et y est resté depuis. Tous les groupes terroristes sont aujourd'hui sur Internet, utilisant librement les plateformes de communication en ligne les plus avancées. Bien que les terroristes n'aient jamais développé ou inventé de nouvelles technologies en ligne, ils ont très rapidement appris et appliqué les nouvelles formes de ces canaux en ligne. Par conséquent, leur présence en ligne a considérablement changé au fil des ans. Comme le révèle la partie suivante, l'impact combiné des changements technologiques, de la sophistication croissante des terroristes cyber compétents et du lancement de mesures antiterroristes en ligne, constitue un changement radical dans la cyber-présence terroriste.

6.21 Diffusion

Une tendance émergente du terrorisme en ligne est la «diffusion ciblée»: la diffusion de l'information (généralement par la radio, la télévision ou Internet) à un public restreint et pas au grand public. Elle est aussi appelé «marketing de niche» ou «marketing ciblé» et elle vise à l'envoi des messages médiatiques à des segments spécifiques du public. Ces segments sont définis par des caractéristiques telles que les valeurs, les préférences, les attributs démographiques ou l'emplacement. Le concept est basé sur l'idée postmoderne selon laquelle les audiences de masse n'existent pas. Les terroristes ont appris ce nouveau concept et l'appliquent dans leurs cyber-campagnes. Au lieu d'un «site unique pour tous», les terroristes compétents ciblent des sous-populations spécifiques, notamment des enfants, des femmes, des «loups solitaires», des communautés d'outre-mer et des diasporas.

Les ciblages tels que les enfants et les femmes ne sont que deux exemples de l'utilisation croissante de la diffusion ciblée en ligne par les terroristes. Ils utilisent cette tactique pour attirer, séduire et recruter des sous-populations ciblées, y compris des membres de la soi-disant communauté de la diaspora ou des supporteurs potentiels qui

[69] --. 2010a. Learning Counter-Narrative Lessons from Cases of Terrorist Dropouts. The Hague: National Coordinator for Counterterrorism. https:// www.washingtoninstitute.org/uploads/Documents/opeds/4b7aaf56ca52e.pdf.

vivent à l'étranger, dans les sociétés occidentales. Le succès de l'État Islamique et d'autres groupes jihadistes à recruter des centaines d'Européens et d'Américains du Nord pour se battre en Irak et en Syrie est une preuve suffisante du succès de cette tactique de diffusion ciblée.

La métaphore du terroriste « loup solitaire » repose sur l'image des loups solitaires dans la nature. Mais comme le démontrera ce chapitre, les loups ne chassent jamais seuls - dans la nature ou dans le terrorisme -. En fait, le loup est l'un des carnivores les plus sociaux. Dans la nature, il chasse en meutes, groupe d'animaux habituellement liés par des liens de sang. Il vit, se nourrit et voyage en packs. Il se peut que l'on ne voie pas toujours tout le groupe, mais ses attaques reposent sur des cercles et des virages bien coordonnés de la victime. Les terroristes « loups solitaires » ont également leur pack: un pack virtuel. Ces terroristes sont recrutés, radicalisés, enseignés, formés et dirigés par d'autres. La vague des attaques de loups solitaires a été propulsée par l'impact des plateformes en ligne, qui offrent aux loups solitaires des opportunités illimitées. En ligne, un terroriste en herbe peut trouver tout, des instructions sur la construction de bombes artisanales aux cartes et diagrammes de cibles potentielles. En outre, les sites Web, les blogs, les pages Facebook et les forums de discussion offrent tous, des lieux faciles pour cultiver l'extrémisme d'une manière qui auparavant n’était possible qu’uniquement grâce à des rassemblements en personne.

En appliquant le modèle de sélection et de recrutement de la RAND Corporation, la première étape est «le Net»: une population cible peut être engagée équitablement en étant exposée à un message en ligne, à une vidéo, à une conférence enregistrée, etc.

La deuxième étape est le «entonnoir». Comme l'indique le terme, les recrues potentielles commencent d’une extrémité du processus et se transforment (après être réformées) en membres dévoués lorsqu'elles émergent à l'autre extrémité.

L’étape suivante est «l'infection». Les individus ciblés qui sont mécontents de leur statut social ou qui en veulent à leur système politique ou religieux sont dirigés vers l'auto-radicalisation.

La dernière étape, c'est l '«activation» qui implique la libération du loup solitaire pour mener à bien l'action terroriste. ([70]Gerwehr et Daly 2006).

6.22 Des Medias Sociaux

En conclusion, l'Internet s'est avéré être un instrument très utile pour les terroristes modernes qui l'utilisent pour un large éventail d'objectifs, depuis l'extraction de données et la collecte de fonds en ligne jusqu'à l'incitation, le recrutement et la propagande. Cependant, dans ce nouveau champ de bataille virtuel, les terroristes ont dû rénover, modifier et actualiser leur présence en ligne. Ceci a été indispensable parce que les agences antiterroristes ont fermé les principaux sites et forums terroristes. De plus, elles perturbent constamment de nombreux sites web et ainsi les utilisateurs ont de plus en plus de mal à publier du matériel sur ces sites. Les nouveaux terroristes se tournent vers de nouvelles plateformes en ligne. Il y a une nette tendance à l'émigration terroriste vers les médias sociaux en ligne, y compris YouTube, Twitter et Facebook. De plus, cette tendance s'étend aux nouvelles plateformes en ligne, telles qu'Instagram, Flickr et autres. Pour les «nouveaux venus», convertis, adeptes ou sympathisants de jihadistes ou d'autres mouvements terroristes, le seuil d'accès à ce contenu illégal (ou du moins illégitime) sur les nouvelles pages grand public est bien inférieur à celui des forums fermés. Reformulant l'expression classique de Von Clausewitz, les nouveaux médias devraient être considérés comme «une continuation croissante de la guerre par d'autres moyens». Le nouveau domaine du cyberespace, avec ses nombreuses plateformes en ligne, présente de nouveaux défis et nécessite de nouvelles stratégies pour assurer la sécurité nationale et mener le combat antiterroriste. La réflexion stratégique doit prévoir un plan pour l'avenir: C'est indisputable que les terroristes sont compétents et capables d'adapter les nouvelles technologies de communication, afin de continuer leurs attaques. Il est donc indispensable que les autorités antiterroristes envisagent de telles approches pour qu'elles puissent posséder des moyens pour anticiper à l'usage de nouvelles plateformes émergentes par les terroristes.

[70] Gerwehr, Scott et Sara Daly. (2006). "Al-Qaïda: sélection et recrutement terroristes". Dans le manuel de la sécurité intérieure de McGraw-Hill, édité par David Kamien, 73-89. New York, McGraw-Hill.

6.23 Trois méthodes de base pour perturber les systèmes informatiques

Il existe plusieurs méthodes efficaces pour perturber les systèmes informatiques. Ce rapport se concentre sur la méthode connue sous le nom de *cyber attaque*, ou Computer Network Attack (CNA), qui utilise un code informatique malveillant pour perturber le traitement informatique ou voler des données. Une brève description de trois méthodes différentes est citée par la suite. Cependant, à mesure que la technologie évolue, les distinctions futures entre ces méthodes peuvent commencer à s'estomper.

Une attaque contre des ordinateurs peut (1) perturber la fiabilité de l'équipement et du matériel, (2) modifier la logique de traitement, ou (3) voler ou corrompre des données ([71]Wilson Clay, 2006). Les méthodes discutées ici sont sélectionnées en fonction (a) de l'actif technologique contre lequel une attaque est dirigée et (b) des effets que chaque méthode peut produire. Les actifs affectés ou les effets produits peuvent parfois être utilisées pour affronter de différentes méthodes d'attaque.

1. Les armes conventionnelles peuvent être utilisées contre un équipement informatique, une installation informatique ou des lignes de transmission pour créer une attaque physique qui perturbe la fiabilité de l'équipement.

2. La puissance de l'énergie électromagnétique, le plus souvent sous la forme d'une impulsion électromagnétique (EMP), peut être utilisée pour créer une attaque électronique (EA) dirigée contre un équipement informatique ou des transmissions de données. En surchauffant les circuits ou en brouillant les communications, EA perturbe la fiabilité de l'équipement et l'intégrité des données.

3. Un code malveillant peut être utilisé pour créer une cyber attaque ou une attaque de réseau informatique (CNA) dirigée contre un code de traitement informatique, une logique d'instruction ou des données. Le code peut générer un flux de paquets réseau malveillants qui peuvent perturber les données ou la logique en exploitant une

[71] Clay Wilson, (2006). All methods of computer attack are within the current capabilities of several nations. See CRS Report RL31787, *Information Operations and Cyberwar: Capabilities and Related Policy Issue*. disponible à: https://fas.org/irp/crs/RL31787.pdf

vulnérabilité dans un logiciel informatique, ou une faiblesse dans les pratiques de sécurité informatique d'une organisation. Ce type de cyber attaque peut perturber la fiabilité de l'équipement, l'intégrité des données et la confidentialité des communications ([72]Wilson C. 2008)

6.24 Guerre Psychologique

Le terrorisme a souvent été conceptualisé comme une forme de guerre psychologique, et les terroristes ont certainement cherché à mener une telle campagne sur Internet. Ils peuvent le faire de plusieurs façons. Par exemple, ils peuvent utiliser Internet pour répandre des menaces destinées à distiller la peur et l'impuissance, et à diffuser des images horribles d'actions récentes, comme le meurtre brutal du journaliste américain enlevé Daniel Pearl par ses ravisseurs pakistanais en 2002. Ceci avait été diffusé plusieurs fois sur plusieurs sites terroristes. D'autres moyens incluent des avertissements effrayants sur les attaques et les menaces ciblant des nations, des villes ou des populations spécifiques. Internet, un média non censuré porteur d'histoires, d'images, de menaces ou de messages, indépendamment de leur validité ou de leur impact potentiel, est particulièrement adapté pour permettre à un petit groupe d'amplifier son message et d'exagérer son importance ainsi que la menace que cela représente. Très souvent, les terroristes emploient cette méthode et ils alimentent les médias «conventionnels» plutôt que exposer directement leurs menaces. Les journalistes tirent telles déclarations et menaces de publications terroristes en ligne et les reproduisent amplifiant ainsi leur impact ([73]Weimann Gabriel, 2008f, p. 65).

Al-Qaïda a toujours affirmé sur ses sites Web que la destruction du World Trade Center le 11 septembre avait infligé des dommages à la fois psychologiques et concrets à l'économie américaine. Les attentats contre les « Twin Towers » sont décrits comme une agression contre la marque déposée de l'économie américaine, et la preuve de leur efficacité est l'affaiblissement du dollar, le déclin du marché boursier américain après le

[72] Clay Wilson, (2008). For more on electromagnetic weapons, see CRS Report RL32544, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments*. disponible à: https://fas.org/sgp/crs/natsec/RL32544.pdf

[73] Weimann Gabriel, (2008f). WWW.Al-Qaïda: La dépendance d'Al-Qaïda sur Internet - Réponses au cyberterrorisme, édité par le Centre d'excellence - Défense contre le terrorisme, Ankara, Turquie, 61-69 Série OTAN de la science pour la paix et la sécurité, Amsterdam : IOS Press.

11 septembre et la perte supposée de la confiance dans l'économie américaine à la fois aux États-Unis et à l'étranger. L'une des publications d'Oussama ben Laden, publiée en ligne, déclarait que « l'Amérique est en retrait par la Grâce du Tout-Puissant et que l'attrition économique se poursuit jusqu'à aujourd'hui. Mais il faut d'autres coups. Les jeunes hommes doivent chercher les nœuds de l'économie américaine et frapper les nœuds de l'ennemi » (cité dans [74]Hoffman 2006a, p. 124).

6.25 Pourquoi ces gens nous attaquent-ils avec cette horrible violence ?

Les réponses habituelles données dans les discours publics reposent sur une analyse psychologique selon laquelle les terroristes sont soit psychologiquement perturbées, soit tout simplement mauvais. Cependant, l'engagement direct et les explorations en tant que psychiatre et politicien, tant à l'intérieur qu'à l'extérieur du contexte thérapeutique, en Irlande du Nord et ailleurs, ont démontré que la plupart des personnes impliquées dans le terrorisme n'ont aucun trouble névrotique ou psychotique antérieur. Certaines personnes développent un trouble de stress post-traumatique (TSPT) et d'autres réactions à la suite de leurs expériences de violence, mais c'est une question différente. Beaucoup d'entre eux ont grandi dans des communautés où, au fil du temps, la tradition de recourir à la force physique pour résoudre des problèmes politiques s'est développée et leur père et grand-père ont été honorés grâce à leur participation à une lutte historique. En conséquence, leur implication dans le terrorisme était une identification avec ces chiffres significatifs. C'était ego-syntonique et non une expression de conflit interne. Ils ont souvent décrit des expériences de traumatismes majeurs où des amis ou des membres de la famille ont été tués ou gravement blessés lors d'attentats à la bombe, de fusillades et d'autres incidents de violence. Ils ont estimé que des membres des institutions officielles - police, armée et système judiciaire- étaient en effet, les instigateurs de la violence. D'autres, qui ne venaient pas de parties de la communauté ayant des antécédents familiaux de violence politique, ont néanmoins connu le même type de traumatisme et ont réagi en rejoignant une organisation terroriste ou paramilitaire. Cela a été consciemment vu à la fois comme un moyen de se joindre à

[74] Hoffman, Bruce. (2006a). "Inside Terrorism, version révisée." New York: Columbia University Press.

d'autres pour protéger leur communauté et en même temps de satisfaire le désir de vengeance pour leur propre blessure ou la mort ou la blessure d'une personne qui leur était proche.

7. Réfléchir et penser autrement

Comme le spécialiste de la sécurité informatique et cryptologue Bruce Schneier, a noté : "si vous pensez que la technologie peut résoudre vos problèmes de sécurité, vous ne comprenez ni les problèmes ni la technologie." Pour renforcer la sécurité du système, il n'existe pas de «sécurité complète» pour tout réseau connecté au même Internet public qui devrait desservir 15 milliards d'appareils d'ici à 2015 (CISCO Technology, 2011).

Tout gouvernement national a certains responsabilités dans cette guerre de dissuasion contre le cyber terrorisme:

Renforcer la coopération entre les différents domaines de compétence internationale. Sans la coopération et les accords internationaux, les preuves utilisées pour suivre et poursuivre les cyber terroristes peuvent être détruites. D'un point de vue juridique international, plusieurs juridictions sont disponibles pour poursuivre les cyber-terroristes: nationalité de la victime ou de l'auteur (tourisme sexuel contre les enfants, victimes du terrorisme), juridiction territoriale basée sur les frontières d'un État (les entreprises locales), la compétence universelle fondée sur l'extrême gravité du crime (la piraterie, l'esclavage, les crimes de guerre), et la compétence de protection fondée sur la menace contre un État (trahison).

Gable (2009) soutient que la compétence universelle est la plus adaptée au cyber terrorisme et constitue le moyen le plus efficace pour dissuader de tels crimes. La compétence universelle peut être fondée sur des traités entre nations ou sur le droit international. De nombreux traités existent pour poursuivre des terroristes, tels que la Convention sur la prévention et la répression des actes de terrorisme revêtant la forme de crimes contre les personnes et d'extorsions connexes d'importance internationale, et la Convention internationale pour la répression des attentats terroristes à l'explosif. Ces traités peuvent être appliqués contre le cyber-terrorisme (Gable, A. Kelly, 2009). De même, le Conseil de sécurité des Nations Unies (ONU) a condamné le terrorisme par le

biais des résolutions 1373, 1566 et 1624 du Conseil de Sécurité. La résolution 51/210 de l'ONU vise spécifiquement le cyber terrorisme.

Financer la recherche sur l'adoption des technologies d'authentification Internet. Les technologies actuelles de suivi des cyber-terroristes sophistiqués manquent de capacités de traçage principalement en raison de la conception du protocole TCP/IPv4 (Transmission Control Protocol/ Internet Protocole version 4). Avec des investissements accrus dans l'adoption universelle d'IPv6, le problème de suivi de tous les paquets peut être résolu. Cependant, même IPv6, qui utilise IPsec (Internet Protocol Security) pour chiffrer tous les paquets de données au niveau OSI (Open Systems Interconnection) Layer 3, ne résout peut-être pas tous les problèmes, d'autant qu'IPv6 avec rétrocompatibilité va à l'encontre de l'objectif de l'authentification. De plus, les terroristes peuvent réussir à acquérir une machine préalablement authentifiée. Un financement accru pourrait être orienté vers la création de protocoles et de processus intégrant l'authentification à tous les niveaux ([75]Lipson Howard, 2002).

Renforcer la coopération entre les forces de l'ordre et les fournisseurs de services Internet locaux. Si les FAI peuvent utiliser des technologies avancées pour enregistrer toutes les demandes de connexion, il est beaucoup plus facile pour les enquêteurs de suivre et de verrouiller les cyber terroristes (Morris Loveday, 2010).

Éduquer et former le public pour le protéger du cyber-terrorisme. Une politique obligeant tous les utilisateurs sans fil à mettre en œuvre un système de contrôle d'accès à leurs réseaux sans fil pourrait empêcher les cybers terroristes d'acquérir facilement des ressources Internet. La politique peut exiger que la configuration par défaut de tous les points d'accès sans fil soit définie sur un protocole sécurisé et interdire tout accès sans une clé unique attribuée à chaque individu ([76]Morris Daniel, 2001). Cependant, cela doit être équilibré par les droits de la vie privée.

Créer une infrastructure juridique qui mènerait à une poursuite rapide et efficace des pirates informatiques et des crimes informatiques en col blanc. L'infrastructure devient

[75] Lipson F. Howard, (2002). Tracking and tracing cyber-attacks. disponible à: http://www.cert.org/archive/pdf/02sr009.pdf

[76] Daniel A. Morris, (2001). “Tracking a Computer Hacker,” May 2001. Disponible à : https://www.justice.gov/sites/default/files/usao/legacy/2006/06/30/usab4903.pdf

un mécanisme de signalisation pour les cyber-terroristes potentiels et augmente ainsi leurs coûts de mener des activités nuisibles.

8. Conclusion

Cet essai visait à une recherche et une étude approfondie du phénomène en question. Dès le début, nous étions conscient de la complexité du sujet et c'est donc naturel que nous ne songions pas à une conclusion claire et nette.

Nous nous contentons, alors, à des réflexions différentes et parfois contradictoires, car nous avons essayé de comprendre ce phénomène de différents points de vue.

D'un côté, en tant que citoyen-victime potentielle du cyber terrorisme, exigeant d'être protégé par les autorités de notre pays, nous avons cherché à trouver les moyens qui pourraient limiter au moins, la menace des cyber terroristes et par conséquence la panique et la peur que celle-ci entraine.

De l'autre côté, pour être objectif, nous devrions se demander comment et pourquoi l'optique des cyber terroristes est tellement différente de la nôtre. Nous tenons, à ce point, ouvrir une parenthèse pour citer un exemple qui fait partie de l'histoire de notre pays, Chypre : Les combattants d'EOKA, l'organisation pour la libération de Chypre des colonisateurs britanniques (1955-1959) sont considérés et honorés comme des héros par tous les Chypriotes. Par contre, dans tous les documents historiques d'origine britannique, ceux mêmes individus sont traités de terroristes.

Où en est donc la vérité ou encore la réalité absolue ?

Tenant compte de tous les faits présentés dans cette étude et les positions de différents experts du domaine, nous pourrions conclure que croire pouvoir éliminer le cyber terrorisme serait une utopie car le fruit de l'évolution constante de la technologie ne signifie que le développement du terrorisme et des organisations terroristes.

Les nouveaux produits de la mondialisation et le développement de la technologie ont donné une nouvelle dimension au terrorisme en changeant complètement sa structure organisationnelle, sa doctrine, sa stratégie, ses méthodes de communication, son financement et son action. La révolution de l'information a conduit à la création et au

renforcement de formes d'organisation en réseau, en plus des formes hiérarchiques, c'est-à-dire des groupes différents mais qui agissent pour la même cible. Dans l'avenir les formes hiérarchiques auront tendance à former des réseaux, parce que leur prolifération et leur camouflage ne peuvent pas être éradiqués. Par conséquent, les modes de financement ont changé. Ayant modifié leur structure, les organisations terroristes ont trouvé de nouvelles façons de se financer.

Pourtant, il y a des moyens pour limiter tout cela. C'est bien vrai que le développement des techniques et des technologies rend le cyberespace illimité, mais connaissant l'évolution du terrorisme et des organisations terroristes, leurs façons et méthodes d'action à travers l'utilisation de produits technologiques dans le cyberespace, nous pourrions créer un cadre législatif qui filtrerait certaines activités qui devraient être interdites.

Le combat antiterroriste devrait être orienté vers l'identification du flux d'informations, des fonds et de leur fin, afin de désactiver le fonctionnement et la coordination des activités cyber terroristes et en même temps atteindre l'objectif primordial : protéger les infrastructures critiques. Le raccourcissement du flux financier vers les organisations terroristes est essentiel dans la lutte contre le terrorisme. Ce qui est important de savoir et de se rappeler, c'est que la diminution des ressources financières des organisations terroristes affectera fortement leur potentiel, en réduisant leur pouvoir et leur capacité de réaliser les attaques prévues. D'autre part, cela causerait de la confusion et de la panique dans l'organisation terroriste, de peur qu'elle ne réalise pas ses projets. C'est évident que les organisations terroristes chercheront d'autres moyens pour acquérir des fonds, ce qui accroîtra le risque, l'insécurité et l'incertitude dans leurs activités opérationnelles, et qui, en termes de tactique, peut contribuer efficacement à :

- Affaiblir la légitimité morale et la hiérarchie au sein de l'organisation terroriste.

- Rationaliser l'organisation terroriste pour révéler son bouclier et atteindre des activités qui normalement n'auraient jamais eu lieu.

À long terme, l'infraction de financement du terrorisme, les sanctions financières ciblées liées au terrorisme et au financement du terrorisme, les sanctions financières ciblées liées à la prolifération; et les organisations à but non lucratif, sont recommandés. Ce que

ces recommandations indiquent, c'est que pour détecter une implication terroriste dans des activités financières par ailleurs légitimes, les institutions financières doivent assurer une application solide du principe «Connaitre son client» et des politiques et procédures de diligence raisonnable envers les clients. Une attente fondamentale existe donc dans la déclaration des transactions suspectes qui pourraient indiquer une activité criminelle soutenant le terrorisme. Alors que les autorités nationales compétentes ont identifié des modèles ou des indicateurs de blanchiment d'argent, il existe encore peu de modèles de financement du terrorisme connus que les institutions financières, en particulier, peuvent utiliser.

Peu importe la structure du groupe terroriste, il est clair que ces groupes recourent à un large éventail de méthodes pour recueillir des fonds pour leurs causes. L'utilisation des crimes organisés et transnationaux est particulièrement troublante. Du trafic d'héroïne en Afghanistan, en Asie du Sud et dans d'autres régions, à l'extorsion de communautés expatriées dans le monde entier, l'utilisation de ces tactiques fournit un financement à de nombreux groupes terroristes. La portée de ces réseaux financiers s'étend à travers le monde, ce qui pose un problème pour de nombreux pays. Il est de la plus haute importance de se concentrer sur le financement des activités terroristes. Si un groupe terroriste n’a plus de moyens financiers à sa disposition, il devient moins puissant et moins susceptible de mener des attaques à grande échelle.

La criminalité transnationale est un phénomène mondial et par conséquent la lutte contre ce phénomène devrait également être mondiale. La collecte d'informations et surtout le partage de celles-ci, est le seul moyen pour résoudre cette situation problématique. Il est également important de cibler le lien entre le crime organisé et le terrorisme afin de supprimer tous les moyens de soutien financier et logistique aux groupes terroristes. Les groupes criminels organisés ont des réseaux bien établis qui peuvent aider les groupes terroristes à obtenir et à déplacer des explosifs et d'autres armes, ainsi que de transférer des fonds. En ciblant ces activités, on pourrait non seulement perturber les activités criminelles, mais également perturber les canaux utilisés pour financer le terrorisme.

Enfin, tous les pays ne sont pas équitablement équipés pour lutter contre le terrorisme ou les activités criminelles transnationales. Par conséquent, cela devrait être une

responsabilité partagée par tous, incluant le partage des meilleures pratiques, l'aide aux pays pour renforcer leur capacité à lutter contre les réseaux criminels, contribuer à ce que ces pays renforcent les lois destinées à cibler les réseaux criminels et terroristes, et partager plus efficacement l'information et le renseignement pour aider à combattre ce problème. Découvrir ces réseaux qui fournissent un soutien monétaire et logistique est une étape clé dans la lutte contre le terrorisme mondial.

L'effort des terroristes à dissimuler les fonds et leur origine afin de poursuivre leurs activités présente une similitude au blanchiment d'argent. En effet, les terroristes et leurs partisans recourent à des outils et des techniques similaires à ceux utilisés par les blanchisseurs dans le crime organisé pour transférer des fonds. Néanmoins, lorsque le financement du terrorisme a lieu, il n'y a souvent aucune infraction criminelle qui précède la tentative de cacher le transfert des fonds. Il y a, bien sûr, une intention criminelle, mais il n'est pas raisonnable de considérer les fonds «comme le produit de cette intention criminelle». Cela soulève de sérieux doutes quant à l'efficacité de l'inclusion d'un système de lutte contre le blanchiment d'argent conçu pour tracer, empêcher ou limiter la capacité des criminels à utiliser leurs gains mal acquis pour contrer le financement du terrorisme.

Pendant notre recherche, nous avons remarqué une exagération concernant les inquiétudes exprimées à propos de la menace du cyber terrorisme. Ceci pourrait être dû à de nombreuses raisons. Tout d'abord, comme l'a observé Denning, «le cyber terrorisme et les cyber attaques sont sexy en ce moment, le cyber terrorisme est original et il capture l'imagination des gens.» Deuxièmement, les médias omettent souvent de faire la distinction entre piratage et cyber terrorisme. Ils aboutissent à un raisonnement à partir de fausses analogies telles que: «Si un garçon de seize ans peut faire cela, alors qu'est-ce qu'un groupe terroriste bien financé pourrait faire?» L'ignorance est un troisième facteur. Le cyber terrorisme fusionne deux sphères - le terrorisme et la technologie - que beaucoup de gens, y compris la plupart des législateurs et des hauts fonctionnaires de l'administration, ne comprennent pas complètement et ont donc tendance à en éprouver de la peur. De plus, il y a certains groupes qui désirent exploiter cette ignorance. De nombreuses entreprises technologiques, toujours sous le choc de l'effondrement de la bulle technologique, ont cherché à attirer des subventions de

recherche fédérales en se refondant comme des innovateurs en sécurité informatique et donc des contributeurs essentiels à la sécurité nationale. Les consultants en application de la loi et en sécurité sont également très motivés pour nous faire croire que la menace contre la sécurité de notre nation est sévère. Une quatrième raison est que certains hommes politiques, que ce soit par conviction réelle ou par désir d'attiser l'inquiétude du public sur le terrorisme afin de faire avancer leurs propres agendas, ont joué le rôle de prophètes de malheur. Le dernier facteur est l'ambiguïté sur la signification même du «cyber terrorisme», qui a embrouillé le public et donné naissance à d'innombrables mythes.

En outre, comme le soutient Denning, la prochaine génération de terroristes grandit dans un monde numérique, où les outils de piratage sont sûrs de devenir plus puissants, plus simples à utiliser et plus faciles d'accès. Le cyber terrorisme peut également devenir plus attrayant à mesure que les mondes réel et virtuel deviennent plus étroitement liés. Par exemple, un groupe terroriste pourrait simultanément faire exploser une bombe dans une gare et lancer une cyber attaque sur l'infrastructure de communication, amplifiant ainsi l'impact de l'événement. À moins que ces systèmes ne soient soigneusement sécurisés, mener une opération en ligne qui nuit physiquement à quelqu'un peut être aussi facile que de pénétrer un site Web aujourd'hui.

A ce point, tournons la monnaie de l’autre côté et passons aux positions de certains analystes qui suggèrent que le terrorisme est le résultat de l'inégalité et de la pauvreté postcoloniale. Bien sûr, il existe un impératif moral de s'attaquer aux inégalités douloureuses de l'éducation, de la santé et du bien-être économique dans le monde, mais ce n'est généralement pas lorsque les sociétés sont les plus pauvres qu'elles sont victimes du terrorisme. Que ce ne soit pas au plus profond des privations, mais au point d'amélioration que les choses deviennent plus vulnérables à l'effondrement. Il est donc suggéré que le lien avec le désavantage socio-économique et la réaction émotionnelle vient du sentiment que le désavantage relatif est vécu comme injuste. Ce n'est pas seulement une réaction aux expériences actuelles, mais peut-être un sens durable et historique de l'injustice qui survit longtemps après que la période réelle d'injustice traumatique est passée, et le contexte a complètement changé. Lorsque les gens croient que leur désavantage relatif est le résultat d'une éducation médiocre ou de

différences sociales ou culturelles, ils peuvent même les accepter comme des causes malheureuses mais justifiables de leur désavantage. Lorsque leurs possibilités d'éducation s'améliorent et qu'ils se sentent aussi capables que l'autre, ils commencent à voir leur désavantage en termes de discrimination historique, culturelle, raciale ou politique. La remédiation consiste à essayer de changer cela par des moyens politiques pacifiques, mais lorsque les options non-violentes sont épuisées, l'utilisation de la force physique apparaît à l'ordre du jour. Cette explication relativement rationnelle de l'émergence de la violence en dernier recours pourrait être considérée comme une «realpolitik» de la gauche.

Ceci était la première indication claire de la montée de l'ISIS et d'autres de ce genre, et le déroulement des événements s'est avéré juste. Par exemple, le refus d'aborder les préoccupations du peuple palestinien a conduit à la naissance de l'Organisation de libération de la Palestine (OLP). L'échec à créer de réels progrès avec l'OLP a conduit à la montée du Hamas (groupes terroristes). L'échec de s'engager avec le Hamas conduit à la montée d'autres manifestations plus extrêmes et régressées. En plus de ces défis, la mondialisation, une conséquence des progrès technologiques dans les communications, les voyages et les armes de masse, a suscité une profonde inquiétude de groupe et une régression de la pensée sociétale envers le fondamentalisme religieux et non religieux et culturellement vers d'anciens thèmes et structures sociétaux qui paraissaient rassurer les gens. La réaction est complexe à cause de l'ambivalence profonde avec l'Occident. D’un côté, ces gens ressentent de l’antipathie envers sa domination et son intrusion et de l’autre côté, ils souhaitent posséder certains des bénéfices de l'éducation, de la santé et de la prospérité économique que représentent les États occidentaux.

Enfin, cette problématique portée à notre réflexion fait et fera encore le sujet de beaucoup des débats sociaux.

9. Les références

Ahmed Al-Rawi, (2016). "La réponse en ligne aux incidents brûlants du Coran", dans L'Islam politique et les médias mondiaux: les frontières de l'identité religieuse, édité par Noha Mellor et Khalil Rinnawi (Londres: Routledge, 2016), 105-21.

Ajello, Nicolas, (2015). "Monter une cheville carrée dans un trou rond: le bitcoin, le blanchiment d'argent et le cinquième élément d'auto-incrimination", Brooklyn Law Review, Vol. 80 No. 2, pp. 435-461.

Akil N. Awan, (2015). "L'Attaque de Charlie Hebdo: Le Double Dilemme de l'Aliénation", The National Interest, 13 janvier 2015. Disponible à : http://nationalinterest.org/feature/the-charlie-hebdo-attack-thedouble-alienation-dilemma-12021

Alex Bilger, (2014). "Les rapports annuels d'ISIS révèlent un commandement militaire axé sur les métriques", Institut pour l'étude de la guerre, 22 mai 2014. Disponible à : http://www.understandingwar.org/backgrounder/ISISAnnual-Reports-Reveal-Military-Organization

Alex P. Schmid et Danny De Graaf, (1982). La violence comme communication: le terrorisme insurrectionnel et les médias d'information occidentaux (Londres: Sage, 1982), p. 14.

Al Arabiya, (2014). "Comment ISIS a conquis les médias sociaux", 24 juin 2014, http://english.alarabiya.net/fr/media/digital/2014/06/24/How-has-ISIS-conquête-social-media-.html

Ali Fisher, (2015). "Comment les réseaux djihadistes maintiennent une présence en ligne persistante", Perspectives on Terrorism 9, no. 3 (2015): p. 4.

Angela Gendron, (2007). "Al-Qaïda: Stratégie de propagande et de médias, Série Tendances de l'ITAC dans le terrorisme", vol 2007-2 (Ottawa: Centre canadien d'études sur le renseignement et la sécurité, 2007).

Arnaudovski Ljupco, (2002). "Interdiscipline et interdépendance du terrorisme et du crime organisé" Annuaire de la Faculté de sécurité, Université "St. Kliment Ohridski", Skopje, Centre pour le personnel éducatif dans le domaine de la sécurité-Skopje, Skopje, 2002, p. 92

Bayern, Shawn, (2013). "De Bitcoins, indépendamment des logiciels riches, et l'essai en ligne LLC zéro membre", Northwestern University Law Review, vol. 108, pages 1485-1500.

Ben Brumfield, (2014). "Officiels: 3 Denver Girls ont joué Hooky de l'école et ont essayé de rejoindre ISIS", CNN, 22 octobre 2014. Disponible à : http://edition.cnn.com/2014/10/22/us/colorado-teens-syriaodyssey/index.html

Berger M. James, et Jonathon Morgan, (2015). "Le recensement Twitter d'ISIS: Définir et décrire la population des partisans d'ISIS sur Twitter", The Brookings Project sur les relations des Etats-Unis avec le monde islamique 3, no. 20, p. 2, (2015), http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf

Bill Roggio, (2012). "Les États-Unis ajoutent Taliban Financier, Haqqani Network Operative à Terror List", The Long War Journal (17 mai 2012), disponible à : http://www.longwarjournal.org/archives/2012/05/the_us_treasury_depa.php

Bob Francis, (2005). "Know Thy Hacker", Infoworld, 28 janvier 2005 disponible à: http://www.infoworld.com/article/05/01/28/05OPsecadvise_1.html

Bonneau Joseph, Miller, A., Clark, J., Narayanan, A., Kroll, J.A. et Felten, E.W. (2015). "SoK: perspectives de recherche et défis pour le bitcoin et les cryptomonnaies", symposium de l'IEEE sur la sécurité et la confidentialité, Fairmont, SAN JOSE, CA, 18-20 mai 2015, pp. 104-121.

Bouchard Martin, (2007). "Sur la résilience des marchés de drogues illicites", Global Crime, Vol. 8 No. 4, pp. 325-344. Box, S. (1983), Pouvoir, Crime et Mystification, Tavistock, Londres.

Brian Krebs, (2007). "Trois ont travaillé sur le Web pour aider les terroristes", The Washington Post, 6 juillet 2007, p. D01.

Byman Daniel, (2005). Connexions mortelles: États qui commanditent le terrorisme, Cambridge University Press, Cambridge, New York, NY.

Chaum David, (1982). Signature aveugle pour les paiements introuvables, Advances in Cryptology-Eurocrupt 82, Plenum Press, New York, NY, pp. 199-203.

Clay Wilson, (2006). All methods of computer attack are within the current capabilities of several nations. See CRS Report RL31787, *Information Operations and Cyberwar: Capabilities and Related Policy Issue*. disponible à:
https://fas.org/irp/crs/RL31787.pdf

Clay Wilson, (2008). For more on electromagnetic weapons, see CRS Report RL32544, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments*. disponible à:
https://fas.org/sgp/crs/natsec/RL32544.pdf

Claire Hardaker, (2010). “Trolling in Asynchronous Computer-mediated Communication: From User Discussions to Academic Definitions” (2010): p. 218–9.

Charlie Winter, (2015). The Virtual “Caliphate”: Understanding Islamic State’s Propaganda Strategy (London: The Quilliam Foundation, 2015).

Christopher Baker-Beall, Charlotte Heath-Kelly, and Lee Jarvis, eds.,(2015). “Counter-Radicalisation: Critical Perspectives” (Abingdon: Routledge: 2015), pp. 1–13.

Cronin Audrey Kurth, (2002-2003). “Behind the curve: globalization and international terrorism”, *International Security*, Vol. 27 No. 3.

Cobb, Tyrus W. (2013). “Two Worrisome Scenarios on the Boston Bombers.” National Security Forum, May 16. disponible à: http://nationalsecurityforum.org/domestic-news/homeland-security/two-worrisome-scenarios-on-the-boston-bombers/.

Dan Verton, (2003). “A Definition of Cyber-terrorism”, *Computerworld*, August 11, 2003, disponible à: http://www.computerworld.com/securitytopics/security/story/0,10801,83843,00.html

David Kaplan, (2003). “Playing Offense: The Inside Story of How U.S. Terrorist Hunters Are Going after Al Qaeda,” *U.S. News & World Report*, June 2, 2003, pp. 19-29.

David Smith, (2012). “Africa’s Islamist Militants ‘Co-ordinate Efforts in Threat to Continent’s Security,’” The Guardian (June 26, 2012), disponible à: http://www.guardian.co.uk/world/2012/jun/26/africa-islamist-militants-coordinating-threat

Deatherage Robert H, (2008). Security Operations: An Introduction to Planning and Conducting Private Security Details for High Risk Areas Perfect. Santa Fe: Turtle Press.

Jan Camenisch, Susan Hohenberger, Anna Lysyanskaya, (2005). “Compact e- cash”, *Advances in Cryptology – EUROCRYPT*, Springer, Berlin Heidelberg, pp. 302-321.

Des Freedman and Daya Thussu, (2012). “Introduction: Dynamics of Media and Terrorism,” in Media & Terrorism: Global Perspectives, edited by Des Freedman and Daya Thussu (Thousand Oaks, California: Sage, 2012), p. 10.

Dion, Derek, (2013). "Je vous échangerai volontiers deux bits mardi pour un octet aujourd'hui: Bitcoin, régulant la fraude dans l'économie de Hacker-cash", Revue de droit, technologie et politique, vol. 1, pages 165-201.

Donath S. Judith, (1999). “Identity and Deception in the Virtual Community,” in Communities in Cyberspace, edited by Peter Kollock and Marc Smith (London: Routledge, 1999), p. 27–58.

Dorothy Denning, (2001). «Activisme, hactivisme et cyberterrorisme: Internet comme outil d'influence sur la politique étrangère», dans John Arquilla et David Ronfeldt, éd.,

Networks and Netwars, (Rand 2001), p. 241. Dorothy Denning, la guerre informatique est-elle la prochaine? Conseil de recherches en sciences sociales, novembre 2001, disponible à : http://www.ssrc.org/sept11/essays/denning.htm

Dorothy Denning, (2004). «Niveaux de cyberterrorisme: Terroristes et Internet», disponible à : http://www.cs.georgetown.edu/~denning/infosec/Denning-Cyberterror-SRI.ppt, présentation, et Zack Phillips, «Homeland Tech Shop Wants pour lancer des idées de cybersécurité », CQ Homeland Security, 14 septembre 2004, disponible à : http://homeland.cq.com/hs/display.do?docid=1330150&sourcetype=31&binderName=news-all

Dorothy Denning, (2011). «Terror's Web: Comment Internet transforme le terrorisme», dans Yvonne Jewkes et Majid Yar, éd., Handbook of Internet Crime (Abingdon: Routledge, 2011), p. 194-213.

Duncan Gardham, (2009). L'otage britannique Edwin Dyer Exécuté par al-Qaïda au Mali, The Telegraph (3 juin 2009), disponible à : http://www.telegraph.co.uk/news/worldnews/africaandindianocean/mali/5437960/British-hostage-Edwin-Dyer-executed-by-al-Qaeda-in-Mali.html

Enders Walter, (2004). "Terrorisme: une introduction" Disponible à : http://assets.cambridge.org/97805218/51008/excerpt/9780521851008_excerpt.pdf

Eric Schmittdec, (2014). "Dans Battle to Defang ISIS, les États-Unis ciblent sa psychologie", The New York Times, 28 décembre 2014, disponible à : http://www.nytimes.com/2014/12/29/us/politics/in-battle-todefang-isis-us-targets-its-psychology-.html?_r=0

Eskandari, S., Barrera, D., Stobert, E. et Clark, J. (2015). "Un premier regard sur la facilité d'utilisation de la gestion des clés bitcoin", Workshop on Usable Security (USEC), pp. 1-12.

Frey H. Christopher, Cullen, Alison C., (1999). "*Probabilistic Techniques in Exposure Assessment.*" A Handbook for Dealing with Variability and Uncertainty in Models and Inputs. Springer Science & Business Media.

Gable, A. Kelly, (2009). Cyber-Apocalypse now: Securing the Internet against cyber terrorism and using universal jurisdiction as a deterrent. disponible à: http://ssrn.com/abstract=1452803

Gabriel Weimann, (2015). www.Terror.Net: How Modern Terrorism Uses the Internet, Special Report 116 (Washington, DC: United States Institute of Peace, 2004);

Maura Conway, (2006). «Terrorisme et Internet: nouveaux médias - nouvelle menace», Affaires parlementaires, 59 (2) (2006), p. 283-298;

Stuart Macdonald et David Mair, (2015). «Terrorisme en ligne: un nouvel environnement stratégique», dans Lee Jarvis, Stuart Macdonald et Thomas M. Chen, éd., Terrorisme en ligne: politique, droit et technologie (Abingdon: Routledge, 2015), pp. 10-34.

Gambrell Jon, (2012). "Al-Qaïda blâme l'Allemagne pour la mort d'un otage lors d'un raid", Associated Press (12 juin 2012). Gardham, Duncan, otage britannique Edwin Dyer Exécuté par al-Qaïda au Mali, The Telegraph.

George Gorman, (2010). Blog d'Al-Qaïda au Maghreb Islamique, The Long War Journal (5 août 2010), disponible à : http://www.longwarjournal.org/today-in/2010/08/al_qaeda_in_the_islamic_59.php

Glenn Curtis et Tara Karacan, (2002). Le lien entre les terroristes, les trafiquants de stupéfiants, les prolifératéurs d'armes et les réseaux de criminalité organisée en Europe occidentale, une étude préparée par la Division fédérale de la recherche, Bibliothèque du Congrès, décembre 2002, p. 22, disponible à : http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf

Grand Jury Acte d'accusation, (2000). U.S. c. Mohamad Youssef Hammoud, et al, Dossier 3: 00CR-147-MU (Cour de district des États-Unis pour la Division de loterie du District de l'Ouest de la Caroline du Nord, 31 juillet 2000), disponible à : http://fl1.findlaw.com/news.findlaw.com/wp/docs/terrorism/ushammoud32801ind.pdf

Gregory Crabb, (2007). "NOUS. Service postal Global Investigations », et Yuval Ben-Itzhak,« CTO Finjan », Présentation au Gartner IT Security Summit 2007, Washington, DC, 4 juin 2007.

Helen Pidd, (2012). "Contexte: L'Enlèvement d'Edwin Dyer", The Guardian (3 juin 2009), disponible à : http://www.guardian.co.uk/world/2009/jun/03/edwin-dyer-hostage-killed-al-qaida

kathy Gilsinan, (2015). “Is ISIS’s Social-Media Power Exaggerated?”. The Atlantic daily (23 Feb 2015), disponible à: https://www.theatlantic.com/international/archive/2015/02/is-isiss-social-media-power-exaggerated/385726/

Nabeelah Jaffer, (2015). “The Secret World of ISIS Brides: ‘U dnt hav 2 pay 4 ANYTHING if u r wife of a martyr,’” The Guardian, June 24, 2015, disponible à: http://www.theguardian.com/world/2015/jun/24/isis-brides-secret-world-jihad-western-women-syria

James Lewis, (2002). «Évaluation des risques du cyberterrorisme, de la guerre cybernétique et d'autres menaces cybernétiques», décembre 2002 disponible à l'adresse http://www.csis.org/tech/0211_lewis.pdf

James P. Farwell, (2014). "La stratégie médiatique de l'Etat islamique", Survival 56, no. 6 (2014): 50.

Jeremy White, (2012). "L'endoctrinement virtuel et le Digihad: l'évolution de la stratégie médiatique d'Al-Qaïda" Small Wars Journal, 19 novembre 2012. Disponible à : http://smallwarsjournal.com/jrnl/art/virtual-indoctrination-and-the-digihad

Jeroen Gunning et Richard Jackson, (2011). "Qu'est-ce donc" religieux "au sujet du" terrorisme religieux "?" Critical Studies on Terrorism 4 (3) (2011), pp. 369-388.

Jerrold Post, (2007). L'esprit du terroriste: la psychologie du terrorisme de l'IRA à Al-Qaïda (Basingstoke: Palgrave, 2007).

Jessica Stern et J. M. Berger, (2014). "ISIS: l'état de terreur" (Londres: William Collins, 2015); Patrick Cockburn, «La montée de l'État islamique: ISIS et la nouvelle révolution sunnite» (Londres: Verso, 2014).

Jessica Stern et J. M. Berger, (2015). " ISIS and the Foreign-Fighter Phenomenon. Why do people travel abroad to take part in somebody else's violent conflict? The Atlantic 8 Mar 2015. Disponible à : https://www.theatlantic.com/international/archive/2015/03/isis-and-the-foreign-fighter-problem/387166/

Joseph Lieberman et Susan Collins, (2008). L'extrémisme islamiste violent, Internet et la menace terroriste interne (Washington, DC: Comité sénatorial américain sur la sécurité intérieure et les affaires gouvernementales, 2008). Disponible à : https://www.hsdl.org/?view&didD485776

John Swartz, (2004). «L'impact du cyberterrorisme, la défense sous surveillance», USA Today, 3 août 2004, p. 2B.

John Rollins et Clay Wilson, (2007). Capacités terroristes pour la cyberattaque: Aperçu et questions de politique (Rapport CRS RL33123). Disponible à : https://fas.org/sgp/crs/terror/RL33123.pdf

Jonathan Bishop, (2014). "Représentations des" Trolls "dans la communication de masse: Une revue des textes médiatiques et des paniques morales relatives à la" pêche à la traîne sur Internet "," International Journal of Web Based Communities 10, no. 1 (2014): p. 12.

Harowitz Richard (2010). "The global anti money laundering regime: a short review." Cayman island.

Haroro J. Ingram, (2014). "Trois Traits de la Guerre d'Information de l'Etat Islamique", The RUSI Journal 159, no. 6 (2014): p. 4.

Holly Fletcher, (2008). «État sponsor: Syrie», Council on Foreign Relations (février 2008), disponible à : http://www.cfr.org/syria/state-sponsor-syria/p9368

Horand Knaup, (2012). "Attaques suicides au Nigeria: le réseau islamiste terroriste gagne en force en Afrique", Spiegel Online (4 janvier 2012), disponible à : http://www.spiegel.de/international/world/suicide-attacks-in-nigeria-islamist-terror-network-gains-strength-in-africa-a-806749.html

Ivona Pastor Perisa, (2012). "Formes organisationnelles de l'organisation terroriste moderne", Polemos 15 (2012) 2: p. 139-156.

Irwin Angela, Slay Jill, Choo Kim-kwang Raymond, et Lui Lin, (2013). "Les transactions financières menées dans des environnements virtuels sont-elles vraiment anonymes?: Une recherche expérimentale d'un point de vue australien", Journal of Money Laundering and Control, Vol. 16 No. 1, pp. 6-40.

Irwin Angela, Slay Jill, Choo Kim-kwang Raymond, et Lui Lin, (2014). "Le blanchiment d'argent et le financement du terrorisme dans les environnements virtuels: une étude de faisabilité", Journal of Money Laundering Control, Vol. 17 No. 1, pp. 50-75, doi: 10.1108 / JMLC-06-2013-0019.

Kien-Meng Ly, M. (2014). "Coining Bitcoin's 'Legal-bits': examiner le cadre réglementaire pour Bitcoin et les monnaies virtuelles", Harvard Journal of Law and Technology, vol. 27 No. 2, pp. 587-606.

Krieger, Tim. et Meierrieks, Daniel. (2011). "Financement du terrorisme et blanchiment d'argent", disponible à : http://groups.uni-paderborn.de/fiwi/RePEc/Working%20Paper%20neutral/WP40%20-%202011-07.Pdf

LaVerle Berry, Glenn E. Curtis, John N. Gibbs, Rex A. Hudson, Tara Karacan, Nina Kollars, (2002). Un aperçu mondial des groupes terroristes et autres groupes extrémistes financés par des stupéfiants, Division de la recherche fédérale, Bibliothèque du Congrès, Washington, DC, mai 2002.

Laqueur Walter, (1999). Le nouveau terrorisme: le fanatisme et les armes de destruction massive, Oxford University Press, Oxford.

Levitt Matthew, (2007). "Le Hezbollah finance: financer la fête de Dieu", dans Giraldo, J.K. et Trinkunas, H.A. (Eds), Financement du terrorisme et réponses des États: Perspective comparative, Stanford University Press, Standford, CA.

Lipson F. Howard, (2002). Tracking and tracing cyber-attacks. Disponible à: http://www.cert.org/archive/pdf/02sr009.pdf

Louise Shelly, (2004). Crime organisé, Cybercriminalité et Terrorisme, Centre de recherche sur la criminalité informatique, 27 septembre 2004, disponible à : http://www.crime-research.org/articles/Terrorism_Cybercrime/

Manuel Torres, Javier Jordán et Nicola Horsburgh, (2006). "Analyse et évolution de la propagande du mouvement djihadiste mondial", Terrorisme et violence politique 18 (3) (2006), pp. 399-421.

Martha Crenshaw, (1981). "The Causes of Terrorism", Comparative Politics 13 (4) (1981), pp. 379-399.

Martin James, (2014). "Perdu sur la route de la soie: la distribution de drogue en ligne et le" Cryptomarket "", Criminology and Criminal Justice, Vol. 14 No. 3, pp. 351-367.

Mark Eddy, (2004). Guerre contre la drogue: Réautorisation de l'Office de la politique nationale de contrôle des drogues, Rapport CRS RL32352. DC Préfontaine, cr, et Yvon Dandurand, Réflexions sur le terrorisme et le crime organisé sur un lien insaisissable et son implication pour la réforme du droit pénal, Réunion annuelle de la Société internationale pour la réforme du droit criminel - Montréal, 8 au 12 août, Atelier D-3 Crime organisé, 11 août 2004, disponible à : http://www.icclr.law.ubc.ca/Publications/Reports/International%20Society%20Paper%20of%20Terrorism.pdf

Matthew Lee et Katherine Shrader, (2007). Al-Qaïda a été reconstruite, avertit l'agence américaine Intel, Associated Press, 12 juillet 2007, disponible à : http://news.yahoo.com/s/ap/20070712/ap_on_go_pr_wh/us_terror_threat_32;_ylt=AuURr2eP8AhBrfHyTOdw714Gw_IE. Associated Press, «La récolte de pavot en Afghanistan pourrait rapporter plus que le record de 2006, selon l'ONU», International Herald Tribune, 25 juin 2007 , disponible à : http://www.iht.com/articles/ap/2007/06/25/asia/AS-GEN-Afghan-Drugs.php

Matthew David, Amanda Rohloff, Julian Petley et Jason Hughes, (2011). "L'idée des dimensions morales de la panique du conflit", Criminalité, Médias, Culture 7, no. 3 (2011): 215-28; Gary Clapton, Vivien E. Cree et Mark Smith, «Paniques morales et travail social: vers une vision sceptique de la protection de l'enfance au Royaume-Uni», Critical Social Policy 33, no. 2 (2013): p. 197-217.

Meiklejohn Sarah, (2013). "Une poignée de Bitcoins: caractériser les paiements entre hommes sans noms", IMC, disponible à: https://cseweb.ucsd.edu/_smeiklejohn/files/imc13.pdf

Middlebrook, Stephen T., Hughes, Sarah Jane, (2014). "Réglementer les cryptomonnaies aux États-Unis: problèmes actuels et orientations futures", William Mitchell Law Review, vol. 40, pp. 813-848.

Michele K. Esposito, (2003). Rapport trimestriel sur les conflits et la diplomatie, Journal of Palestine Studies 33 (1) (automne 2003), pp. 116-138, disponible à http://www.palestine-studies.org/files/pdf/jps/5663.pdf

Mitchell D. Silber et Arvin Bhatt, (2007). Radicalisation dans l'Ouest: la menace Homegrown (NYPD Intelligence Division, 2007), disponible à : http://www.nypdshield.org/public/SiteFiles/documents/NYPD_Report-radicalization_in_the_West.pdf

Michael George, (2012). La terreur des loups solitaires et la montée de la résistance sans chef, Vanderbilt University Press, Nashville, TN.

Middlebrook, S. (2014). "Bitcoin pour les commerçants: considérations juridiques pour les entreprises souhaitant accepter les bitcoins comme mode de paiement", Business Law Today, disponible à: www.americanbar.org/publications/blt/2014/11/02_middlebrook.html

Daniel A. Morris, (2001). “Tracking a Computer Hacker,” May 2001. Disponible à: https://www.justice.gov/sites/default/files/usao/legacy/2006/06/30/usab4903.pdf

Morris, Loveday. (2010)."The Anatomy of a Suicide Bomber? National (Abu Dhabi), October 24. http://www.thenationalae/news/the-anatomy-of-a-suicide-bomber.

Nabeelah Jaffer, (2015). "Le monde secret de Brides ISIS: 'U dnt hav 2 payer 4 TOUT si vous êtes la femme d'un martyr,'" The Guardian, Juin 24, 2015, disponible à : http://www.theguardian.com/world/2015/jun/24/isis-brides-secret-world-jihad-western-women-syria

Nakamoto, Satoshi, (2008). "Bitcoin: un système de paiement électronique Peer-to-Peer", disponible à: https://bitcoin.org/bitcoin.pdf

Napoleoni Loretta, (2005). Terror Incorporated: Tracer les dollars derrière les réseaux terroristes, Seven Stories Press, New York, NY.

Nimmo Kurt, (2012). "Attaque terroriste française: toutes les caractéristiques d'une intelligence psy-op et d'un faux drapeau", disponible à: www.infowars.com/french-terror-attack-all-the-hallmarks-of-an-intelligencepsy-op-and- faux drapeau/

Makarenko Tamara, (2004). "Le continuum crime-terreur: traçage de l'interaction entre le crime organisé transnational et le terrorisme", Global Crime, Vol. 6, pp. 129-145.

Oftedal Emilie, (2015). "Le financement des cellules terroristes djihadistes en Europe", Centre norvégien de recherches pour la défense, rapport FFI 2014/02234.

Paul Best, Roger Manktelow et Brian Taylor, (2014). «La communication en ligne, les médias sociaux et le bien-être des adolescents: un examen narratif systématique», Revue des services à l'enfance et à la jeunesse 41 (2014): p. 27-36.

Pearce Rohan, (2012). "Blanchiment d'argent en utilisant des mondes virtuels, Bitcoin sur le radar de surveillance", disponible à: www.computerworld.com.au/article/433634/money_laundering_using_virtual_worlds_bitcoin_watchdog_radar/#closeme

Peresin Anita, (2007). "Paradigma novog terorizma informacijskoga doba" Politicka Misao Vol. XLIV, (2007), br. 2, p. 93-112.

Petrovic S. (2007). Informatique policière, criminalistique et académie de police, Belgrade, 2007, p. 110.

Pflaum Isaac et Hateley Emmeline, (2014). "Un peu de problème: la régulation nationale et extraterritoriale de la monnaie virtuelle à l'ère de la désintermédiation financière", Georgetown Journal of International Law, vol. 45 No. 4, pp. 1169-1215.

Rand Beers et Francis X. Taylor, (2002). Département d'Etat américain, Narco-Terror: Le lien mondial entre la drogue et la terreur, témoignage devant le Comité judiciaire du Sénat américain, sous-comité sur la technologie, le terrorisme et l'information gouvernementale, 13 mars 2002.

Rick Kania, (2011). "Le projet de Karachi: le Pakistan utilise-t-il la terreur pour contrebalancer l'avantage militaire de l'Inde?" Institut pour l'étude des groupes violents (25 juillet 2011), disponible à : http://www.isvg.org/follow/blog/2011/07/25/the-karachi-project-is-pakistan-using-terror-to-balance-against-indias-military-advantage/

Robert Windrem, (2003). «Détenu du 11 septembre: Attaque réduite», 21 septembre 2003, disponible à : http://www.msnbc.com/news/969759.asp

Rollie Lal, (2005). «Les terroristes et le crime organisé unissent leurs forces», International Herald Tribune, 25 mai 2005, disponible à : http://www.nytimes.com/2005/05/24/opinion/terrorists-and-organized-crime-join-forces.html

Senator Lieberman et Collins, (2009). "Extrémisme islamiste violent". Disponible à : https://fas.org/irp/congress/2009_hr/violent.pdf

Sara Fritz et Joel Havemann, (1991). "Les premiers signes du scandale BCCI ont été ignorés", The Los Angeles Times (4 août 1991), disponible à : http://articles.latimes.com/1991-08-04/news/mn-268_1_bcci-scandal

Shawn Pogatchnik, (2005). 3 Fugitifs liés à l'IRA de retour en Irlande - FARC formés en Colombie - Se sont cachés au Venezuela / Cuba, The Boston Globe (6 août 2005), disponible à : http://www.freerepublic.com/focus/f-news/1458099/posts

Simser Jeffrey, (2011). "Le financement du terrorisme et la menace pour les institutions financières", Journal of Money Laundering Control, Vol. 14 No. 4, pp. 334-345.

Spaaij Ramon, F.J. (2012). Comprendre le terrorisme des loups solitaires: modèles, motivations et prévention dans le monde, Springer, Dordrecht.

Susan Herring, Kirk Job-Sluder, Rebecca Scheckler et Sasha Barab, (2002). "À la recherche de la sécurité en ligne: gérer la pêche à la traîne dans un forum féministe", The Information Society 18, no. 5 (2002): p. 371 à 384, p. 372.

Tom McTague, (2014). "Plus de Britanniques signant un combat contre les activistes jihadistes en Irak et en Syrie que pour la Réserve de l'armée britannique", Daily Mail, 17 juin 2014. Disponible à : http://www.dailymail.co.uk/news/article- 2659237 / More-Britanniques-signature-combat-djihadistes-militants-Irak-Syrie-UK-Army-Reserve.html

Unger Brigitte, Daan van der Linde, (2013). Manuel de recherche sur le blanchiment d'argent, Edawrd Elgar Publishing, Londres.

Veal, Anthony James, (2011). *Research methods for leisure and tourism: a practical guide.* Harlow: Financial Times Prentice Hall

Vittori, Jodi, (2011). Financement du terrorisme et ressourcement, Palgrave Macmillan, New York, NY.

Nouvelles de la BBC (19 octobre 2011). Les chercheurs avertissent du nouveau ver Stuxnet. Disponible à : http://www.bbc.com/news/technology-15367816

BBC news, (2012). "BBC," Abou Qatada perd la dernière offre pour la liberté ", BBC News (Juillet 31, 2012), disponible à : http://www.bbc.co.uk/news/uk-19064369

Associated Press BBC, (2012). "Un ingénieur allemand enlevé au Nigeria a été tué au cours d'une tentative de sauvetage ratée". Disponible à : http://www.bbc.com/news/world-africa-18278740

BBC news, (2012). "Des Nigérians accusés de liens avec Al-Qaïda dans la péninsule arabique", BBC News Africa (6 juillet 2012), disponible à : http://www.bbc.co.uk/news/world-africa-18732176

Réseau du ministère de la Trésorerie sur les crimes financiers (2013). "Application du règlement FinCEN aux personnes qui administrent, échangent ou utilisent des monnaies virtuelles", disponible à : http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf

Site Web du FBI, (2001). Stats-Services. Disponible à : http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror

Le Groupe d'action financière (2001). "Rapport sur les typologies de blanchiment d'argent 2000-2001", The Financial Action Task Force.

Le Groupe d'action financière (2003). "Rapport sur les typologies de blanchiment d'argent 2002-2003", The Financial Action Task Force.

Le Groupe d'action financière (2003-2004). "Rapport sur les typologies de blanchiment d'argent 2003-2004".

Le Groupe d'action financière (2008). "Financement du terrorisme".

GAFI (2008), «Financement du terrorisme» GAFI + GAFI, Paris, www.fatf-gafi.org;

Le Groupe d'action financière (2012). Normes internationales de lutte contre le blanchiment d'argent et le financement du terrorisme et de la prolifération.

Groupe d'action financière (2014). "Monnaies virtuelles - définitions clés et risques potentiels de LBC / FT", Groupe d'action financière, disponible à: www.fatfgafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

GAFI (2015). "L'action du GAFI en matière de financement du terrorisme", disponible à : www.fatf-gafi.org/documents/news/fatfaction-on-terrorist-finance.html

Site web de la FEMA, (2017). Disponible à : http://www.fema.gov/pdf/onp/toolkit_app_d.pdf

Federal Bureau of Investigation (2013). "L'avocat américain de Manhattan annonce la saisie d'une valeur additionnelle de 28 millions de dollars de bitcoins appartenant à Ross William Ulbricht, propriétaire présumé et exploitant du site Web" route de la soie ", disponible à : http://www.liberation.fr/ecrans/2013/10/04/the-silkroad-le-fbi-fait-tomber-l-amazon-de-la-drogue_936748

HM Treasury (2007), Le défi financier de la criminalité et du terrorisme, HM Treasury, Londres, disponible à : http://webarchive.nationalarchives.gov.uk/+/http:/www.hm-treasury.gov.uk/media/C/B/financialchallenge_crime_280207.pdf

ICE.gov, (2011). «Mohamad Youssef Hammoud, condamné à 30 ans de prison pour financement du terrorisme» (Communiqué de presse de l'ICE, 27 janvier 2011), disponible à : http://www.ice.gov/news/releases/1101/110127charlotte.htm

Nydailynews.com, (2012). "Un ingénieur allemand kidnappé au Nigéria a été tué au cours d'une tentative de sauvetage ratée", New York Daily News (31 mai 2012), disponible à : http://www.nydailynews.com/news/world/german-engineer-kidnapped-nigeria-killed-failed-rescue-attempt-article-1.1087360

OnlineNigeria.com, (2012). "Boko Haram donne raison à Robbing Banks", Nigeria News, (14 février 2012), disponible à : http://news2.onlinenigeria.com/latest-addition/139998-boko-haram-gives-reason-for-robbing-banks.html

Sécurité publique Canada, (2012). "Entités actuellement listées", disponible à : http://www.securitepublique.gc.ca/prg/ns/le/cle-fra.aspx;

Reuters, (2011). "Terror Market:" Le TTP a vendu un kamikaze à des militants afghans "" The Express Tribune (4 juillet 2011), disponible à : http://tribune.com.pk/story/201828/insurgents-bought-suicide-bomber-from-pakistan-taliban-afghan-spy-agency/

Agence de lutte contre la criminalité organisée (2006). "L'évaluation de la menace de crime organisé grave au Royaume-Uni", disponible à: www.soca.gov.uk/assessPublications/downloads/threat_assess_unclass250706.pdf

Statista, (2017). "Nombre d'utilisateurs de Smartphone dans le monde de 2014 à 2020 (en millions)," Statista. Disponible à : http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

La Commission nationale sur les attentats terroristes contre les États-Unis, «Le rapport de la Commission sur le 11/9» (17 juillet 2004), p. 169, disponible à : http://govinfo.library.unt.edu/911/report/911Report.pdf

The Economist, (2005). "Financer le terrorisme: regarder dans les mauvais endroits" (20 octobre 2005), disponible à : http://www.economist.com/node/5053373

Thisdaylive.com, (2011). "Boko Haram, Armed Robbers attaque 100 succursales bancaires," This Day (10 décembre 2011), disponible à : http://www.thisdaylive.com/articles/boko-haram-armed-robbers-attack-100-bank-branches/104715/

Ahlers, Mike M. (2004). "Des plans pour les terroristes?" CNN.com, 19 Octobre. http://www.cnn.com/2004/US/10/19/terror.nrc/.

Amble, John Curtis. (2012). "Combattre le terrorisme dans le nouvel environnement médiatique." Etudes sur les conflits et le terrorisme 35 (5): p. 339-53.

Buckley, Cara et William K. Rashbaum. (2007). "4 hommes accusés de complot pour exploser les terminaux et les canalisations de l'aéroport Kennedy: New York Times, 3 juin. http://www.nytimes.com/2007/06/03/nyregion/03plot.html.

Denning, Dorothy. (1998). Information Warfare and Security, New York: Addison-Wesley.

--. 2000. «Cyberterrorisme: Témoignage devant le Groupe spécial de contrôle du terrorisme». Déclaration à la Chambre des représentants des États-Unis, Comité des services armés, 23 mai.
http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf.

--. 2001. «Activisme, hactivisme et cyberterrorisme: Internet comme outil pour influencer la politique étrangère». Dans Réseaux et réseaux: l'avenir de la terreur, du crime et de la militantité, édité par John Arquilla et David Ronfeldt, 239-88. Santa Monica, Californie: RAND Corporation.

--. 2010. "Web Terror: Comment Internet transforme le terrorisme." Dans Handbook of Internet Crime, édité par Yvonne Jewkes et Majid Yar, 194-213. Cullompton, Royaume-Uni: Willan Publishing.

Commission européenne. (2008). «Processus de radicalisation conduisant à des actes de terrorisme», Groupe d'experts sur la radicalisation violente, Commission européenne, http://www.clingendael.nl/sites/default/files/20080500_cscp_report_vries.pdf.

Europol. (2012). Rapport annuel sur la situation et les tendances en matière de terrorisme. Office européen de police.
https://www.europol.europa.eu/sites/default/files/publications/europoltsat.pdf.

Fouda, Yosri et Nick Fielding. (2003). "Les cerveaux de la terreur: la vérité derrière l'attaque terroriste la plus dévastatrice que le monde ait jamais vue." New York: Arcade.

Gerwehr, Scott et Sara Daly. (2006). "Al-Qaïda: sélection et recrutement terroristes". Dans le manuel de la sécurité intérieure de McGraw-Hill, édité par David Kamien, 73-89. New York, McGraw-Hill.

Hafner, Katie et Saritha Rai. (2005). "Les gouvernements tremblent à la vue de Bird's-Eye de Google." New York Times, 20 décembre. Disponible à:
http://www.nytimes.com/2005/12/20/technology/20image.html.

Harding, Thomas. (2007). "Les terroristes utilisent Google Maps pour frapper les troupes britanniques." Daily Telegraph (Londres), 13 janvier. Disponible à: http://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html.

Hoffman, Bruce. (2006a). "Inside Terrorism, version révisée." New York: Columbia University Press.

--2006b. «L'utilisation d'Internet par des extrémistes islamiques», témoignage présenté à la Chambre du Comité permanent des renseignements, 4 mai 2006. http://www.au.af.mil/au/awc/awcgate/congress/hoffman_testimony4may06.pdf

Hoffman Bruce, Mary Habeck, Aaron Y. Zelin, et Matthew Levitt. (2012). "Est-ce que Al-Qaïda Central est toujours pertinent?" Institut de Washington pour la politique du Proche-Orient, 10 septembre. https://www.washingtoninstitute.org/policy-analysis/viewns-al-qaeda-central-still-relevant.

Jacobson Michael, (2008). “Why Terrorists Quit: Gaining from Al Qa'ida's Losses." CTC Sentinel 1 (8): p. 1-4. https://www.ctc.usma.edu/posts/why-terrorists-quit-gaining-from-al-qaida%E2%80%99s-losses.

--. 2010a. Learning Counter-Narrative Lessons from Cases of Terrorist Dropouts. The Hague: National Coordinator for Counterterrorism.

https:// www.washingtoninstitute.org/uploads/Documents/opeds/4b7aaf56ca52e.pdf.

-.2010b."Terrorist Financing and the Internet." Studies in Conflict& Terrorism 33 (4): 353-63. Jenkins, Brian. 1975. International Terrorism. Los Angeles: Crescent Publication.

--. 2011. Is Al Qaeda's Internet Strategy Working? Santa Monica, CA: RAND Corporation. http://www.rand.org/pubs/testimonies/CT371.html

Merriam, Lisa. (2011). "La marque Al-Qaïda est morte la semaine dernière." Forbes, 6 octobre. Disponible à: http://www.forbes.com/sites/realspin/2011/10/06/the-al-qaeda-brand-died-last-week/.

Minei, Elizabeth, and Jonathan Matusitz. 2011."Cyberterrorist Messages and Their Effects on Targets: A Qualitative Analysis? Journal of Human Behavior in the Social Environment 21 (8): p. 995-1019.
--.2012. "Cyberspace as a New Arena for Terroristic Propaganda: An Updated Examination:'Poiesis & Praxis 9 (1-2): p. 163-76.

Obama, Barack. (2014). "Transcription du discours du président Obama sur les réformes de la NSA." NPR, 17 janvier. Disponible à: http://www.npr.org/blogs/itsallpolitics/2014/01/17/263480199/transcript-of-president-obamas-speech-on-nsa-reforms.

Peter Bergen, (2006). “The Taliban, Regrouped and Rearmed,” *The Washington Post*, September 10, 2006, p. B1. Helen Cooper, “NATO Chief Says More Troops Are Needed in Afghanistan,” *The New York Times*, September 22, 2006, p. 10.

Rumsfeld, Donald. (2006). "Les nouvelles réalités à l'ère des médias." Discours au Council on Foreign Relations, 17 février. Disponible à: http://www.cfr.org/publication/9900/new_realities_in_the_media_age.html.

Schmitt, Eric et Michael S. Schmidt. (2013). "La fuite de complot de Qaeda a troublé l'intelligence des Etats-Unis." New York Times, le 29 septembre. http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html.

Schmittdec Eric, (2014). “In Battle to Defang ISIS, U.S. Targets Its Psychology,” The New York Times, December 28, 2014, Disponible à: http://www.nytimes.com/2014/12/29/us/politics/in-battle-todefang-isis-us-targets-its-psychology-.html?_r=0

Schneier Bruce, (2009). "Les terroristes peuvent utiliser Google Earth, mais la peur n'est pas une raison pour l'interdire." Guardian (Londres), 28 janvier. http://www.theguardian.com/technology/2009/jan/29/read-me-first-google-earth.

Siddiqui Sabrina et Jaweed Kaleem. (2013). "Les musulmans se concentrent sur l'extrémisme en ligne, la radicalisation après les attentats de Boston." Huffington Post, 4 juin.http://www.huffingtonpost.com/2013/06/04/muslims-online-extremism-radicalization-boston_n_3380159.html.

Shane Scott, (2013). "Un style de terreur fait à la maison: les djihadistes poussent de nouvelles tactiques." New York Times, Mat 5. Disponible à: http://www.nytimes.com/2013/05/06/us/terrorists-find-online-education-for-attacks.html.

SITE Monitoring Service. 2005. "Salafi Group for Call and Combat Issues Fatwa Calling for Jihad Against Foreigners in Algeria:' March 11. http://ent.siteintelgroup.com/Jihadist-News/salafi-group-for-call-and-com-bat-issues-fatwa-calling-for-jihad-against-foreingners-in-algeria.html.

--. 2008. "Al-Nusra Media Battalion Distributes Guide for 'Martyrdom:" December 18. http://entsiteintelgroup.comaihadist-News/al-nusra-media-battalion-distributes-guide-for-martgdom.html.

-- 2011a. "Jihadist Offers Tips for Facebook Users to Increase Page Viewership." June 2. https://news.siteintelgroup.com/index.php/21-social-network-jihad/776-jihadist-offers-tips-for-facebook-users-to-increase-page-viewership.

-- 2011b. "Jihadists Strategize to Evade YouTube Censorship? April 28. http://ent.siteintelgroup.com/Social-Network-Jihad/site-intel-group-4-28-11-jfm-youtube-strategies.html.

--. 2011c. °Jose Pimentel and the Use of Social Networks for Jihadist Recruitment" January 14. https://news.siteintelgroup.com/Social-Network-Jihad/jose-pimentel-and-the-use-of-social-networks-for-jihadist-recruitment.html.

--. 2012a. "'Cyber Fighters' Announces 'Phase 2' of Banking Website Hacks!' December 11. http://entsiteintelgroup.comahadist-News/cyber-fighters-announces-phase-2-of-banking-website-hacks.html.

-- 2012b. "Jihadist Gives Analysis of Electronic Jihad? January 6. http://news.siteintelgroup.com/index.php/19-jihadist-news/1462-jihadist-gives-analysis-of-electronic-jihad.

--. 2013a. "Al-Qaeda Electronic Army' Threatens to Hit Vital Sectors of the US!' April 12. http://entsiteintelgroup.comaihadist-News/al-qaeda-electronic-army-threatens-to-hit-vital-sectors-of-us.html.

--2013b. "AQIM Blames Hezbollah for Tripoli Bombings, Promises Retribution:' August 23. http://entsiteintelgroup.comahadist-News/aqim-blames-hezbollah-for-tripoli-bombings-promises-retribution.html.

--. 2013c. °Facebook Page Serves as Official Facebook Outlet for Ansar al-Islam? August 6. https://news.siteintelgroup.com/index.php/19-jihadist-news/3342-facebook-page-serves-as-official-facebook-outlet-for-ansar-al-islam.

-- 2013d.lihadists Create Twitter-based Jihadi Media Group, Al-Battar Media Battalion" July 19. https://news.siteintelgroup.comilihadist-Newsnihadists-create-twitter-based-jihadi-media-group-al-battar-media-battalion.html.

--. 2014a. "Female Jihadists Promote Attacks in West in Third Issue of Magazine? January 15. https://news.siteintelgroup.com/Jihadist-News/female-jihadists-promote-attacks-in-west-in-third-issue-of-magazine.html.

-- 2014b. "Jihadist Invites to 'Electronic Islamic Army" Gives DDOS Program Tutorial? January 15. https://news.siteintelgroup.comahadist-News/jihadist-invites-to-qelectronic-islamic-armyq-gives-ddos-program-tutorial.html.

--. 2014c. "Social Network Jihad: Hezbollah's Capitalization of Facebook:' January 14. https://news.siteintelgroup.com/Social-Network-Jihad/social-network-jihad-hezbollahs-capitalization-of-facebook.html.

--.2014d."TheThird Palestinian Intifada's Facebook Page.” January 15. https://news.siteintelgroup.com/Featured-Article/the-third-palestinian-intifadas-facebook-page.html.

Thomas, Timothée. (2003) "Al-Qaïda et Internet: le danger de la cyber-planification". Paramètres (ressort): p. 112-23. Disponible à: http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/03spring/thomas.pdf.

Groupe de travail de l'ONU sur la lutte contre le terrorisme. (2011). Contrer l'utilisation d'Internet à des fins terroristes: aspects juridiques et techniques. New York: Nations Unies.
--. 2012. «L'utilisation d'Internet pour contrer l'attrait de la violence extrémiste» Résumé de la conférence et suivi / Recommandations: Perspectives sur le terrorisme 6 (1): 80-91 http://www.terrorismanalysts.com/pt/index.php/pot/article/view/CTITF-Utilisation-de-Internet/html.

Office des Nations Unies contre la drogue et le crime (ONUDC). (2012). L'utilisation d'Internet à des fins terroristes. New York: Nations Unies.

Conseil de sécurité des Nations Unies. (2009). "Comité du Conseil de sécurité créé par les résolutions 1267 (1999) et 1989 (2011) concernant Al-Qaida et les personnes et entités associées:" Consulté le 13 octobre 2013. http://www.un.org/sc/committees/1267/NSQ123608E.shtml.
--. 2014. "Liste des sanctions contre Al-Qaida" Consulté le 1er octobre 2014. http://www.un.org/scicommittees/1267/AQList.htm.

Vaccani, Matteo. (2010). "Alternative Remittance Systems and Terrorism Financing." Document de travail n ° 1980. D'abord imprimé en novembre 2009. Washington, DC: Banque mondiale. http://elibrary.worldbank.org/doi/pdf/10.1596/978-0-8213-8178-6.

United Nations Office on Drugs and Crime (UNODC). (2012). The Use of the Internet for Terrorist Purposes. New York: United Nations.

Venhaus John, (2010). “Why Youth Join al-Qaeda. United States Institute of Peace,” United States Institute of Peace, May, 2010, Disponible à: http://www.usip.org/sites/default/files/SR236Venhaus.pdf

Verton, Dan. (2003). "Black Ice: la menace invisible du cyber terrorisme." New York: McGraw-Hill Osborne Media.

Weimann, Gabriel. 2005a."Cyberterrorism: The Sum of All Fears?" Studies in Conflict & Terrorism 28 (2): 129-49.

-- 2005b. "How Terrorists Use the Internet? Journal of International Security Affairs 8:91-105.

--.2005c."Terrorist Dot Com: Using the Internet for Terrorist Recruitment and Mobilization.” In The Making of a Terrorist: Recruitment, Training, and Root Causes, edited by James J. F. Forest, 53-65. Westport, a: Praeger.

--. 2006a. "Cyberterrorism.” In Security, Terrorism and Privacy in Information Society, edited by Katharina Von Knop and Boaz Ganor, 41-52. Bielefeld, Germany: W. Bertelsmann Verlag.

-- 2006b. Terror on the Internet: The New Arena. The New Challenges. Washington, DC: United States Institute for Peace (USIP) Press.

--. 2006c. "Virtual Disputes: The Use of the Internet for Terrorist Debates? Studies in Conflict & Terrorism 29 (7): 623-39.

--. 2006d. “Virtual Training Camps: Terrorist Use of the Internet? In Teaching Terror: Strategic and Tactical Learning in the Terrorist World, edited by James Forest, 110-32. Boulder, CO: Rowman & Littlefield.

--. 2007a. "Using the Internet for Terrorist Recruitment and Mobilization? In Hypermedia Seduction for Terrorist Recruiting, edited by Boaz Ganor, Katharina Von Knop, and Carlos Duarte, 47-58. NATO Science for Peace and Security Series. Amsterdam: IOS Press.

-- 2007b. “Virtual Terrorism: How Modern Terrorists Use the Internet? In The Internet and Governance in Asia: A Critical Reader, edited by Indrajit Banerjee,
189-216. Singapore: Asian Media Information and Communication Centre and Wee Kim Wee School of Communication and Information, Nanyang Technological University.

--2008a."Al-Qa'ida's Extensive Use of the Internet." CTC Sentinel. January 15. http://www.ctc.usma.edu/posts/al-qaida%E2%80%99s-extensive-use-of-the-internet.

--2008b."Cyber-Terrorism: Are We Barking at the Wrong Tree?" Harvard Asia Pacific Review 9 (2) (Spring 2008): 41-46.

--2008c."How Terrorists Use the Internet to Target Children." inSite 1 (8): 14- 16. http://sitemultimedia.org/docs/inSITE_December_2008.pdf.

--2008d. "Online Terrorists Prey on the Vulnerable? Yale Global Online. March 5. http://yaleglobaLyale.edu/content/online-terrorists-prey-vulnerable.

--.2008e."The Psychology of Mass-Mediated Terrorism:' American Behavioral Scientist 52 (1): 69-86.

--. 2008f. "WWW.AI-Qaeda: The Reliance of al-Qaeda on the Internet? In Responses to Cyber Terrorism, edited by Centre of Excellence-Defence Against Terrorism, Ankara, Turkey, 61-69. NATO Science for Peace and Security Series. Amsterdam: IOS Press.

--. 2009a. "Online Training Camps for Terrorists; InSite, Vol. 2 No. 9. http://sitemultimedia.org/docs/inSITE_Nov_2009.pdf.

--2009b. "Virtual Sisters: How Terrorists Target Women Online." InSite 2 (1): 19-22. http://sitemultimedia.org/docs/ingTE_January_2009.pdf.

--. 2009c. "War by Other Means: Econo-Jihad." Yale Global Online. June 4. http://yaleglobaLyale.edu/content/econo-jihad.

--2009d. "When Fatwas Clash Online: Terrorist Debates on the Internet? In Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas, edited by James Forest, 49-74. Westport, a: Praeger Security International.

--. 2010a. "Terror on Facebook, Twitter, and Youtube." The Brown Journal of World Affairs 16 (2): 45-54. http://brown.eduAnitiatives/journal-world-affairs/16.2/terror-facebook-twitter-and-youtube.

--2010b/Terrorism's New Avatars-Part II? Yale Global Online. January 12. http://yaleglobaLyale.edu/content/terrrorisms-new-avatars-part-ii.

--. 2010c. 'Terrorist Facebook: Terrorists and Online Social Networking? In Web Intelligence and Security, edited by Mark Last and Abraham Kande1,19-30. NATO Science for Peace and Security Series. Amsterdam: IOS Press.

--. 2011a. "Al Qaeda Has Sent You a Friend Request: Terrorists Using Online Social Networking? Paper presented at annual conference of the Israeli Communication Association, Haifa, Israel, April 14.
--2011b."Cyber-Fatwas and Terrorism: Studies in Conflict & Terrorism 34 (10): 765-81.
--. 2012a. “Lone Wolves in Cyberspace.” Journal of Terrorism Research 3 (2): 75-90. --2012b. "The Role of the Media in Propagating Terrorism? In Countering Terrorism: Psychosocial Strategies, edited by Updesh Kumar and Manas K. Mandal, 182-200. London: Sage Publications.
--. 2014a. New Terrorism and New Media. Commons Lab, Science and Technology Innovation Program. Washington, DC: Woodrow Wilson International Center for Scholars. http://www.wilsoncenter.org/publication/new-terrorism-and-new-media.
-- 2014b. "Virtual Packs of Lone Wolves.” Medium.com/@thewilsoncenter, February 28. https://medium.com/its-a-medium-world/virtual-packs-of-lone-wolves-17b12f8c455a.

Weimann Gabriel et Gabrielle Vail Gorder (2009). "Al-Qaïda vous a envoyé une demande d'ami: les terroristes utilisent les réseaux sociaux en ligne." InSite 2: 6. http://sitemultimedia.org/docs/inSITE_June_2009.pdf.

Zanini, Michele et Sean J. A. Edwards. (2001). «Le réseautage de la terreur à l'ère de l'information», dans Réseaux et réseaux: l'avenir de la terreur, de la criminalité et de la militance, sous la direction de John Arquilla et David Ronfeldt, 29- 60. Santa Monica, CA: RAND Corporation.

Thomas, Timothée. (2003) "Al-Qaïda et Internet: le danger de la cyber-planification". Paramètres (ressort): p. 112-23. Disponible à: http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/03spring/thomas.pdf.

U.K. House of Commons (2006), Report of the Official Account of the Bombings in London on 7th July 2005. Disponible à: https://www.gov.uk/government/publications/report-of-the-official-account-of-the-bombings-in-london-on-7th-july-2005