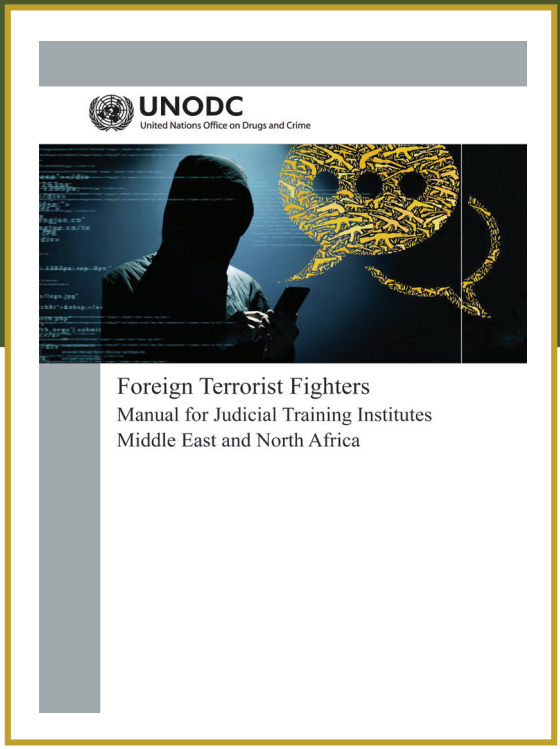
Numéro
35

التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

RAPPORTS
INTERNATIONAUX



Les combattants terroristes étrangers

Manuel des instituts de formation judiciaire au Moyen-Orient et en Afrique du Nord

Mars
2022

Rapports Internationaux

Une publication mensuelle de la Coalition Islamique Militaire pour Combattre le Terrorisme

---

Superviseur général

Le Général-Major Mohammed bin Saïd Al-Mughaidi

Secrétaire Général désigné de la Coalition Islamique Militaire pour Combattre le Terrorisme

---

Rédacteur en chef

Ashour Ibrahim Aljuhani

Directeur du Département des Études et des Recherches

Rapports Internationaux
35
Mars 2022

LES COMBATTANTS TERRORISTES ÉTRANGERS

MANUEL DES INSTITUTS DE FORMATION JUDICIAIRE AU MOYEN-ORIENT ET EN AFRIQUE DU NORD

L'organisation terroriste Daech (État Islamique) a attiré l'attention sur le danger du phénomène des combattants terroristes étrangers (CTE) qui a précédé son émergence, mais l'organisation terroriste en a fait une menace pour la paix et la sécurité internationales. Au plus fort de l'essor de l'organisation en Irak et en Syrie, vers 2015, près de 40.000 personnes de plus de 120 pays se sont rendues dans les deux pays pour rejoindre les rangs de Daech.

La base de données d'INTERPOL sur l'EI comprend 53.000 noms, collectés sur les champs de bataille en Irak et en Syrie. Selon les estimations de la Coalition mondiale anti-Daech, il y avait moins d'un millier de terroristes de l'organisation dans le champ d'opérations de la Coalition fin 2017. Si le soi-disant État de Daech a disparu, or ce n'est pas le cas pour l'organisation toujours active dans nombre de pays, tels que le Yémen, Egypte, Libye, région du Sahel en Afrique et ailleurs.

Menaces et dangers

Les recherches indiquent que quelque 14.900 CTE ont quitté l'Irak et la Syrie, dont certains se sont échappés déguisés, sans chercher à retourner dans leurs pays d'origine craignant d'être traduits en justice, de perdre leur nationalité ou d'être soumis à d'autres sanctions. Ils ont cherché des sanctuaires dans d'autres pays et constitué des renforts aux groupes terroristes locaux.

Mais comment les pays du Moyen-Orient et d'Afrique du Nord font-ils face à ce danger imminent ? Ce rapport, émis par l'Office des Nations Unies contre la drogue et le crime, fournit aux pays de la région un manuel dédié aux instituts de formation judiciaire pour une gestion optimale des CTE de retour. Le rapport a analysé le phénomène, le cadre juridique permettant de lui faire face aux niveaux régional et international et présenté les meilleures pratiques pour mener à bien les enquêtes en ligne sur les crimes des CTE.

L'une des principales menaces auxquelles sont confrontées les juridictions du Moyen-Orient et d'Afrique du Nord est le retour des CTE dans leur pays d'origine. Certaines études estiment qu'environ 15.000 personnes originaires des pays de la région se sont rendues en Irak et en Syrie entre fin 2012 et 2017, le nombre de femmes et d'enfants atteignant environ 35 %.

Lorsque l'EI a perdu le contrôle des terres qu'il avait saisies en Syrie et en Irak, des avertissements ont été émis selon lesquels les pays d'origine des CTE devraient se préparer à un afflux de rapatriés, mais le nombre de CTE rapatriés, bien qu'inquiétant, était beaucoup plus faible que prévu. On estime que 30 % des CTE sont rentrés chez eux ou ont déménagé dans un pays tiers. En novembre 2017, une équipe des Nations Unies estimait, selon les statistiques de 79 pays, qu'environ 7000 combattants étrangers étaient morts sur les champs de bataille, tandis que 14.900 autres avaient quitté les zones de conflit, dont 5395 sont actuellement emprisonnés, soit seulement 36 %. Parmi eux, 6837 combattants, soit 46 %, ne sont pas soumis au système de justice pénale.

Les CTE constituent sans aucun doute une menace exceptionnelle pour la région en raison de leur expérience au combat et de la formation qu'ils ont reçue au maniement des armes et des explosifs. Plus important encore, le sort de beaucoup d'entre eux est encore inconnu, car il existe un grand écart entre le nombre total de ces personnes et le nombre de ceux qui ont été comptés parmi les morts, détenus, renvoyés ou transférés.

Pourquoi reviennent-ils ?

Les motivations des CTE à revenir chez eux varient, certains étaient déçus face aux idéologies de l'extrémisme violent ou à la vie dans les territoires contrôlés par des organisations terroristes. D'autres voulaient rejoindre leurs familles ou améliorer leurs conditions sociales et économiques, ou bien pour commettre des attentats et promouvoir le du terrorisme dans leurs pays. Il y a une mise en garde sur la nécessité de faire la distinction entre les CTE qui se sont rendus en Irak et en Syrie à des fins terroristes, et ceux qui sont allés pour d'autres fins. De nombreux rapatriés ont quitté la Syrie avant que Daech ne déclare son prétendu califat en 2014, et la plupart de ces rapatriés (de la première vague) avaient d'autres motifs différents de se rendre à l'étranger, comme de s'opposer au régime syrien injuste ou fournir une aide humanitaire au peuple syrien opprimé.

Dans tous les cas, il n'est pas facile de prévoir la réaction des CTE rapatriés au fil du temps même s'ils subissent une évaluation psychologique et sécuritaire solide, car les circonstances peuvent les pousser à nouveau à rechercher des solutions violentes à leurs problèmes, surtout s'ils rechutent dans les mêmes conditions antérieures.

Le discours politique concernant les CTE rapatriés s'est concentré sur les risques sécuritaires qu'ils représentent. Dans de nombreux cas, l'EI a appelé les rapatriés à attaquer des cibles dans leur pays d'origine pour redorer le blason de l'organisation terroriste. On pense que les CTE rapatriés constituent un important risque pour plusieurs raisons, notamment : ils peuvent utiliser le réseau de relations qu'ils ont établi avec d'autres terroristes alors qu'ils étaient actifs à l'étranger, pour lancer des attaques à grande échelle. De même, ils constituent autant d'agents potentiels de l'EI à l'étranger.

L'examen empirique semble confirmer ces craintes, car l'un des indicateurs bien connus des opérations terroristes menées dans les pays du Moyen-Orient et d'Afrique du Nord est l'existence de contacts réels entre l'EI et les exécutants. Une étude menée sur environ 510 attaques lancées par Daech en dehors

de la Syrie et de l'Irak, jusqu'au 31 octobre 2017, a conclu que des CTE ont participé à plus de 25 % à ces attaques, dont 87 attaques ont été menées en dehors de leur pays d'origine.

En plus de leur participation directe à des attaques terroristes, les CTE ont contribué à la création d'un nouveau type d'action terroriste, à savoir les attaques dirigées par des (planificateurs virtuels) qui utilisent des communications sécurisées pour diriger les attaques à distance.

Cependant, la menace des CTE rapatriés pour la sécurité ne doit pas être surestimée. Selon Europol, les attaques contre l'Union Européenne ont été commises par des terroristes nationaux qui ne se sont pas rendus à l'étranger pour rejoindre des groupes terroristes. Une étude du Service de recherche du Parlement Européen a conclu que la majorité des CTE rapatriés peuvent ne pas avoir l'intention de planifier des attaques terroristes à leur retour, avec très peu de cas réels de CTE ayant l'intention de lancer des attaques en Europe.

Par conséquent, on peut dire que les CTE rapatriés ne partagent pas les mêmes caractéristiques, car ils ne se sont pas tous rendus dans les zones de conflit avec l'intention de commettre des actes terroristes. Certains rapatriés, en particulier les femmes et les jeunes enfants, peuvent ne pas avoir reçu de formation au combat violent, ou commis des crimes violents. Après leur retour, certains d'entre eux se sont complètement retirés de toute activité extrémiste. Certains rapports indiquent que la participation d'anciens CTE a joué un rôle déterminant dans les efforts visant à prévenir l'extrémisme violent. En tant que tel, il n'est pas approprié de traiter tous les CTE rapatriés comme des attaquants terroristes potentiels.

La menace d'attaques par des CTE peut être classée comme à fort impact et à faible probabilité. La recherche révèle que seulement 18% des attaques menées en Occident, entre juin 2014 et juin 2017, ont été commises par des CTE connus. Pourtant, les attaques qu'ils ont menées étaient presque parmi les plus meurtrières. Une attaque a tué environ 35 personnes.

Dans la région du Moyen-Orient et Afrique du Nord, les attaques terroristes locales soutiennent l'évaluation de l'équipe de l'ONU sur la menace des CTE dans la région comme «menace grave». Le principal défi pour les autorités de la région reste la détection et le suivi des intentions des CTE rapatriés.

Cadre juridique

Au niveau international, 19 conventions et résolutions ont été adoptées au cours des 60 dernières années pour lutter contre le terrorisme, ayant traité divers sujets tels que: la répression du financement du terrorisme, le terrorisme lié aux transports, le terrorisme nucléaire et radiologique, les prises d'otages et la répression des attentats à la bombe. Ces instruments internationaux sont complétés par les résolutions du

Conseil de sécurité des Nations Unies en matière de prévention et de lutte contre le terrorisme. Ensemble, ils créent les obligations des États membres stipulées par le droit international, devant figurer dans la législation nationale et être strictement mises en œuvre. La mise en œuvre de ces conventions et résolutions est guidée par les orientations fournies par la Politique antiterroriste mondiale des Nations Unies, ainsi que par les résolutions de l'Assemblée générale des Nations Unies.

Concernant les crimes liés aux CTE dans le contexte international et régional (Moyen-Orient et Afrique du Nord), les résolutions du Conseil de sécurité se démarquent, à savoir : la résolution 1373 de 2001, 2178 de 2014 et 2396 de 2017. La première de ces résolutions est la plus complète de ces résolutions, et les autres doivent être interprétées et comprises selon elle. Adoptée à la suite des attentats du 11 septembre 2001 contre les États-Unis, elle constitue le moteur d'une série d'instruments internationaux ciblant l'extrémisme violent et le terrorisme. La résolution 2178 a établi une définition des CTE et appelé les États membres à renforcer les moyens d'y faire face, selon trois catégories de mesures : les lois pénales, les sanctions et les mesures préventives. La résolution 2396 concerne les risques des CTE revenant des zones de conflit, contrairement à la résolution 2178 ciblant les CTE se rendant à l'étranger.

Plan global

Le 8 septembre 2006, l'Assemblée générale des Nations Unies a adopté un plan stratégique pour lutter contre le phénomène des CTE, et bien qu'il ne soit pas juridiquement contraignant pour les États membres, contrairement aux résolutions du Conseil de sécurité adoptées en vertu du chapitre VII de la Charte des Nations Unies, il est considéré comme un instrument mondial sans précédent pour renforcer les efforts nationaux et internationaux contre le terrorisme. Tous les États membres ont convenu, pour la première fois, d'adopter ce plan, selon une approche commune de la lutte contre le terrorisme, fondée sur quatre fondements principaux, à savoir :

1. S'attaquer aux conditions propices à la propagation du terrorisme.
2. Prévenir et combattre le terrorisme.
3. Renforcer les capacités des États à prévenir le terrorisme et renforcer les efforts des Nations Unies à cet égard.
4. Garantir le respect des droits de l'homme et la primauté du droit.

Le plan repose sur les approches de justice pénale et de gouvernance, qui se renforcent mutuellement. L'approche de justice pénale appelle les États membres à formuler un ensemble d'infractions pénales et à les appliquer aux pratiques d'extrémisme violent et de terrorisme, et l'approche de gouvernance sert à prévenir l'extrémisme violent en réduisant les conditions propices à ce fléau, car il est difficile de résoudre les problèmes politiques, économiques et sociaux, qui sont les causes profondes de l'extrémisme violent, avec une approche de justice pénale.

L'Assemblée générale des Nations Unies révise et met à jour son plan de lutte contre le terrorisme tous les deux ans pour répondre à l'évolution des priorités. L'Assemblée a procédé au sixième examen de cette stratégie les 26 et 27 juin 2018, et cet examen a conduit à l'adoption de la résolution de l'Assemblée n° 72/284 relative aux risques des CTE rapatriés et qui a appelé à la coopération aux niveaux international, régional et bilatéral pour contrer cette menace, notamment en améliorant l'échange rapide d'informations opérationnelles, le soutien au renseignement et le renforcement des capacités.

Directives internationales

Outre les accords internationaux, les résolutions du Conseil de sécurité, les résolutions de l'Assemblée générale des Nations Unies et le Plan stratégique des Nations Unies pour lutter contre le terrorisme, le cadre juridique pour faire face aux CTE au niveau international comprend certains instruments qui ont formulé des recommandations importantes, clarifié les meilleures pratiques et exhorté les États membres à les adopter et renforcer leur réponse à la menace des CTE.

Parmi ces instruments figurent :

Le Mémorandum de La Haye-Marrakech

Il s'agit d'une initiative lancée par le Maroc et les Pays-Bas en 2014, dans le cadre du Forum mondial de lutte contre le terrorisme. Elle vise à réunir les décideurs politiques et les praticiens d'un large éventail de pays pour échanger les leçons apprises et les meilleures pratiques afin de contrer la menace posée par les CTE.

Le mémorandum a identifié 19 meilleures pratiques incitant les gouvernements à développer leurs propres politiques pour faire face à la menace des CTE. En 2015, une annexe a été ajoutée à ce mémorandum comprenant sept recommandations relatives aux CTE rapatriés.

Principes de Malte

Il s'agit d'une initiative conjointe du Centre de recherche Hedayah et de l'Institut international pour la justice et l'état de droit. Présentée en 2016, elle comprend 22 principes pour aider les États membres à concevoir leurs politiques et programmes visant à réhabiliter les CTE rapatriés.

Directives de Madrid

Il s'agit d'une initiative résultant d'une réunion spéciale du Comité contre le terrorisme du Conseil de sécurité, accueillie par le Gouvernement espagnol à Madrid les 27 et 28 juillet 2015. La réunion a émis 35 principes directeurs dans son document final ratifié par le Conseil de sécurité en décembre de la même année.

Ces principes se déclinent en trois thèmes :

1. Détecter l'incitation et le recrutement des CTE et faciliter, contrer et confiner leurs activités.
2. Empêcher les déplacements des CTE par divers moyens dont des mesures visant à renforcer la sécurité aux frontières.
3. Les poursuivre en justice, les réhabiliter et les réintégrer et promouvoir la coopération internationale.

Suite à la défaite de Daech, l'attention du Conseil de sécurité s'est tournée vers la menace persistante posée par le retour des CTE. Dans sa résolution n° 2396 de 2017, il a demandé au Comité contre le terrorisme d'examiner les Lignes directrices de Madrid à la lumière du danger que représente le retour des CTE. Une réunion spéciale du comité le 13/12/2018, dans l'État de New York, a abouti à la rédaction d'un addendum aux Lignes directrices de Madrid de 2015, proposant 17 bonnes pratiques supplémentaires pour aider les États membres dans leurs efforts à contrer le phénomène des CTE de retour.

Cadre régional

Au Moyen-Orient et en Afrique du Nord, le cadre juridique de lutte contre le terrorisme, élaboré par la Ligue des États Arabes (LEA) et l'OCI, est lié à la question de lutte contre les CTE. La LEA a approuvé l'instrument contraignant de base dans la lutte contre le terrorisme, qui est la Convention Arabe Contre le Terrorisme, le 22 avril 1998, entrée en vigueur le 7 mai 1999. Elle a approuvé les recommandations lors du 26ème Sommet de la Ligue Arabe, qui s'est tenu en Égypte en 2015, dont la création d'une force militaire conjointe pour relever les défis posés par les groupes terroristes et les CTE de retour.

Quant à l'OCI, elle a publié un code de conduite pour les États membres dans la lutte contre le terrorisme international et l'a adopté en 1994, puis elle a adopté le Traité de l'OCI sur la lutte contre le terrorisme international en 1999 entré en vigueur le 7 novembre 2002. Ce traité présente certains avantages, notamment le fait que le deuxième article excluait du champ d'application des dispositions du traité les personnes participant à ce qu'il considère comme une lutte armée légitime pour l'autodétermination. Reconnaissant les défis qui ont entravé le traité de 1999, l'organisation a indiqué en 2016 son intention de proposer des règles supplémentaires et de mettre à jour certaines dispositions du traité afin d'améliorer les niveaux actuels de coopération.

L'enquête électronique et ses sources

La formation à l'enquête électronique et à la collecte de preuves informatiques est devenue une priorité dans l'enquête et la poursuite des CTE. Les ordinateurs, les téléphones portables et Internet font désormais partie des enquêtes modernes sur les affaires de terrorisme, étant susceptibles de contenir des preuves de crimes.

Les crimes impliquant des preuves électroniques présentent un défi unique pour les législateurs, les enquêteurs, les procureurs et les juges concernés. Une fois les suspects arrêtés, la plupart des poursuites judiciaires reposent sur l'utilisation de preuves électroniques, notamment des données de localisation, les publications sur les réseaux sociaux, les SMS, les e-mails et les enregistrements d'appels téléphoniques.

Tous les cas transfrontaliers impliquant des activités terroristes ou du blanchiment d'argent nécessitent des preuves stockées dans les serveurs des fournisseurs d'accès Internet (FAI) mais ces cas demeurent compliqués à cause des disparités entre les pays dans les cadres juridiques, les procédures internes,

les compétences et les expertises, ainsi qu'à cause des différentes pratiques entre les FAI et leur niveau de coopération lors de la réception de demandes de données de la part des autorités chargées de l'application des lois.

La capacité de mener des enquêtes électroniques devient de plus en plus incontournable dans toutes les poursuites, et comme les délais impartis aux FAI pour conserver les données sur leurs abonnés varient, les enquêteurs doivent rapidement soumettre des demandes formelles aux FAI pour conserver les données pertinentes jusqu'à la délivrance de l'ordonnance judiciaire autorisant l'extraction des documents. L'une des premières étapes des enquêtes est le traçage des adresses IP pour connaître les données du FAI et identifier la personne qui utilise l'appareil ciblé.

Dans les enquêtes criminelles, l'adresse du protocole Internet est généralement la seule information qui relie le crime à l'individu, mais en raison du nombre limité d'adresses IPv4, les FAI utilisent la technologie pour compenser ce manque à gagner, ce qui pourrait avoir des résultats dangereux menaçant les enquêtes des forces de l'ordre, en partageant une seule adresse IP avec des milliers d'abonnés en même temps, ce qui rend impossible l'identification des abonnés individuels.

Il existe des outils de recherche en ligne gratuits que les enquêteurs doivent prendre en compte lorsqu'ils commencent à collecter des informations d'open sources, telles que Intel Techniques, Net Boot Camp et Research Clinic, ainsi que l'Information Framework, outre l'Open Source de renseignement, fournissant une infographie qui aide à collecter des informations auprès d'outils ou de sources gratuits, ainsi que le Guide 2018 des Informations d'Open Sources de renseignement, fournissant une liste complète d'outils qui aident les enquêteurs à explorer les informations disponibles sur les réseaux sociaux.

Facebook et Twitter

Facebook est l'un des sites de réseaux sociaux les plus populaires au monde, avec plus de 2,224 milliards d'utilisateurs en juin 2020. Dans la région du Moyen-Orient et Afrique du Nord, le nombre de ses utilisateurs en Égypte a atteint 42,4 millions, au Royaume d'Arabie Saoudite 23,72 millions, Irak 22,03 millions, Maroc 18,33 millions, Tunisie 7,445 millions et Jordanie 5,755 millions.

Suite à la publication de nombreuses publicités négatives et de problèmes de protection des données, Facebook a annulé le moteur de recherche de données, ce qui a compliqué la recherche des usagers du site lorsque seul l'e-mail ou le numéro de téléphone était disponible. Mais il demeure possible d'utiliser le moteur de recherche de Facebook pour accéder à un grand nombre d'informations. Même si la personne recherchée s'est bloquée à la vue du public, elle peut toujours être retrouvée en recherchant dans la liste des parents, ou dans le langage de balisage utilisé dans la documentation de la page. Certains outils Internet permettent aussi la recherche d'images et où elles ont été prises.

En 2020, le nombre d'internautes sur Twitter est passé à 330 millions usagers mensuels dans le monde, dont environ 42% fréquentent quotidiennement la plateforme. Le nombre de comptes sur Twitter travaillant au profit de Daech a atteint environ 46.000 comptes en 2015.

Twitter peut être considéré comme un moyen d'envoyer des SMS sur Internet, ce qui rend fastidieuse la recherche dans d'énormes quantités de messages. Twitter fournit des instructions aux enquêteurs sur les procédures à suivre pour obtenir des enregistrements. La première chose à comprendre lorsque l'on mène des enquêtes avec Twitter est que les résultats de recherche sur ce site se divisent en plusieurs sections, et il est possible d'interchanger les catégories au sein de l'application elle-même : personnes, photos, tweets et vidéos.

Il existe des outils en ligne gratuits disponibles pour aider les enquêteurs sur Twitter, notamment : Geosocial Footprint; TweetBeaver; NodeXL, utiles pour télécharger et analyser les mégadonnées sur Twitter; outre Maltego outil très utilisé aussi.

Preuves à recueillir

- **Informations stockées électroniquement:** créées, stockées ou utilisées avec la technologie numérique, telles que : les fichiers de traitement de la parole, les messages électroniques et les messages textuels.
- **Preuves électroniques informatiques:** informations et données utiles pour les enquêtes, stockées ou transmises sur ordinateur, devenant ainsi des preuves latentes telles que les empreintes digitales ou l'ADN.

- **Preuves numériques:** classées en informations et données utiles pour l'enquête, stockées, envoyées ou transmises par un appareil électronique, de telles preuves étant requises si des données ou des appareils électroniques sont saisis.
- **Sites Web et cookies:** toute information disponible sur Internet stockée dans le système informatique, et récupérable par la criminologie matérielle. Mais certaines de ces informations peuvent être volatiles, de sorte que leur contenu peut être modifié ou supprimé avant que ces appareils ne soient localisés et examinés. Dans de tels cas, il serait nécessaire de capturer les preuves directement à partir d'Internet, lors d'une interaction en direct avec le suspect, ou en se procurant le contenu du site Web en direct.

Une fois qu'un site Web est capturé ou que son contenu collecté, l'enquêteur peut accéder à des informations pouvant être utiles à l'enquête. L'enquêteur doit envisager l'utilisation des cookies, qui sont de petits fichiers stockés sur l'ordinateur de l'utilisateur, conçus pour contenir une petite quantité de données sur un client ou un site Web spécifique, et accessibles via le serveur Web ou l'ordinateur client.

- **Registres Internet:** ce sont les documents informatiques, e-mails, messages SMS, messages instantanés, transactions, photos et archives Internet, pouvant être collectés à partir d'appareils électroniques et utilisés comme preuves significatives. Les sites Web enregistrent les adresses IP. Le Gmail, par exemple, enregistre les titulaires de compte et l'adresse IP d'origine à partir de laquelle le compte a été enregistré. Les appareils mobiles, les ordinateurs portables et les ordinateurs de bureau utilisent des systèmes de sauvegarde en ligne, appelés (Cloud informatique).

Les systèmes basés sur le cloud permettent aux enquêteurs d'accéder aux messages textuels et aux photos à partir d'un téléphone spécifique et de conserver 1000 à 1500 des derniers messages textuels envoyés et reçus à partir de ce téléphone. De nombreux appareils mobiles stockent des informations sur l'endroit où l'appareil a pu se déplacer, ainsi que des informations sur le temps que le propriétaire du téléphone a passé dans chaque endroit. Pour obtenir ces informations, l'enquêteur peut accéder aux 200 derniers sites cellulaires atteints par l'appareil mobile.

Dans tous les cas, l'enquête et la poursuite des affaires qui incluent des preuves numériques nécessitent des compétences spéciales en matière d'enquête pénale, ainsi que la disponibilité de l'expertise, des connaissances et de l'expérience nécessaires pour appliquer ces compétences, et la connaissance de toutes les exigences et procédures légales liées à l'acceptation et règles de preuve aux niveaux local et international. Les enquêteurs peuvent se référer au document de l'ONUDC intitulé « Directives de base à l'intention des enquêteurs et des procureurs pour demander des données/preuves électroniques/

numériques aux juridictions étrangères », et qui contient plusieurs bonnes pratiques.

Collecte de preuves électroniques

L'un des principaux défis du point de vue de la justice pénale : la collecte et l'acceptation de preuves électroniques dans les procédures pénales. Des précautions doivent toujours être prises lors de la collecte, de la conservation et de la transmission de ces preuves pour les garder en sécurité. Parmi les bonnes pratiques à cet égard figurent :

- Rassembler les appareils et autres matériels après avoir sécurisé la scène du crime, par l'autorité légale chargé de confisquer les preuves.
- Enregistrement photo ou vidéo de la scène du crime, avant d'en extraire quoi que ce soit. Prendre des photos pour documenter toute activité sur l'ordinateur ou les appareils, et enregistrer toute information sur l'écran. Faute de caméra, dessiner le schéma du système afin de pouvoir le reconstruire ultérieurement.
- Consigner les chargeurs, câbles, périphériques et manuels associés, supports de données, téléphones portables, disques durs externes et cadres photo électroniques.
- Documenter toute activité sur l'ordinateur et ses périphériques en prenant des photos et en enregistrant toute information apparaissant à l'écran pour éviter toute altération des preuves numériques.
- Quatre principes sont pris en compte lors de cette étape de l'enquête, à savoir :

1. Aucune action des forces de l'ordre ou de leurs équipes affiliées ne doit altérer les données des ordinateurs ou des supports de stockage sur lesquels le tribunal peut s'appuyer ultérieurement.
2. Dans les circonstances où une personne considère qu'il est nécessaire d'accéder aux données originales stockées dans des ordinateurs ou des supports de stockage, cette personne doit être qualifiée pour le faire et être en mesure de fournir des preuves expliquant la pertinence de ses actions.
3. Une piste d'audit, ou tout autre enregistrement de toutes les opérations effectuées sur les preuves informatiques et électroniques, doit être créée, et ces preuves doivent être conservées. Un tiers indépendant devra être autorisé à examiner ces processus et à arriver à la même conclusion.
4. La personne en charge de l'enquête a l'entière responsabilité d'assurer le plein respect de la loi.

Analyse criminologique des données

Le traitement des preuves est l'un des aspects les plus importants de l'informatique judiciaire de plus en plus utilisée. L'une des transformations les plus récentes dans le traitement des preuves est le passage du simple (débranchement) de l'appareil, première étape de la collecte de preuves, à l'adoption de méthodes pour obtenir des preuves directement à partir de l'ordinateur personnel du suspect.

L'approche traditionnelle du « débrancher la prise » ignore les énormes quantités de données volatiles stockées dans la mémoire qui peuvent être perdues. Par conséquent, si un ordinateur est allumé, un expert en criminologie informatique devra intervenir, car éteindre l'ordinateur peut entraîner la perte de preuves d'activités criminelles. Si l'ordinateur est allumé, mais qu'il exécute un programme qui efface les informations, l'alimentation doit être immédiatement coupée de l'ordinateur pour préserver ce qui reste dans l'appareil.

L'évolution rapide de l'environnement informatique a créé des défis nécessitant un changement dans la collecte de preuves numériques. Il est devenu possible d'installer des applications à partir de supports amovibles, tels que des lecteurs flash, puis de les placer par défaut dans la RAM, sans laisser aucune trace. Il est également possible que le malware soit complètement présent dans la RAM, sans aucune trace de sa présence sur le disque dur. Les utilisateurs peuvent exécuter des fichiers ou des partitions cryptés cachés ou secrets dans l'espace du disque dur pour cacher des preuves. Les navigateurs Web bien connus permettent à l'utilisateur de masquer ses traces et de supprimer les fichiers journaux de son activité lorsque le navigateur est fermé.

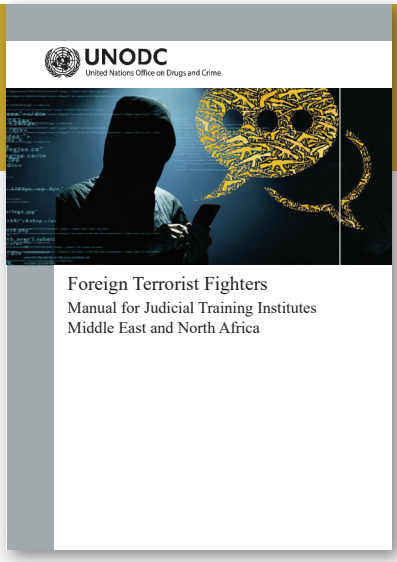
Face aux défis ci-dessus, l'archivage et l'analyse des données volatiles peuvent offrir le seul moyen de trouver des indices importants qui ne seraient normalement pas disponibles si l'appareil était éteint.

Les utilisateurs d'ordinateurs ne réalisent souvent pas que certains services sont activés lorsqu'ils utilisent l'ordinateur à l'insu de l'utilisateur, de sorte que la découverte de pilotes enregistrés peut fournir aux enquêteurs des informations sur les périphériques associés à l'appareil d'un suspect.

L'enquêteur ne doit pas tenter d'utiliser un appareil mobile verrouillé, mais tenter de retirer sa batterie, car un téléphone éteint conserve des informations sur l'emplacement de la tour de téléphonie cellulaire et le journal des appels, de plus, si l'appareil reste allumé, les preuves qu'il contient peuvent être détruites à l'aide de commandes à distance, à l'insu de l'enquêteur. Certains téléphones implémentent automatiquement les mises à jour pouvant mettre en danger les données du téléphone. Retirer la batterie demeure donc la meilleure solution.

Mais si le portable est en mode de fonctionnement, il doit être maintenu dans cette position le plus longtemps possible, sachant que l'enquêteur doit conserver des chargeurs adaptés aux différents types d'appareils. Il doit également essayer de déverrouiller l'écran si possible, et l'appareil doit être mis en mode (Avion) pour arrêter sa connexion au (Wi-Fi), Bluetooth, ou tout autre système de communication.

Si le portable est allumé et que son écran est éteint, le connecter à une source d'alimentation le fera souvent synchroniser avec les services cloud lors de l'exécution, ce qui devra augmenter la quantité de preuves disponibles dans le cloud informatique.



LES COMBATTANTS TERRORISTES ÉTRANGERS

MANUEL DES INSTITUTS DE FORMATION JUDICIAIRE AU MOYEN-ORIENT ET EN AFRIQUE DU NORD

Éditeur

l'Office des Nations Unies contre la drogue et le crime (ONUDC)

février 2021


التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

التحالف الإسلامي العسكري لمحاربة الإرهاب

ISLAMIC MILITARY COUNTER TERRORISM COALITION