Cyberterrorisme:
Risque de menace et moyens de contrôle

Sonny Zulhuda

Chercheur indonésien et professeur agrégé, Faculté de la Loi Ahmed Ibrahim Université islamique internationale de Malaisie.

Avec les grands progrès technologiques dans le domaine de l'information et de la communication via Internet, il est devenu très aisé pour les criminels et les terroristes de recourir à ces technologies avancées dans l'élaboration, la mise en œuvre et la promotion de leurs plans criminels et terroristes, au point que ces technologies modernes semblent constituer une menace sérieuse qui pèse sur l'ensemble de la communauté internationale.

Dr. Nah Liang Tuang, Professeur d'Études Internationales au Rajaratnam College de Singapour, estime que cette avancée technique est une arme à double tranchant. Alors que le premier tranchant peut être utilisé comme ligne de défense face au crime et au terrorisme, l'autre tranchant sert à commettre le crime et le terrorisme. Les technologies avancées telles que le cryptage des téléphones intelligents, l'Internet des objets, la propagation des réseaux informatiques dans tous les secteurs vitaux, en particulier sécuritaires et militaires, et dans les services publics vitaux, offrent de nombreux avantages pratiques, mais ouvrent en même temps, la porte aux cyber-menaces dangereuses et engendrent des cyber vulnérabilités.

Cet article vise à analyser la nature du cyberterrorisme, expliquer sa portée, mettre en évidence les derniers développements relatifs à l'initiative internationale pour la promulgation de mesures juridiques contre cette menace mondiale, et focaliser sur la Convention sur la cybercriminalité.

La menace du cyberterrorisme

Le rapport, sur les risques mondiaux 2019 du Forum Économique Mondial, affirme que le cyberterrorisme est devenu une réalité inévitable. Le rapport décrit les cyber-attaques ou les logiciels malveillants comme autant d'agents qui causent de grands dommages économiques, des perturbations géopolitiques ou créent des situations dans lesquelles la confiance dans l'Internet est largement rompue. Les attaques terroristes à grande échelle sont menées par des individus ou des groupes non gouvernementaux

ayant des objectifs politiques, religieux ou sociaux visant à causer des dommages humains ou matériels généralisés.

Le rapport du Forum Économique Mondial a également révélé les graves dangers des cyber-attaques terroristes, étroitement liés à l'effondrement de l'infrastructure d'information et au risque de recourir à des armes de destruction massive, d'autant plus que nous vivons aujourd'hui dans un monde largement interdépendant et interconnecté, dans lequel les infrastructures de données vitales sont de plus en plus numérisées, et donc la dépendance à leur égard augmente régulièrement. Le cyberterrorisme est devenu dans ce contexte de plus en plus populaire en raison de son utilisation aisée et de son prix abordable. Il ne nécessite pas des terroristes d'obtenir des armes classiques coûteuses, ni à les transférer à l'endroit souhaité, de même que les contraintes temporelles et spatiales ne dissuadent pas les terroristes de sévir, car ils peuvent lancer des attaques dans cette réalité virtuelle de n'importe où, et n'importe quand, tout en étant capable de s'éclipser derrière l'écran de la technologie.

Ainsi, l'impact peut être énorme et effrayant, selon l'objectif à atteindre. L'action subversive use de nombreux moyens dont des programmes malveillants, des virus informatiques, des attaques par de déni de service, des logiciels d'es pionnage sur le réseau, ...etc.

Portée du cyberterrorisme

Mais la question qui se pose ici est la suivante: Qu'est-ce que le cyberterrorisme? Fornell et Warren définissent le cyberterrorisme comme étant l'utilisation par des groupes de cyber-terroristes du cyberespace. Cela suppose une transition du terrorisme conventionnel qui repose sur des moyens matériels (armes, munitions, ...etc.), vers le terrorisme moderne, qui repose davantage sur des technologies invisibles. James Lewis définit le cyberterrorisme comme: L'utilisation d'outils de réseau informatique pour détruire ou perturber d'importantes infrastructures nationales telles que l'énergie, les transports et les opérations gouvernementales, dans le but de contraindre ou d'intimider le gouvernement ou les civils.

À partir de cette définition, on peut décrire le cyberterrorisme en examinant deux aspects:

Premier Volet: L'importance de la composante «Cyber-menace», sorte d'attaque visant à détruire ou à perturber le cyber-environnement (systèmes informatiques), ce qui fait craindre la propagation de plans et d'idées terroristes, ou des attaques contre les systèmes militaires et l'infrastructure vitale numériques du pays, comme le montre la figure 1:

Figure 1: Portée du cyberterrorisme, premier volet (attaquer le système)

Deuxième volet: L'importance de l'élément "lieu de préparation", qui est le lieu d'où le cyber système est piraté, lorsque des terroristes utilisent l'Internet ou les systèmes d'information et de communication tels l'Internet des objets, les appareils mobiles, l'intelligence artificielle, les mégadonnées, le cryptage et les logiciels automatisés, aux fins de planifier, préparer et lancer des attaques terroristes efficaces. Dans ce contexte, Peter Grabowski décrit l'utilisation extensive des technologies de l'information comme moyen au service du terrorisme, dont le piratage de renseignements, l'extraction de données, la collecte de fonds, le recrutement, la mobilisation et la formation à distance qui comprend entre autres les technologies et les compétences de piratage, le partage d'informations, la diffusion des manuels pour la fabrication d'armes, ...etc., comme le montre la figure 2:

Figure (2): Types de cyberterrorisme, deuxième volet

Le deuxième volet des activités de cyberterrorisme a pris de l'importance en Malaisie au cours de la dernière décennie, et des poursuites ont été engagées en vertu du code pénal du pays. Les dispositions sont classées sous les n° (C-130) et (Y-130), de divers actes commis dans le cadre d'actes terroristes, par exemple: Le recrutement de personnes pour rejoindre des groupes terroristes, ou pour participer, promouvoir ou inciter à des actes terroristes, fournir de la formation et de l'éducation aux groupes

terroristes, recevoir de la formation de la part de ces groupes, diriger leurs activités nuisibles et pernicieuses et rechercher le soutien des groupes terroristes.

Initiative de lutte contre sur le cyberterrorisme

Le cyberterrorisme est une menace mondiale et un problème international qui nécessite une solution mondiale. L'ancien Secrétaire Général des Nations Unies, Ban Ki-moon, a déclaré: «Internet est un excellent exemple du comportement transfrontalier des terroristes». Les États doivent donc réfléchir et agir ensemble au-delà des frontières nationales, malgré l'existence de lois et de politiques locales sur le cyberterrorisme. Nous devons d'urgence répondre à cette menace mondiale, d'une action commune et complémentaire au niveau international. Par conséquent, des initiatives internationales ont été lancées pour lutter contre la menace du cyberterrorisme. En 2012, l'Office des Nations Unies Contre la Drogue et le Crime, en coopération avec l'Équipe Spéciale des Nations Unies sur la Lutte Contre le Terrorisme, a publié un rapport de travail sur le cyberterrorisme.

Le manque de formation spécialisée sur les aspects juridiques et pratiques des enquêtes et des poursuites relatives aux affaires de terrorisme impliquant l'utilisation d'Internet est préoccupant. Par conséquent, l'Office des Nations Unies Contre la Drogue et le Crime vise à développer des ressources liées à la lutte contre le terrorisme et la cybercriminalité pour lutter contre cette menace en évolution. Le Bureau souligne qu'il existe certains facteurs fondamentaux et nécessaires pour déterminer la réponse internationale aux mesures antiterroristes, notamment:

1) Cadres politiques et législatifs communs.
2) Enquêtes et collecte de renseignements.
3) Coopération et solidarité internationales.
4) Enquêtes et poursuites judiciaires.
5) Coopération du secteur privé avec les agences gouvernementales.

Tous ces facteurs fondamentaux dépendent de l'engagement inter-pays pour combattre les menaces terroristes à l'intérieur de leurs frontières nationales et au-delà de ces frontières.

Convention sur la Cybercriminalité

C'est l'une des conventions mondiales parmi les plus importantes, étant la seule convention internationale sur le cyberterrorisme. Nous constatons que bien que cette convention ne traite pas spécifiquement du cyberterrorisme, elle a été rédigée de manière à pouvoir suivre l'ampleur des menaces terroristes, dont le crime de cyberterrorisme.

La meilleure réponse pour faire face à la menace du cyberterrorisme est de modifier la Convention et d'y inclure les délits de cyberterrorisme de manière plus précise. De même, le plus grand défi est d'impliquer davantage de pays pour en faire un outil mondial et international de lutte contre ce type de criminalité.

En 2016, le Comité de la Convention sur la Cybercriminalité a publié une note d'orientation sur les aspects du cyberterrorisme en vertu de l'accord de Budapest, déclarant que «les infractions citées dans la Convention peuvent également être des actes terroristes au sens de la loi en vigueur». Cette note supplémentaire au titre de l'accord arrive en temps opportun, et souligne que cette convention n'est pas un traité spécifique au terrorisme, mais on peut dire que: Les infractions dans la Convention peuvent être considérées comme des actes terroristes, facilitant ou soutenant le terrorisme, du point de vue du financement, ou des travaux préparatoires.

En outre, les outils internationaux d'assistance judiciaire procédurale contenus dans la Convention sont disponibles pour les enquêtes et les poursuites terroristes. En vertu de l'accord, chaque partie s'appuie sur des mesures législatives et autres qui peuvent être nécessaires pour définir des pouvoirs et des procédures aux fins de mener des enquêtes ou des procédures pénales spécifiques, sachant que ces pouvoirs et procédures ne s'appliquent pas seulement à la cybercriminalité spécifique, comme indiqué dans l'accord, mais également aux criminalité et autres cyber-violations commises via des systèmes informatiques. Par conséquent, selon la note d'orientation de 2016, cela pourrait conduire à une application plus large de la Convention sur la cybercriminalité à tout crime terroriste, tant qu'il est commis par le biais de systèmes informatiques.

Grâce à cette extension, le fait de faire partie de l'accord serait une source importante de soutien et d'assistance à l'État pour lutter contre le cyberterrorisme dans sa juridiction, indiquant que le pays en question serait éligible au soutien mutuel, à l'assistance et à la coopération entre les États Membres. Ainsi, les parties (de la Convention) doivent s'entraider, aussi largement que possible, pour mener les enquêtes sur les délits liés aux cyber-violations et aux violations liées aux systèmes informatiques et de données, ou pour collecter électroniquement les preuves d'un délit. Cela signifie, également, que la partie à l'accord obtiendra sa juste part de la coopération internationale et qu'elle sera autorisée à obtenir une assistance mutuelle même en l'absence des accords internationaux en vigueur entre les pays.

Enfin

Nous concluons que le cyberterrorisme est une nouvelle forme d'acte terroriste qui a souvent un impact significatif, mais les politiques et la législation de nombreuses autorités judiciaires se distancient encore de ce type de terrorisme, en dépit de son importance, son impact et son danger.

Le cyberterrorisme est une menace mondiale qui nécessite une réponse internationale et une coopération mondiale, ainsi que le besoin urgent d'une politique commune et d'un cadre législatif commun, qui établissent des normes minimales et les meilleures pratiques pour y faire face. Un effort concerté est nécessaire pour collecter et échanger les renseignements. La coopération internationale dans les enquêtes et les poursuites, ainsi que la coopération entre les secteurs public et privé est extrêmement importante.