Astuces et méthodes malveillantes

Tentatives d'acquisition d'armes non classiques par les mouvements terroristes

Dr. Ihab Khalifa

Chercheur et écrivain spécialisé dans les technologies et les questions liées à l'extrémisme, Égypte

L'idée que les groupes terroristes devraient acquérir des armes non classiques, telles que des armes nucléaires, chimiques ou biologiques, demeurait longtemps peu probable en raison de la difficulté, en particulier des armes nucléaires, due aux mesures de sécurité strictes appliquées par les États dans la production, le transport et la circulation des matières nucléaires. Même si nous supposons que des groupes terroristes ont obtenu une arme nucléaire par vol ou de toute autre manière, le transfert et l'utilisation de ces armes dans des opérations terroristes exigent de nombreuses procédures spéciales sur le terrain que les groupes terroristes ne peuvent pas faire comme par l'obtention de missiles balistiques ou d'avions géants.

Mais cela n'a pas empêché des groupes terroristes de faire tout de même des tentatives, comme celle de Bruxelles en 2016 qui visait l'explosion d'un réacteur nucléaire ou de voler des matières nucléaires.

Bombardement de drones

En septembre 2022, Abu Muhammad al-Masri, l'un des dirigeants d'al-Qaïda, a publié un livre intitulé « Opérations du 11 septembre entre vérité et doutes », dans lequel il a parlé des tentatives de groupes terroristes de mener une explosion nucléaire en dirigeant un drone chargé de milliers de conteneurs de carburant hautement inflammables, vers l'un des réacteurs nucléaires en Amérique.

Si nous examinons de près le grand développement observé par les cyberarmes au cours de la dernière décennie et ce qu'elles ont provoqué en pénétrant dans les installations nucléaires, ou en falsifiant les systèmes de sécurité à l'intérieur des réacteurs, comme cela s'est produit à l'installation iranienne de Natanz en 2009, notre inquiétude au sujet des groupes terroristes lançant des cyberattaques ciblant les réacteurs nucléaires augmente.

Dans le même livre, Abu Muhammad al-Masri a énuméré des idées non

conventionnelles pour mener à bien une explosion nucléaire, telles que compter sur des membres des communautés musulmanes et des minorités travaillant dans des installations nucléaires, et utiliser leur haine envers les États-Unis d'Amérique en raison de leurs politiques de discrimination raciale, pour les recruter afin de mener des attaques à l'intérieur de ces installations, ou pour effectuer des sabotages qui conduisent à des fuites radioactives et rendent certaines zones impropres à la vie humaine.

À cet égard, l'auteur déclare : Compte tenu de l'énorme stock d'armes nucléaires à l'intérieur du territoire américain, ce qui est une faiblesse majeure si des groupes militants peuvent y accéder, et en tester une partie sur le sol américain, de sorte que cela rend l'Amérique invivable. Ce n'est pas difficile à réaliser, mais il faut réfléchir à la manière d'accéder à ce stock stratégique. »

Ceci est au niveau des idées théoriques auxquelles s'ajoutent les tentatives pratiques de sabotage nucléaire par des groupes extrémistes, comme par exemple : les attentats de Bruxelles perpétrés par Daech en mars 2016, qui ont révélé que les auteurs de l'opération prévoyaient de provoquer une attaque nucléaire en faisant sauter une centrale nucléaire, en tuant le gardien de l'une des installations et en obtenant sa carte d'accès afin de procéder à une explosion à l'intérieur de l'installation.

Cyberattaques nucléaires

L'un des dangers des cyberarmes ou des virus informatiques est leur capacité à cibler les installations nucléaires. Bien que la cybersécurité nucléaire de l'installation soit l'élément le plus important de la sûreté et de la sécurité, une étude publiée en 2016 dans le cadre de la « Nuclear Threat Initiative » a montré que la moitié des pays dotés d'installations nucléaires dans le monde n'ont pas de législation ou de procédures de cybersécurité pour préserver les installations des cyberattaques

Si un groupe terroriste parvient à posséder l'un de ces virus, à l'acheter via le Dark Web, à le divulguer auprès de certains gouvernements ou à l'obtenir en recrutant des pirates professionnels, les groupes terroristes peuvent provoquer une menace nucléaire réelle, qui ne constituera en aucun cas une explosion nucléaire en raison des mesures de sûreté et de sécurité à l'intérieur de ces installations, mais peut entraîner des dommages aux appareils et aux systèmes, ainsi que des fuites radioactives.

Le « ver Stuxnet » est le premier modèle d'utilisation d'une cyberarme pour cibler un réacteur nucléaire, et il a été utilisé pour cibler le programme nucléaire iranien en 2009, et a été considéré comme l'un des types de cyberarmes les plus dangereux. Dès lors, le risque de cyberattaques qui menacent les installations nucléaires a augmenté.

En décembre 2014, la South Korean Hydro and Nuclear Power Company a annoncé que ses systèmes informatiques avaient été piratés en cyber, mais que seules des données insignifiantes en avaient été extraites. Les autorités ont trouvé des preuves indiquant la suppression d'un ver électronique à faible risque des appareils connectés à certains systèmes de contrôle d'une centrale nucléaire, et ont accusé la Corée du Nord d'être impliquée dans l'attaque. Cependant, le virus n'a pas affecté le réacteur car les processus industriels sont déconnectés d'Internet.

Les modèles précédents soulignent le besoin urgent de reconsidérer les procédures de cybersécurité dans les installations nucléaires, et si cela ne se produit pas, elles deviendront vulnérables aux menaces. Si un groupe terroriste a une organisation et un leadership forts déterminés à atteindre les objectifs, il peut provoquer le sabotage de certaines installations nucléaires qui conduit à une fuite radiologique dangereuse.

Composés chimiques et biologiques

Les armes chimiques et biologiques sont moins nocives que les armes nucléaires, mais leur utilisation peut entraîner des pertes importantes en vies humaines parce qu'elles sont faciles à transporter et infectent un très grand nombre d'individus, telles que : la libération d'un virus dans une rivière ou la libération de composés chimiques et de gaz mortels sur l'une des places principales, ou dans les bus et les trains. Par conséquent, les armes chimiques et biologiques sont devenues une alternative aux armes nucléaires pour les mouvements terroristes, car elles sont faciles à obtenir ou à installer, à transporter et à déployer. L'Organisation pour l'Interdiction des Armes Chimiques a surveillé l'utilisation de l'agent moutarde dans une attaque lancée par l'organisation terroriste Daech en 2015 dans le nord de la Syrie, qui a fait au moins 20 blessés. La ville de Marea, située près de la frontière turque dans la province d'Alep, qui est alors sous le contrôle de l'opposition, a été bombardée avec des munitions remplies de produits chimiques soupçonnés d'être du soufre moutarde. La police criminelle allemande a arrêté deux extrémistes appartenant à Daech, qui prévoyaient de lancer un attentat à la bombe biologique dans le pays en juin 2018. Le rapport d'accusation préparé par le parquet antiterroriste indiquait qu'ils avaient décidé à l'automne 2017 de lancer une attaque

en Allemagne et de faire exploser un engin explosif dans une grande foule de personnes, pour tuer et blesser autant de personnes que possible.

En conclusion, nous affirmons que la révolution technique moderne et ses moyens intelligents ont contribué à modifier les sources d'énergie et les méthodes d'emploi, de sorte que l'information, qui est le principal élément du pouvoir, est devenue disponible sur les sites Internet, y compris des informations sur les installations vitales susceptibles de devenir la cible d'un attentat terroriste tels que: les installations nucléaires, les centrales électriques, les aéroports et les laboratoires de recherche, ainsi que des informations sur la fabrication d'engins explosifs, l'achat de matières explosives ou d'armes conventionnelles, ou la préparation de virus informatiques pour lancer des cyberattaques, ciblant les centrales nucléaires, les biocarburants et les infrastructures importantes des pays. Ce changement significatif dans les sources de pouvoir a permis aux mouvements terroristes extrémistes d'atteindre des objectifs qui leur étaient impossibles dans un passé récent, et ce développement technologique, tout comme il a aidé les mouvements terroristes à modifier leurs plans militaires au cours des dernières années, pourrait les aider encore plus dans les années à venir, s'ils ne tarissent pas leurs sources et ne combattent pas leurs outils.