Le Cyber-terrorisme: Une menace pour le monde

Abdul-Sattar Abdul-Rahman

Journaliste et Chercheur

L'évolution technologique des moyens de communication modernes a fondamentalement transformé le terrorisme et contribué à remodeler ses formes actuelles; de sorte qu'il ne garde plus sa forme traditionnelle susceptible d'être ciblée et atteinte, mais il est devenu transfrontalier et donc difficile à contrôler en fermant ou en sécurisant les frontières. Les groupes terroristes sont désormais préoccupés par la propagation de l'idée et le recrutement d'éléments via Internet. Les camps d'entraînement sont désormais passés du monde réel au monde virtuel. Il n'est plus nécessaire de former des individus dans un camp terré dans une grotte ou au sommet d'une montagne, mais il suffit que le nouvel élément obtienne la formation dont il a besoin en puisant dans les sites Web des Groupes Terroristes.

Les plans et les outils terroristes en vogue ont changé au fil du temps, et le spectre du cyber-terrorisme se profile à l'horizon, grâce auquel les terroristes ciblent les infrastructures, les systèmes d'information et les bases militaires de l'État. Qu'est-ce que le cyber-terrorisme et quels sont ses risques et ses opportunités pour qu'on puisse y faire face et le surmonter?

Terrorisme électronique

Dans les années 80, *Barry Collin*, Chercheur à l'Institut de Sécurité et de Renseignement de Californie, a inventé le terme «*Cyber-terrorisme*» en référence à la convergence du cyberespace et du terrorisme. En 1998, le projet mondial du crime organisé relevant du Centre d'études stratégiques et internationales à Washington (CSIS) a publié un rapport intitulé: «*Cyber-criminalité, Cyber-terrorisme et Cyber-guerre: Éviter une Waterloo électronique*», qui a été la première contribution majeure dans ce domaine.

Bien que le cyber-terrorisme soit devenu populaire ces dernières années et constitue une menace majeure à l'échelle internationale, en particulier avec le développement rapide des technologies de communication et la dépendance croissante des humains à (*Internet*) et aux médias sociaux, il n'y a pas d'unanimité sur une véritable définition mondiale du cyber-terrorisme! Les définitions se sont multipliées écartelées entre le FBI, le Département Américain de la Défense, l'OTAN et d'autres institutions et centres de recherche concernés, portant leur nombre à plus de 27 définitions dont le dénominateur commun est que le cyber-terrorisme est le point où le terrorisme croise le cyberespace, tout en étant différend de la cyber-criminalité, du vol de données, de la fraude bancaire, ...etc.

Médias mondiaux

Le cyberespace constitue un important élément d'attraction pour les Organisations Terroristes de toutes sortes compte tenu des médias mondiaux qu'il met à leur disposition, devenant ainsi une redoutable arme dévastatrice. L'organisation terroriste Daech "EI" est considérée comme le Groupe qui menace le plus la sécurité d'Internet, en l'utilisant pour la propagande, le recrutement, le financement, la collecte d'informations, la coordination des attaques terroristes et la mobilisation de sympathisants de différentes parties du monde. Cette organisation a recruté une armée médiatique spécialisée dans les médias électroniques, opérant sous différents noms.

Il existe des facteurs qui incitent les Organisations Terroristes à utiliser le terrorisme électronique, notamment le fait qu'il peut être mis en œuvre de n'importe où dans le monde, de même que l'assaillant n'a pas besoin de se trouver sur le lieu de l'acte terroriste, les connexions Internet nécessaires pour mener l'attaque à l'aide d'un téléphone mobile moderne étant largement disponibles.

La vitesse des attaques électroniques ne dépend pas de la vitesse de la connexion Internet utilisée par l'attaquant, mais il est même possible de tirer profit de la vitesse élevée de la connexion Internet utilisée par les ordinateurs ciblés par l'attaque. Les virus et les autres logiciels nuisibles peuvent se propager le plus rapidement possible sans avoir besoin d'une action additionnelle de la part de l'agresseur.

Les actes commis par le biais du réseau peuvent être gardés anonymes et intraçables grâce aux services d'anonymisation et à des techniques de camouflage similaires, tels que l'utilisation d'ordinateurs piratés et sous contrôle. De plus, les preuves numériques

peuvent être falsifiées intentionnellement. La tentation du terrorisme électronique peut s'aggraver à cause du faible coût d'Internet et du grand nombre de cibles exposées aux attaques et ne jouissant pas de la protection adéquate.

À la lumière de ces tentations, divers groupes terroristes et extrémistes se sont précipités pour avoir leurs propres sites Internet, en particulier sur les réseaux sociaux. Certains possèdent plus d'un site et dans plus d'une langue, afin de présenter leurs organisations, leurs histoires, leurs fondateurs, leurs activités, leurs références idéologiques et sociales, leurs objectifs intellectuels et politiques, et leurs actualités, et pour s'attaquer à leurs adversaires et aux penseurs, érudits, gouvernements et services de sécurité.

Ainsi, Daech a soutenu ses capacités électroniques en unissant ses cyber-armes, telles que (*Le Califat fantôme*), (*L'armée des enfants du califat*), (*La Cyber Armée du Califat*) et (*Kalashnikov de la securité électronique*), autrement nommé: Groupe Unifié des Pirates du Califat Cybernétique.

Ces dernières années, un groupe de pirates de Daech a réussi à infiltrer certains sites Web pour les déformer et y diffuser de la propagande extrémiste, comme les sites du ministère britannique de la Santé, de la Police Royale Malaisienne, des Malaysia Airlines, de la chaîne de télévision française TV5 et de ses stations, et du Commandement Central Américain.

Deux catégories interdépendantes

Puisqu'il n'y a pas de définition précise et convenue du concept de cyber-terrorisme, deux catégories différentes de terrorisme se chevauchent: Le cyber-terrorisme pur et le cyber-terrorisme hybride.

Le premier type: le terrorisme électronique pur, concerne les attaques directes contre la cyber-infrastructure de la victime, telle que: Les ordinateurs, les réseaux et les informations qui y sont stockées; pour atteindre divers objectifs tels que la détérioration des fonctions des systèmes d'information, la destruction des actifs virtuels et physiques, le blocage de sites Web et la perturbation de la vie quotidienne en ciblant les infrastructures gérées par des logiciels, à l'instar des installations médicales, des bourses, du transport et des systèmes financiers, ...etc.

Quant au deuxième type; le terrorisme électronique hybride, il porte sur l'utilisation par les terroristes du cyberespace dans leurs diverses activités. Parmi ses modèles les plus importants, on peut citer:

1. Propagande et guerre psychologique. Ainsi: Daech compte sept agences de presse, en plus de 37 bureaux de presse dans différents pays. Al-Qaïda possède une branche médiatique appelée *Sahab*.
2. Communication sécurisée. L'objectif est d'envoyer des messages cryptés, dissimuler le contenu des discussions secrètes, ou planifier et coordonner des attaques, comme lors du meurtre du prêtre français en Normandie en Juillet 2016, dont les assassins ont reçu leurs instructions via le réseau.
3. Recruter de nouveaux membres. Un rapport du GAFI de 2015 a noté que le web est devenu l'outil le plus utilisé pour le recrutement et le soutien aux organisations terroristes.
4. Formation. Publier sur les sites des organisations les manuels de formation expliquant comment lancer des attaques et fabriquer des explosifs.
5. Collecte de dons.
6. Collecte d'informations sur les objectifs humains potentiels.

Risques terrifiants

Les bombes électroniques sont parmi les moyens les plus importants pour mener des opérations de terrorisme électronique, en vue de: Perturber et brouiller les communications, écouter les appels, transmettre des informations trompeuses, imiter les voix, en particulier les voix des chefs militaires pour émettre des ordres dangereux, cibler pour sabotage les réseaux informatiques en y propageant des virus, effacer la mémoire des dispositifs hostiles, empêcher le flux de fonds et modifier le cours des dépôts, empêcher les centrales de fonctionner par le biais d'une bombe électronique spéciale appelée CBU 49, destinée à cette tâche, qui lance à son tour plusieurs bombes en l'air, visant les centrales électriques pour les incendier et les détruire complètement.

Dans un papier intitulé: (*L'avenir du terrorisme électronique*) présenté lors du (11e Symposium International Annuel sur les Questions de Justice Pénale), le Chercheur *Barry Collin*, a présenté une liste terrifiante d'activités cyber-terroristes potentielles qui menacent l'avenir de l'humanité, dont notamment:

- Accès à distance aux systèmes de contrôle des usines de céréales, modification des niveaux de suppléments de fer, pour nuire à la santé des consommateurs.
- Ajustements à distance des préparations pour nourrissons pour nuire à leur santé.
- Perturber les banques, les transactions financières internationales et les bourses, afin de faire perdre confiance dans le système économique.
- Transformer à distance les ingrédients de l'industrie pharmaceutique en charge des sociétés pharmaceutiques.
- Modifier la pression dans les conduites de gaz et les charges des réseaux électriques, ce qui entraîne de terribles explosions et des incendies.
- Attaquer les systèmes de contrôle du trafic aérien et faire entrer en collision deux avions civils, en accédant aux capteurs dans les cockpits de l'avion, ce qui est également possible sur les chemins de fer.

Et si ces risques du cyber-terrorisme ne sont que des perceptions théoriques qui n'ont jamais eu lieu, grâce à Allah, cela ne devra pas pousser à peu s'en soucier, mais appelle plutôt à anticiper les vœux des terroristes et être fin prêts à avorter toute tentative insidieuse.

Nécessité de la confrontation

Les débuts des efforts internationaux pour lutter contre la cyber-criminalité et le terrorisme numérique remontent à trois décennies, lorsqu'Interpol a discuté en 1981 de la possibilité d'élaborer une législation juridique sur la cyber-criminalité. Depuis lors, les progrès ont été lents, mais ils se sont accélérés après la fin de la guerre froide. La création du *Cyberspace Law Institute* à l'Université de Georgetown en 1995 pourrait être considérée comme un indicateur de la prise de conscience du problème. Les pays ont eu tendance à adopter de nombreuses initiatives aux niveaux national, bilatéral, régional ou international, afin de protéger l'infrastructure mondiale de l'information contre les cyber-menaces et se sont activés à trouver de nouveaux cadres législatifs pour faire face à ce phénomène émergent en formulant un nouveau concept de sécurité nationale, avant de passer ensuite à la coopération internationale.

Heureusement, le monde comprend les risques des délits de cyber-terrorisme et cherche à les affronter en adoptant une stratégie internationale dans le domaine de la sécurisation du cyberespace, à travers un ensemble de lois et d'initiatives, dont la plus importante est l'Initiative de partenariat international multilatéral pour lutter contre le cyber-terrorisme (IMPACT) qui vise à mobiliser les efforts internationaux des secteurs gouvernementaux, du secteur privé et de la société civile afin de répondre aux menaces

croissantes du cyber-terrorisme, avoir des visions et des idées sur la formation et l'échange d'expériences, créer de nombreux sites Web pour lutter contre ce terrorisme et protéger la cyber-sécurité. Ces sites ont été un point de rencontre pour les experts de la sécurité de l'information et les politiciens pour discuter de la menace du terrorisme électronique et comment y faire face, tel le groupe de renseignement "SITE", qui est une agence de renseignement spécialisée dans la surveillance du terrorisme via Internet, l'étude des principales sources des terroristes, le suivi de leurs conversations et le contrôle de leur propagande.

Dans son article susmentionné, *Barry Collin* a fourni une liste d'éléments à respecter lors de la création d'un programme électronique de lutte contre le terrorisme:

- Construire une cyber-équipe en temps opportun, jouissant d'une grande flexibilité.
- Changer la façon dont nous traitons la lutte contre le cyber-terrorisme.
- Collaborer et partager les informations de renseignement selon de nouvelles procédures.
- Recourir aux individus qui comprennent la guerre à laquelle nous sommes confrontés.
- Connaitre les nouvelles règles, les nouvelles technologies et les nouveaux acteurs.
- Contrairement aux terroristes traditionnels, si un terroriste électronique est vaincu aujourd'hui, il ne meurt pas mais apprend et acquiert de l'expérience de sa défaite en utilisant ce qu'il a appris dans une nouvelle tentative réussie à l'avenir.

Dans leur recherche: "*Étude Internationale sur le Risque de Cyber-terrorisme*", publiée en Janvier 2019, *Suhania Bonusami* et *Geetha Robasendram* ajoutent d'autres éléments nécessaires pour lutter contre le cyber-terrorisme:

- Créer un cadre international solide et coordonné pour lutter contre le cyber-terrorisme, convenu par les gouvernements et les organismes de réglementation, afin de pouvoir échanger des renseignements et d'autres formes de coopération.
- Fournir une plus grande formation aux institutions des secteurs public et privé pour développer les technologies en usage vulnérables au cyber-terrorisme, et faire en sorte que la sécurité soit au premier plan lors de l'élaboration de nouveaux systèmes, afin de réduire les vulnérabilités auxquelles ils peuvent être confrontés.
- Développer une technologie sécurisée capable d'identifier les activités suspectes en analysant les données publiques et privées et en rendant les ordinateurs et leurs systèmes moins vulnérables.

Défis houleux

Les menaces de cyber-terrorisme augmentent avec la croissance constante et régulière et le développement rapide des technologies informatiques, et ce en dépit des mesures sécuritaires draconiennes prises par les gouvernements pour contrer ces menaces, dont la surveillance via Internet. Toutefois, de nombreux obstacles compliquent ces mesures, notamment le fait que la plupart des entreprises et des applications utilisent le cryptage pour protéger la confidentialité de leurs utilisateurs, ce qui permet aux terroristes de naviguer sans coup férir sur les plates-formes et les applications qui offrent à leurs utilisateurs le plus haut degré de protection et de cryptage.

Les rapports sont quasi-unanimes sur l'augmentation du nombre d'utilisateurs sur le *Dark* et le *Deep Web* (*The Onion Router*) par rapport aux autres navigateurs en raison de problèmes de confidentialité et de préférences pour les identités anonymes, ce qui augmente le risque de cyber-terrorisme. L'inquiétude grandit parmi les internautes et avec elle la pression des organisations de la société civile face aux législations strictes édictées par les gouvernements pour lutter contre le terrorisme sur le réseau, sous prétexte de protéger la vie privée et la liberté de circulation de l'information. Lorsque la ministre britannique de l'Intérieur, *Amber Rudd*, a exprimé son intention de modifier la loi pour augmenter la peine de prison de 10 à 15 ans pour les personnes qui regardent constamment les contenus terroristes sur Internet, elle a rencontré de grandes objections.

Compte tenu du nombre croissant d'Internautes dans le monde qui ont atteint plus de 4,5 milliards d'utilisateurs, du manque de sensibilisation à la sécurité et de la dépendance croissante à l'égard des communications en ligne pour fournir les services, les difficultés de lutte contre les menaces du cyber-terrorisme augmentent et l'impératif de faire face à ces menaces s'impose en même temps.

Certes, les secteurs gouvernementaux du monde entier ont édicté des réglementations, des programmes, des politiques, des lois et diverses autres mesures strictes, afin de lutter contre ces menaces, mais cette bataille ardue nécessite une mise à jour et un suivi constants, en particulier à cause de la croissance des menaces, et ses effets négatifs sur les gouvernements, les entreprises et les particuliers concernant leurs activités, leurs informations, leur confidentialité et leur sécurité.