Corona et la Propagation des Cyberattaques Terroristes

Dr. Sonny Zulhuda

Professeur adjoint à la Faculté de Droit Ahmed Ibrahim, Université Islamique Internationale de Malaisie

Depuis que l'Organisation Mondiale de la Santé a annoncé en mars 2020 que le nouveau Coronavirus «Covid» 19 était devenu une pandémie mondiale, la vigilance face à la propagation de la maladie et les inquiétudes quant à son endiguement se sont accrues. Beaucoup ont par ailleurs, adopté les réseaux électroniques pour obtenir plus d'informations sur la pandémie, d'autres ont été occupés à partager des messages sur les réseaux sociaux. Les activités électroniques ont acquis de nouvelles habitudes, comme la tenue de réunions via Internet, l'apprentissage à distance, le partage de clips vidéo... notamment lors de la phase de quarantaine imposée par de nombreux pays.

La Cybersécurité

La peur et l'anxiété sociale liées à la pandémie se sont aggravées, de sorte que des centaines de millions de personnes ont été forcées de travailler ou d'étudier à domicile... La panique des mesures strictes de quarantaine a provoqué l'émergence de comportements dangereux et illogiques, ce qui vaut également pour la sécurité du cyberespace, devenu un espace tentant pour les pirates et les cyberterroristes de faire des ravages sur Terre.

Ceci est soutenu par des nouvelles et des rapports confirmant l'émergence, pendant la pandémie, de nombreuses pratiques abusives et cyberattaques dans le cyberespace. L'Organisation Mondiale de la Santé a, en outre, indiqué - à cet égard - en avril dernier, que le nombre de cyberattaques visant des organismes internationaux a été multiplié par cinq. Le pourcentage de cybermenaces en Malaisie, a quant à lui, dépassé 80% et le nombre de cyberattaques en Indonésie a atteint entre janvier et avril 2020, 88 millions d'attaques. L'Inde a de son côté, signalé une augmentation au cours de cette période, du nombre d'attaques de cybersécurité soutenues par les États qui ciblent des agences gouvernementales. Tout cela confirme que la crise Corona est une cause majeure de la propagation des cyberattaques.

Découvrir les vulnérabilités

L'augmentation significative des cyberattaques qui affectent aussi bien les organisations que les individus peut être considérée comme un avertissement de danger pour les agents de lutte contre le terrorisme, car cette augmentation révèle des faiblesses dans l'infrastructure de l'information liée aux affaires publiques ou privées de l'État (comme Internet et les mégadonnées) que les organisations terroristes exploitent pour lancer leurs cyberattaques. Le Dr. Alex Schmid du Centre International de Lutte Contre le Terrorisme (ICCT) à La Haye, affirme que la croissance des organisations terroristes, à l'heure actuelle, est due à de nombreux facteurs, y compris les effets résultant de la mondialisation, tels que la libéralisation des marchés financiers, des services bancaires externes et électroniques et l'exploitation d'Internet à des fins offensives.

La persistance des organisations terroristes et des groupes cybercriminels à exploiter les failles ou les faiblesses des systèmes de gouvernance a incité le gouvernement américain à déclarer qu'il ne permettra pas à ces groupes criminels d'exploiter la pandémie pour menacer la vie des Américains. Il est certain que ces terroristes sont désireux de profiter des pressions résultant de la pandémie sur les épaules des institutions étatiques, en vue d'exploiter les lacunes de sécurité émergentes dans l'infrastructure du cyberespace et de réaliser leurs intérêts et leurs objectifs de sabotage et de terrorisme.

Exploiter le cyberespace

L'exploitation par les terroristes à travers divers moyens, du cyberespace des réseaux Internet, a enregistré, pendant la pandémie du Coronavirus, une augmentation apparente, en raison de la disponibilité de facteurs qui facilitent cette exploitation, dont les plus importants sont:

Premièrement: Les gens ont soif d'informations, beaucoup d'entre eux souhaitant obtenir plus d'informations sur la pandémie.

Le comportement des individus face à Internet change pendant les pandémies: Par conséquent, à mesure qu'ils sont plus désireux d'obtenir et de publier des informations et sont plus susceptibles de cliquer sur des liens ou des ressources sur le Web.

Les cybercriminels et les terroristes s'adaptent en fait, rapidement, à ce comportement d'urgence et saisissent toutes les opportunités pour propager des logiciels malveillants, en exploitant des liens non autorisés, de faux e-mails ou des messages

trompeurs.

Deuxièmement: Le travail à distance (à domicile) permet aux cybercriminels d'exploiter des systèmes informatiques non protégés.

Les nouvelles lois de distanciation sociale, les interdictions et l'auto-isolement ont forcé des millions de personnes à travailler et à étudier depuis leur domicile, en utilisant des ordinateurs moins sécurisés, dans un environnement techniquement peu favorable, comparé aux installations de travail idéales disponibles et au soutien technique qui était fourni avant la pandémie.

Troisièmement: L'utilisation d'applications externes pendant la quarantaine, en particulier des applications sans licence.

L'utilisation excessive de plates-formes électroniques externes, telles que les sites de réseautage social, les plates-formes de réunion électroniques et les services cloud qui ne sont pas correctement protégés, ou qui échappent au contrôle du propriétaire de l'entreprise, est confrontée à des risques de sécurité sensibles, abondants, et entraîne de nombreux autres problèmes de sécurité.

Pandémie Corona et terrorisme

L'une des questions urgentes à cet égard est la suivante: La pandémie du Coronavirus permet-elle la propagation d'attaques terroristes? Pour répondre à cette question, plusieurs éléments doivent être pris en compte:

1. Les terroristes sont toujours désireux d'exploiter les vulnérabilités du cyberespace. Les nouvelles habitudes qui ont émergé pendant la période de quarantaine ont conduit de nombreuses personnes à se rendre dans le cyberespace. Il est ainsi devenu facile, en raison de la forte augmentation de la dépendance à Internet, de dissimuler l'identité de terroristes ou du moins certaines activités terroristes dans le cyberespace.

2. Rien n'indique une baisse des activités de cyberterrorisme pendant la pandémie; plusieurs rapports indiquent au contraire, que les terroristes ont commencé à utiliser toutes leurs capacités pour tirer le meilleur parti de cette crise épidémique. Le chef des forces de maintien de la paix des Nations Unies a déclaré début juin 2020, dans ce contexte, que la pandémie du Coronavirus pose de nombreux défis sécuritaires complexes dans la région du Sahel et en Afrique, étant donné que les groupes terroristes font tout ce qui est en leur pouvoir pour profiter de la pandémie

et lancer des attaques contre les forces nationales et internationales. Plusieurs sources indiquent d'ailleurs, que les terroristes profitent des difficultés imposées par la pandémie pour saper les pouvoirs de l'État et déstabiliser les gouvernements.

3. De nombreuses cyberattaques ciblent l'infrastructure d'information critique (services vitaux ou services de base), qui sont une source essentielle pour le maintien des fonctions sociales essentielles, ou visent les secteurs de la santé, de l'économie ou du bien-être social; considérant que la perturbation de cette infrastructure entraîne des dommages importants, en raison de l'incapacité de protéger ces fonctions et de les maintenir.

Exemples de réalité

Un exemple de ces attaques visant des infrastructures d'information critiques est, ce qui s'est passé en République tchèque, lorsqu'un groupe terroriste a lancé une attaque électronique contre le système informatique d'un hôpital universitaire de la ville de Brno, et a provoqué la suspension de l'un des plus grands laboratoires de dépistage du virus Corona, dans la république. Le programme de rançongiciel qui ciblait le système d'information de l'administration de la santé publique de la ville de Champaign, dans l'Illinois, aux États-Unis, a de son côté, menacé de perturber le système de santé publique utilisé par le service d'information sur la pandémie de Corona.

À Taïwan, la société énergétique publique aurait pour sa part, été attaquée par le ransomware. La société japonaise de télécommunications a pour sa part, déclaré que certains criminels avaient pénétré son réseau interne et volé les données de quelque 621 clients. Certaines sources ont également averti que les infrastructures essentielles de l'Allemagne seraient menacées par la piraterie russe. En Indonésie, une réunion en ligne de haut niveau du Conseil National des Technologies de l'Information a été sabotée par un pirate informatique qui a pu accéder à des fichiers inappropriés et offensants pour le compte d'autres participants. Cet incident a causé beaucoup d'embarras, fait sensation parmi les participants et exposé les informations sensibles discutées lors de la réunion, au risque de fuite.

Tous ces incidents confirment que les cyberattaques ciblent étroitement les infrastructures d'information critiques pendant les pandémies, ce qui pourrait constituer une première étape dans le lancement de nouvelles attaques terroristes.

Gouvernance de l'information

Les facteurs de risque les plus importants résultant de l'épidémie du nouveau Coronavirus ont créé de nombreuses vulnérabilités qui offrent un environnement attrayant pour les attaques terroristes. Dans son analyse, Schmid affirme - à cet égard - que les organisations terroristes doivent financer leurs attaques à partir de diverses sources, et que le surpeuplement dans le cyberespace serait une excellente source de financement et une fenêtre d'opportunité pour le vol de données, l'extorsion, la mise en place les stratagèmes de fraude électronique et la violation des installations bancaires via Internet.

Les terroristes exploitent, en outre, Internet pour promouvoir leurs objectifs intellectuels et politiques, attirer des sympathisants, gagner leur cœur et promouvoir leurs propres objectifs. Par conséquent, ils souhaitent étendre leurs réseaux via Internet, en raison des avantages qui contribuent à la réalisation de leurs intérêts, objectif que la diffusion des médias peut servir.

Le lancement de cyberattaques sur des infrastructures critiques confirme l'insistance de ces groupes à nuire à leurs cibles et à poursuivre leurs actes terroristes, qui pourraient se transformer en une menace cybernétique dangereuse.

La nouvelle pandémie du Coronavirus a intensifié les difficultés à éviter les menaces terroristes de la part des individus et des gouvernements, ce qui confirme la nécessité urgente de développer un cadre complet pour la gouvernance de l'information et de déployer des efforts continus pour assurer la sûreté, la sécurité et la durabilité du cyberespace. Les conséquences dévastatrices de la pandémie du Coronavirus ont exacerbé ces menaces insolubles, qui obligent les responsables de l'infrastructure d'information critique ou ceux des services nécessaires, ainsi que les agences gouvernementales et les organisations privées, à renforcer leurs mesures de sécurité et préventives, leurs dispositions de protection et d'intervention, afin d'éviter et de réduire les menaces terroristes. Cela devrait reposer sur une base solide pour la gouvernance de l'information et être compatible avec les aspects juridiques et techniques.