ASSEMBLEE PARLEMENTAIRE DE L'OTAN

COMMISSION DES SCIENCES ET DES TECHNOLOGIES (STC)

Sous-commission sur les tendances technologiques et la sécurité (STCTTS)

TRANSACTIONS SECRÈTES : L'USAGE DES MESSAGERIES CRYPTÉES, DU *DARK WEB* ET DES CRYPTOMONNAIES PAR LES TERRORISTES

Rapport

par Matej TONIN (Slovénie)
Rapporteur

182 STCTTS 18 F fin | Original : anglais | 18 novembre 2018

.

TABLE DES MATIÈRES

I. INTRODUCTION

1. La volonté de l'espèce humaine de communiquer de façon confidentielle remonterait à la nuit des temps puisque la première tentative connue de chiffrement – à savoir l'utilisation d'un code confidentiel pour crypter et décrypter des messages – date en effet de l'Égypte ancienne, il y a près de 4 000 ans (*Cypher Research Laboratories*, 2014). Jusqu'à la fin du XX^{e} siècle, les technologies de chiffrement les plus puissantes étaient principalement aux mains des États. Aujourd'hui, elles sont disponibles à grande échelle et procurent à leurs utilisateurs plusieurs avantages importants, dont les suivants :

- **Authentification** : Les destinataires peuvent être assurés que leurs interlocuteurs sont bien les personnes qu'ils prétendent être et non des imposteurs.
- **Intégrité** : Les utilisateurs peuvent être assurés que les données qu'ils reçoivent d'autres personnes n'ont pas été modifiées (intentionnellement ou non) entre l'envoi et le lieu/la date de réception.
- **Confidentialité** : Les utilisateurs peuvent être assurés que les données qu'ils reçoivent ne peuvent pas être lues par des tiers.
- **Anonymat** : Selon les méthodes utilisées (notamment pour le chiffrement), les utilisateurs peuvent établir une distance entre leur identité réelle et leur pseudonyme numérique, ce qui leur permet des degrés divers d'anonymat.

2. Les technologies de chiffrement d'aujourd'hui « sont devenues le fondement de l'Internet moderne » (Moore & Rid, 2016). De fait, le chiffrement *par défaut* « est en train de devenir la nouvelle norme de la cybersécurité individuelle » (Buchanan, 2016). Honnêtement, qui aurait raisonnablement confiance dans les banques ou les services d'administration en ligne si nous n'étions pas convaincus que nos données sont suffisamment protégées par un cryptage solide ? Dans les démocraties libérales, les communications confidentielles jouent en outre un rôle vital et légitime au regard de la protection des droits humains fondamentaux, tels que le respect de la vie privée et la liberté d'expression (Chertoff & Simon, 2014). À vrai dire, les technologies de chiffrement modernes « sont au XXI^{e} siècle un ingrédient crucial de tout ordre politique libre » (Moore & Rid, 2016). Sous un régime autoritaire, la communication sous couvert d'anonymat peut faire courir un réel danger de mort à tout militant, dissident ou journaliste.

3. Comme n'importe quelle technologie, le chiffrement moderne présente toutefois une face obscure. Ses avantages attirent inévitablement l'attention d'acteurs malveillants, dont les extrémistes et les terroristes. Ces groupes sont généralement organisés de façon décentralisée, chacun des membres ayant peu – voire pas – d'informations sur les autres cellules en place ou sur les chefs de leur organisation. Même Daech, qui a adopté une structure plus hiérarchisée et territoriale en Iraq et en Syrie a, au fur et à mesure qu'elle a subi des pertes de territoire, accru sa décentralisation. Dans le contexte actuel, un système aussi fluide serait presque impossible à entretenir si les terroristes n'avaient pas accès à des **services de messagerie cryptée** à des fins de propagande, de recrutement, de communication, de commandement et de contrôle, de financement et d'acquisitions illicites. Les technologies modernes de chiffrement ont également favorisé l'émergence de deux autres technologies susceptibles d'élargir le champ des possibles pour les extrémistes et les terroristes, à savoir : le ***dark web*** (web clandestin ou « web sombre »), composé de serveurs Internet volontairement cachés ; et les **cryptomonnaies** (ou monnaies virtuelles) protégées par chiffrement.

4. Ce rapport alimente et complète les travaux menés depuis un certain temps par la commission des sciences et des technologies (STC) sur les technologies de rupture ayant d'importantes implications sur les politiques de défense et de sécurité. Ce rapport adopté lors de la session annuelle qui s'est tenue à Halifax (Canada), en novembre 2018.

5. Ce document présente tout d'abord succinctement le fonctionnement des technologies de chiffrement modernes, des services de messagerie cryptée, du *dark Web* et des cryptomonnaies. Il

examine ensuite quel usage font les groupes extrémistes et terroristes de ces instruments pour leurs communications, leurs tâches de commandement et de contrôle, leur financement et leurs acquisitions illicites. Après quoi, il analyse les grands débats de fond que suscitent ces technologies. Enfin, le rapporteur émet quelques recommandations sur la voie à suivre.

II. PRÉSENTATION DES TECHNOLOGIES DE CHIFFREMENT

A. LE CHIFFREMENT MODERNE

6. Jusque dans les années 1970, la seule méthode disponible pour crypter et décrypter les messages électroniques consistait en un **chiffrement symétrique**, en vertu duquel l'expéditeur et le destinataire devaient posséder la même « clé » pour déverrouiller un message. Si un individu accédait à cette clé ou décryptait le code, alors les communications n'étaient plus protégées. Pendant la guerre froide, l'art de la guerre a acquis une très grande complexité et il est devenu de plus en plus difficile de sécuriser la distribution des clés de chiffrement. À la fin des années 1960, un fonctionnaire du Centre national des communications britannique fut le premier à proposer une nouvelle méthode de chiffrement pour résoudre le problème de la distribution de ces clés. Cela dit, un véritable tournant a été effectué lorsqu'en 1976, des chercheurs de l'université de Stanford en ont fait de même mais cette fois-ci, en publiant leurs conclusions, permettant ainsi aux chercheurs du monde entier de pousser plus loin leurs travaux. Ainsi est né « l'une des inventions majeures du XX^{e} siècle », à savoir : le chiffrement asymétrique à clé publique (Moore & Rid, 2016).

7. Si les mathématiques qui sous-tendent la méthode de **chiffrement asymétrique à clé publique** sont complexes, l'idée, elle, est simple. Les personnes qui souhaitent communiquer en toute confidentialité reçoivent une *clé privée* et une *clé publique*, qui sont liées mathématiquement. Il est important de noter que la clé publique est visible de tous. Par exemple, si Alice veut envoyer un message confidentiel à Pierre, elle doit utiliser la *clé publique* de Pierre pour crypter son message. Pierre étant le seul à avoir accès à la *clé privée*, il est aussi le seul à pouvoir ouvrir le message. Même Alice ne peut plus lire son propre message. L'avantage crucial de cette technique est qu'Alice et Pierre n'ont plus besoin de se rencontrer pour s'échanger les clés ni de recourir à un intermédiaire pour le faire.

8. Pendant près d'une vingtaine d'années, l'administration états-unienne et ses alliés ont veillé à ce que la puissante technique du chiffrement à clé publique ne tombe pas entre les mains du grand public ou des adversaires des États-Unis, allant jusqu'à la classer dans la catégorie « munitions » en 1976 et adoptant des lois très strictes en matière d'exportation (Bartlett, 2014). Cela dit, les fondements de cette technique étaient connus et à mesure que la puissance de calcul augmentait à vitesse grand V, hors de tout contrôle gouvernemental, cette technologie a commencé à se disséminer, à la fois auprès des citoyens mais aussi des États non occidentaux. Malgré les efforts déployés par le gouvernement des États-Unis, la puissante technique du chiffrement à clé publique a finalement échappé à tout contrôle, à mesure que des individus soucieux de la protection de la vie privée et des « cypherpunks » libertaires se sont mis à l'utiliser et à en vanter les bienfaits. En 1996, la technique du chiffrement à clé publique a été ajoutée à la *Commerce Control List* régissant les exportations, ce qui a mis un terme aux « Crypto Wars » (ou guerres de la cryptographie). Aujourd'hui, cette technologie est omniprésente et il est difficile d'imaginer où en serait Internet sans elle. La plupart des utilisateurs d'Internet utilisent à divers degrés le chiffrement – par défaut et souvent sans le savoir – par exemple lorsqu'ils naviguent sur des sites internet sécurisés ou envoient des messages privés par messagerie ou par e-mail. Ceux qui recherchent une plus grande confidentialité – que ce soit pour des raisons candides ou malveillantes – n'ont pas besoin d'aller très loin. Internet regorge d'informations sur la façon de protéger ses données d'une interception par des tiers, qu'il s'agisse d'États, de malfaiteurs ou de terroristes. En d'autres termes, ceux qui veulent laisser le moins d'empreintes possible sur la toile n'ont aucun de mal à le faire, car cela ne requiert que peu de connaissances numériques ou compétences techniques.

B. LES SERVICES DE MESSAGERIE CRYPTÉE

9. Les médias sociaux populaires que sont par exemple Facebook et Twitter font de plus en plus la chasse – quoiqu'insuffisamment aux yeux de certains – aux contenus à caractère extrémiste ou terroriste. Les services de messagerie instantanée cryptée sont donc devenus essentiels pour les communications, les tâches de commandement et de contrôle, les acquisitions et le financement des acteurs concernés.

10. Avec environ 1,5 milliard d'utilisateurs, **WhatsApp** est l'application de messagerie la plus populaire au monde (Statista, 2018). Depuis avril 2016, elle est dotée par défaut d'une technologie de chiffrement à clé publique, appelée « chiffrement de bout en bout ». L'application offre par ailleurs une confidentialité parfaitement constante, du fait que les clés privées et publiques des utilisateurs sont changées régulièrement et automatiquement (Greenberg, 2016). Ce type de confidentialité résout en grande partie le problème de l'intrusion de tierces personnes qui déroberaient secrètement les clés privées et mettraient en danger les communications futures. Avec le nouveau dispositif, même si un intrus réussit à voler ces clés, il ne pourra accéder qu'à une petite quantité de données. L'application WhatsApp est toujours largement utilisée par les extrémistes et les terroristes en raison de sa grande popularité, de ses normes strictes en matière de chiffrement ainsi que de la possibilité d'utiliser facilement un numéro virtuel ou temporaire (Stalinsky & Sosnow, 12 septembre 2017). L'application commence cependant à perdre de son aura auprès de ces derniers (Stalinsky & Sosnow, 3 janvier 2017). D'une part, parce qu'elle coopère généralement volontiers avec les services de police et, d'autre part, parce que les malfaiteurs commencent à suspecter que les services de renseignement et de répression ont des points d'entrée dans ses protocoles de chiffrement.

11. En conséquence, les extrémistes et les terroristes se sont assez vite tournés vers l'application **Telegram**, lancée en 2013 par Nikolai et Pavel Durov, les cofondateurs du réseau social russe **VKontakte**. En 2014, les deux frères à l'esprit libertaire ont refusé d'autoriser le gouvernement russe à accéder à certains comptes russes et ukrainiens sur leur réseau. Aujourd'hui en exil volontaire, ils n'exercent plus la gestion de VKontakte. Telegram permet également d'activer un chiffrement de bout en bout. Son mode de conversation « secret » serait notamment protégé par des protocoles de chiffrement de niveau militaire (Stalinsky & Sosnow, 3 janvier 2017). Les conversations ne laissent donc aucune trace sur les serveurs de l'application ; les messages peuvent être configurés pour « s'autodétruire » et ne peuvent pas être transférés à d'autres utilisateurs. L'utilisation d'un faux numéro de téléphone est aussi plus facile sur Telegram que sur d'autres plateformes. Selon les analystes, l'application signale peu les communications suspectes et les réseaux extrémistes et terroristes y sont rarement suspendus (Stalinsky & Sosnow, 3 janvier 2017). Ces critiques sont toutefois réfutées par Telegram.

12. Il existe évidemment d'autres services de messagerie instantanée cryptée. C'est le cas notamment des jeux en ligne multi-joueurs, ou des nombreux logiciels, appareils ou applications mobiles comportant des services de messagerie instantanée intégrés. Toutefois, leur popularité auprès des terroristes n'a pas (encore) atteint celle de WhatsApp ou de Telegram (Stalinsky & Sosnow, 3 janvier 2017). L'application en code source libre **Signal**, par exemple, est équipée d'une technologie de chiffrement de pointe et jouit depuis peu d'une grande notoriété. Son protocole cryptographique est également utilisé dans d'autres applications dont le code source est fermé (comme WhatsApp) et dans les modes cryptés de **Messenger** (Facebook) et d'**Allo** (Google). Aucune métadonnée n'est conservée, hormis le dernier jour de connexion de l'utilisateur (Lee, 2017). L'un des avantages de Signal est que, grâce à son code ouvert, l'application peut être facilement dupliquée, modifiée et utilisée comme un outil de communication personnalisé par un groupe fermé, en utilisant des serveurs privés pour échanger des données. En revanche, Signal est nettement moins aisé à utiliser que Telegram ou WhatsApp. De plus, il n'est pas possible d'envoyer des fichiers volumineux et le son n'est pas toujours de bonne qualité. Il existe également des services de messagerie fonctionnant par chaîne de blocs ; c'est le cas notamment de **Nynja**, qui

comporte également un marché intégré ainsi que sa propre cryptomonnaie (une fonctionnalité que Telegram envisagerait également de proposer). D'autres applications très sécurisées, comme notamment **Kik**, **SureSpot**, **WeChat** et **Wickr** rencontrent un certain succès.

13. Daech a par ailleurs développé sa propre application cryptée, baptisée **Alrawi**. Conçue pour les membres de l'organisation, elle ne se trouve que sur le *dark web*. Cela signifie qu'elle est très difficile à bloquer, mais également peu accessible. Il semblerait qu'elle ne soit pas aussi sécurisée que d'autres applications du même type. Selon certains experts, elle a été créée en réaction aux fermetures d'autres applications et elle est utilisée pour planifier des attaques de haut niveau et partager des informations sensibles. D'aucuns considèrent qu'Alrawi est davantage un instrument de relation publique visant à attirer l'attention (Niglia, Al Sabaileh & Hammad, 2017).

14. Hormis les services de messagerie instantanée, d'autres systèmes permettent de crypter les communications. C'est le cas, par exemple, du service de messagerie électronique **Protonmail**, qui compte des millions d'utilisateurs légitimes, mais jouit également d'une popularité croissante auprès des extrémistes et des terroristes. La société ne conserve pas les messages sur ses serveurs, ne détient pas de copies des clés de chiffrement et elle propose une option d'autodestruction des messages. En 2017, elle a également lancé un service sur le *dark web*, un réseau privé virtuel (VPN) et la possibilité de payer en bitcoins (Stalinsky & Sosnow, 26 octobre 2017).

C. LE *DARK WEB*

15. Les experts décrivent souvent le *World Wide Web* comme un réseau composé de plusieurs couches (Microsoft, 2016). La première est celle du **web visible**, qui inclut tous les sites pouvant être indexés par le logiciel collecteur des moteurs de recherche classiques. Toutefois, à l'instar d'un filet de pêche traîné à la surface de l'océan, le logiciel collecteur analyse et indexe seulement une petite partie du contenu d'Internet (Bergman, 2001). Les sites internet qui ne peuvent être indexés par ce logiciel se trouvent dans la deuxième couche : le **web invisible**. Les raisons pour lesquelles ils ne peuvent être indexés sont variables. Certains sites sont privés et exigent des identifiants de connexion. D'autres sont impossibles à indexer en raison même de leur nature (ayant par exemple des contenus dynamiques ou dissociés).

16. La troisième couche d'Internet est le ***dark web.*** Le *dark web* est un ensemble de serveurs dont les adresses IP sont masquées, ce qui rend quasiment impossible la localisation des sites qui y sont hébergés. Toutefois, bien que certains de ces sites ne soient pas indexés, la grande majorité figurent sur des listes d'indexation (par exemple *The Hidden Wiki*), des forums d'utilisateurs ou des moteurs de recherche spécialisés (par exemple Ichidan ou Torch) ; cela dit, ces outils ne sont souvent ni complets, ni à validité permanente. En d'autres termes, les sites du *dark web* ne sont pas véritablement cachés. Leurs utilisateurs potentiels n'ont pas besoin de compétences ou d'instructions spécifiques, si ce n'est de comprendre les informations que l'on trouve facilement en ligne. Néanmoins, le risque de commettre des erreurs – et donc de compromettre l'anonymat recherché – est grand, ce qui représente une bonne nouvelle pour les professionnels des services de police et des agences de renseignement.

17. Les sites du *dark web* – que l'on appelle souvent des « services cachés » – sont conçus pour être impossibles à repérer et pour échapper aux restrictions de contenus ou aux opérations de surveillance (Moore & Rid, 2016). Mais le *dark web* a aussi de nombreuses fonctions tout à fait licites et légitimes (Chertoff & Simon, 2014) :

- Les journalistes l'utilisent notamment pour protéger leurs sources ou partager des fichiers, par exemple à l'aide du service *Secure Drop*, utilisé par des journaux aussi prestigieux que le *New York Times*, le *Washington Post* et le *Wall Street Journal*.
- Dans les pays où l'accès à Internet est restreint, il permet aux dissidents de contourner la censure, par exemple en accédant au site du *New York Times*.
- Dans les pays autoritaires, il est utilisé par les défenseurs des droits humains, comme en Iran qui a récemment pris des mesures radicales à l'encontre des logiciels du *dark Web*.
- De nombreux sites du web visible (par exemple Facebook) ont leur pendant sur le *dark web*.
- Les forces armées et les services de renseignement s'en servent pour communiquer, pour les tâches de commandement et de contrôle, ainsi que pour échanger des renseignements.
- Les services chargés de l'application de la loi en assurent la surveillance, l'utilisent pour mener des opérations d'infiltration, voire pour obtenir des tuyaux sous couvert d'anonymat.

18. Il est aujourd'hui impossible de connaître avec exactitude l'étendue des différentes couches du World Wide Web, notamment en raison de la forte expansion et de la fluidité des sites du web invisible et du *dark web,* ainsi que de l'anonymat – total ou partiel – de leurs utilisateurs. En 2016, Microsoft a estimé que le web visible ne représentait que 0,3 % de la totalité des pages Internet (Microsoft, 2016). En ce qui concerne le *dark web*, des chercheurs ont indiqué dans un rapport publié en 2014 avoir dénombré en l'espace de six mois l'existence de quelque 45 000 sites actifs en moyenne (Owen & Savage, 2015). Selon un expert interrogé pour les besoins du présent rapport, ce nombre a toutefois nettement diminué ces dernières années, certains groupes, comme le notoire *Anonymous*, ayant attaqué des serveurs hébergeant des contenus illicites (et notamment des sites pédopornographiques). Cet expert indique qu'il existe un peu moins de 10 000 sites accessibles grâce au logiciel Tor (voir ci-après), outil le plus utilisé pour accéder au *dark web*.

19. Bien que certains projets récents permettent d'accéder aux sites du *dark web* directement à partir du web visible, la plupart des utilisateurs doivent se doter d'un logiciel spécial : **Tor** (connu autrefois sous le nom de *The Onion Router*) est le plus utilisé ; un autre outil très populaire est l'I2P (*Invisible Internet Project)*. La technologie de Tor a été développée à l'origine par le laboratoire de recherche de la Marine des États-Unis pour protéger les communications des services de renseignement du pays. Elle a depuis été diffusée gratuitement et perfectionnée par des particuliers et des organisations privées. Du fait des liens qui existaient autrefois entre Tor et les agences gouvernementales des États-Unis, certains utilisateurs du *dark web* boycottent ce logiciel, car ils le suspectent de collecter des renseignements.

20. Tor a deux fonctions essentielles : d'une part, il masque l'adresse IP (*Internet Protocol*) et d'autres identifiants des utilisateurs souhaitant parcourir la toile sans être repérés. D'autre part, il permet aux utilisateurs d'accéder à des sites et à des services cachés sur le *dark web*. Il convient de noter que l'écrasante majorité des utilisateurs de Tor s'en servent uniquement comme d'un simple navigateur permettant de garder l'anonymat sur le web visible. Les utilisations de services cachés ne représentent que 3 à 6 % du trafic du logiciel (Moore & Rid, 2016). Sur le plan technique, Tor s'appuie sur un réseau d'environ 6 000 ordinateurs formant une structure mondiale de nœuds – également appelés « relais et passerelles » (Tor Metrics, 2018). Le signal de chaque utilisateur est crypté sur plusieurs niveaux (d'où la métaphore de l'oignon) et passe toujours à travers au minimum trois nœuds dont l'adresse IP est dissimulée à tous les autres.

21. Tor – et les autres logiciels – ne permettent pas à eux seuls d'assurer un anonymat parfait ; ils doivent, pour cela, être associés à d'autres technologies. Il est ainsi possible d'utiliser des systèmes d'exploitation « virtualisés », qui peuvent être copiés sur une clé USB, puis facilement supprimés ou détruits pour se débarrasser des preuves. Des méthodes permettent cependant d'accéder aux informations en clair (ou à certaines d'entre elles), ainsi qu'aux adresses IP des utilisateurs, par exemple en surveillant un grand nombre de nœuds ou en exploitant les vulnérabilités du serveur qui « laisse fuiter » ces adresses. En conséquence, certains utilisateurs (et en particulier

les cyber délinquants) ont commencé à s'orienter vers d'autres projets qui protègent mieux leur anonymat, et notamment les solutions pair-à-pair (P2P) ou fonctionnant par chaîne de blocs.

22. Bien évidemment, le *dark web* attire aussi des acteurs malveillants – notamment des extrémistes et des terroristes –, car c'est un endroit presque parfait pour mener secrètement des activités illicites. De fait, les principales utilisations de ce réseau sont les suivantes : trafic de drogues et autres produits illicites, services financiers, extrémisme, pornographie illicite (en particulier la pédophilie), piratage informatique, jeux, meurtres commandités, hacktivisme et trafic d'êtres humains (Moore & Rid, 2016 ; Chertoff & Simon, 2014).

D. LES CRYPTOMONNAIES

23. Selon le réseau *Financial Crimes Enforcement Network* (FinCEN) du département du Trésor des États-Unis, une monnaie virtuelle est « un moyen d'échange qui fonctionne comme une monnaie dans certains contextes, mais qui n'en possède pas toutes les caractéristiques » (FinCEN, 2013). Comme le précise le FinCEN, « une monnaie virtuelle n'a pas de cours légal dans quelque pays que ce soit ». Les cryptomonnaies sont une forme particulière de monnaie virtuelle ; elles sont protégées par chiffrement et au départ, elles ont été inventées pour échapper aux intermédiaires comme par exemple les banques.

24. Les tentatives de création de monnaies virtuelles – dans le but de s'affranchir des institutions financières traditionnelles – ont véritablement commencé dans les années 1990 (Goldman & al., 2017). Les deux principaux exemples sont l'or numérique et le service *Liberty Reserve*. Avec l'or numérique, créé en 1996, les utilisateurs pouvaient acheter, avec des devises bien réelles, des grammes d'or virtuel afin d'échapper aux fluctuations du marché. L'or numérique est vite devenu un refuge pour les activités criminelles et a été stoppé en 2009. En 2006, le service *Liberty Reserve* est donc apparu avec une alternative, principalement destinée à des usages illicites. Ce service a finalement été fermé en 2013.

25. Le véritable tournant en matière de monnaies virtuelles est apparu en 2008 lorsqu'un certain Satoshi Nakamoto a publié un article sur les principes d'une monnaie virtuelle pair-à-pair qui ne reposerait ni sur la confiance entre certains utilisateurs ni sur un contrôle centralisé comme l'était l'or numérique ou *Liberty Reserve*. Le bitcoin créé par Nakamoto était donc pour la première fois disponible en 2009 et les cryptomonnaies étaient nées. Les premiers adeptes du bitcoin ont souvent souligné que cette cryptomonnaie pourrait rendre obsolètes les monnaies gérées par les États de façon centralisée, en les remplaçant par une solution distribuée et décentralisée (Marr, 2017). Sans surprise, ce marché a rapidement été investi par des individus mal intentionnés.

26. L'engouement pour le bitcoin et les cryptomonnaies s'est véritablement développé en 2017. À l'heure actuelle, on dénombre au moins 1 600 cryptomonnaies présentant chacune leurs propres caractéristiques et spécificités. Les cryptomonnaies ont fait sensation sur les marchés financiers, avec une capitalisation totale estimée à plus de 266 milliards de dollars US à la mi-juillet 2018 (en baisse de 67 % par rapport à son niveau le plus élevé en janvier 2018, ce qui souligne bien la volatilité du marché) (Coinmarketcap, s.d.). Le **bitcoin** est toujours la cryptomonnaie la plus largement utilisée, avec une capitalisation boursière s'élevant à plus de 133 milliards de dollars. C'est plus de deux fois celle de la deuxième plus importante cryptomonnaie, l'**ethereum**.

27. Les cryptomonnaies présentent théoriquement de nombreux avantages qui les rendent attrayantes pour les utilisateurs. Ces avantages sont notamment les suivants :

- **Anonymisation / pseudonymisation** : La plupart des cryptomonnaies, dont le bitcoin, n'offrent qu'un semblant d'anonymat. Les identités virtuelles utilisées pour effectuer les transactions (autrement dit les pseudonymes créés par les utilisateurs) n'ont pas besoin d'être reliées à une identité réelle, mais elles doivent rester identiques pour toutes les transactions. Cela signifie que si le lien entre un pseudonyme et une identité réelle parvient à être établi,

tout l'historique des transactions peut alors être mis au jour. C'est l'une des raisons pour lesquelles les toutes nouvelles cryptomonnaies – dont le système de protection se rapproche davantage de l'anonymat – acquièrent un succès croissant. Pour citer un exemple, entre la mi-2016 et la mi-2018, la cryptomonnaie anonyme **Monero** a vu sa valeur multipliée par 90 et devient un moyen de paiement courant utilisé par les malfaiteurs sur le *dark web*.

- **Mobilité** : Les transferts peuvent s'effectuer depuis et vers n'importe quel ordinateur prenant en charge telle ou telle cryptomonnaie.
- **Pas d'obligation de confiance** : Il n'est pas nécessaire qu'un lien de confiance existe entre l'expéditeur et le récipiendaire de cryptomonnaie car pour chaque transaction, les nœuds du réseau vérifient les identités, les transactions et les chaînes de blocs (*blockchain*).
- **Aucune interférence** : Les cryptomonnaies, qui sont décentralisées et échangées entre particuliers (comme le bitcoin), n'ont pas besoin d'intermédiaires tels que des établissements financiers, des banques ou des États. Du fait de la popularité croissante de ces monnaies, les « échanges » – comme on les appelle – augmentent toutefois de façon exponentielle. Ces échanges servent d'interface entre monnaies réelles et virtuelles et constituent le portefeuille virtuel des utilisateurs.
- **Évolutivité** : Dans la mesure où les transferts ne s'accompagnent pas pour l'instant (ni dans un proche avenir) de frais de traitement importants, les utilisateurs peuvent transférer à moindre coût même des petites sommes. Le point positif est que cela a permis aux habitants des pays en développement, qui n'ont pas (ou très peu) accès au système financier officiel, de disposer de nouveaux outils.
- **Sécurité** : Lorsque les clés privées de chiffrement sont stockées en toute sécurité sur des appareils personnels ou sur le « *cloud* », les cryptomonnaies sont très sûres. En revanche, si ces clés sont volées, la cryptomonnaie l'est également.
- **Rapidité** : Il faut environ 10 mn pour qu'un transfert de bitcoins soit confirmé, mais ce délai est déjà plus court que pour de nombreuses autres cryptomonnaies (et d'ailleurs les transactions en bitcoins peuvent elles aussi être accélérées). Bien que ce soit plus long qu'un paiement en ligne par carte de crédit, l'avantage pour le récipiendaire est que l'expéditeur ne peut plus annuler le paiement une fois que la transaction a été confirmée.

28. **Les transactions en bitcoins** s'effectuent ainsi (d'autres cryptomonnaies fonctionnant de la même manière) : tout d'abord, l'expéditeur crée une signature numérique avec une clé privée, autorisant le déblocage et le versement des fonds. Un algorithme mathématique protège cette signature contre toute duplication ou falsification. La quantité de bitcoins est « envoyée » à la clé publique correspondante, qui est visible par tous les nœuds du réseau. Ces nœuds utilisent la clé publique et la signature numérique pour vérifier que l'expéditeur est bien détenteur de la clé privée (sans jamais voir cette dernière). Ensuite, les nœuds vérifient les ressources nécessaires à la transaction. Sachant que la transaction est autorisée, comment peuvent-ils toutefois vérifier que l'expéditeur possède bien les fonds requis ? Parce que l'expéditeur transmet alors des références de transactions antérieures lui ayant procuré les ressources. Le réseau vérifie toutes les transactions réalisées en bitcoins afin de s'assurer que l'argent est disponible. On le surnomme souvent « le grand livre comptable » du bitcoin. Les transactions sont alors passées au crible par l'ensemble du réseau, ce qui prend un certain temps. L'expéditeur pourrait certes tenter de duper le réseau en effectuant simultanément une autre transaction, c'est-à-dire en dépensant ses bitcoins deux fois. Comme le réseau est incapable de savoir quelle transaction a eu lieu en premier, il doit classer les transactions dans l'ordre. C'est là qu'intervient la chaîne de blocs qui a retenu toute l'attention des compagnies d'assurance, des pouvoirs publics, de l'industrie et des prestataires de soins médicaux. Un nœud regroupe un ensemble de transactions dans un bloc et présente ce bloc dans la chaîne des transactions. Les blocs contiennent un problème mathématique très exigeant, que chaque nœud tente de résoudre en premier – toutefois, le problème est si complexe que les nœuds ne peuvent que se contenter de deviner la solution. Le premier nœud qui la trouve est récompensé par une certaine quantité de bitcoins – d'où le terme de « minage » –, et la transaction est irrévocablement confirmée (Driscoll, 2013).

29. Les cryptomonnaies permettant un véritable anonymat n'ont pas encore autant de succès que le bitcoin ou quelques autres monnaies virtuelles. Dans le cas de monnaies fonctionnant à l'aide d'un pseudonyme – facteur déjà très avantageux pour tout acteur mal intentionné –, un fichier public récapitule l'ensemble des transactions effectuées par tel ou tel pseudonyme. Par conséquent, bien que l'opération soit complexe et fastidieuse, il est possible d'identifier les transactions figurant dans la chaîne de blocs en bitcoins. Cela dit, le *dark web* recèle aussi des services permettant de mélanger les transactions en bitcoins associés à d'autres transactions. Une fois le **mélange de monnaies** effectué, le montant requis est envoyé mais en monnaies différentes. Le traçage de l'origine des transactions vers telle ou telle personne est ainsi rendu plus difficile, mais compte tenu du développement considérable du marché des cryptomonnaies, les experts, entreprises et pouvoirs publics sont à la recherche de solutions pour résoudre le problème. Les individus souhaitant que leurs transactions soient difficiles à repérer peuvent utiliser **d'autres raccourcis**. Ainsi, le propriétaire d'une cryptomonnaie peut transmettre ses données de connexion et/ou ses mots de passe de récupération à une tierce personne qui peut, de cette manière, accéder à son compte et son contenu. Autrement dit, le transfert ne peut être tracé.

III. USAGE DES TECHNIQUES DE CHIFFREMENT PAR LES TERRORISTES

30. Depuis les années 1990, les organisations extrémistes et terroristes recourent aux technologies de l'internet pour différents usages, comme l'exploration de données, les communications, la planification et la coordination de leurs opérations, la propagande, le recrutement et la mobilisation, la formation et la collecte de fonds (Weimann, 2015). À mesure que les gouvernements, les entreprises, les organisations et les militants continuent d'intensifier leurs efforts pour contrer l'extrémisme violent et le terrorisme, ceux-ci se tournent progressivement vers les technologies de chiffrement.

31. Les estimations quant au nombre de terroristes et affiliés actifs sur les services de messagerie cryptée et sur le *dark web* ou encore qui réalisent des transactions en cryptomonnaies sont très variables. En fait, seules quelques données disparates permettent d'étayer les faits. À titre d'exemple, le nombre d'utilisateurs de Telegram pourrait se situer entre 10 000 et 80 000 (Stalinsky & Sosnow, 3 janvier 2017). Un *snapshot* en mars 2016 montrait que quelque 700 nouvelles plateformes se revendiquant de Daech avaient été créées (Barak, 2016). Selon l'Institut israélien des études nationales de sécurité, plus de 50 000 sites internet et 300 forums terroristes étaient actifs sur le *dark web* en 2011 (Rosner, London & Mendelboim, 2013). Néanmoins, une étude approfondie menée en 2016 sur quelque 5 205 sites actifs du *dark web* démontrait « la quasi-inexistence d'extrémisme islamique », recensant « seulement » 140 sites de ce type (Moore & Rid, 2016). Les preuves de l'utilisation de cryptomonnaies sont encore plus rares, seuls quelques cas isolés auraient été relevés à Gaza, en Indonésie et aux États-Unis.

A. COMMUNICATIONS, COMMANDEMENT ET CONTRÔLE

32. Pour les groupes extrémistes et terroristes, le web visible et les services de messagerie instantanée ont joué un rôle-clé en termes de communication ainsi que pour leurs tâches de commandement et de contrôle. Les membres de Daech ont par exemple utilisé l'application Telegram avant, pendant et après les attentats de novembre 2015 à Paris (Stalinsky & Sosnow, 3 janvier 2017). Pour tirer profit de ces attentats, l'organisation a ensuite utilisé les médias sociaux pour diffuser sa propagande, par exemple, en diffusant une vidéo montrant les terroristes lors de leur séjour en Syrie (Noack, 2016).

33. À mesure qu'une pression croissante s'exerce sur eux, les extrémistes et les terroristes s'orientent de plus en plus vers les services de messagerie cryptée et le *dark web*, sans pour autant abandonner leur présence sur le web visible (Stalinsky & Sosnow, 3 Janvier 2017). En vérité, extrémistes et terroristes sont devenus très doués pour utiliser simultanément le web visible, le *dark web* et les services de messagerie de manière très dynamique, en jouant sur les atouts de

chaque plateforme : Facebook, Twitter et YouTube permettent d'atteindre de larges audiences, mais sont plus exposés ; les services de messagerie cryptée et le *dark web* offrent une plus grande sécurité et sont mieux adaptés pour toucher les individus isolés et les petits groupes, mais ils ont une portée limitée.

34. L'utilisation de services de messagerie cryptée pour les **communications externes** a considérablement augmenté ces dernières années. Ainsi, l'application Telegram est utilisée, entre autres, pour le recrutement, la communication, la diffusion d'annonces, la distribution de contenus, la diffusion d'informations, la proclamation de menaces et de messages d'intimidation, la revendication d'attentats et les déclarations d'allégeance (Stalinsky & Sosnow, 3 janvier 2017). L'application a également, ces dernières années, introduit de nouvelles fonctionnalités qui rendent la plateforme plus attrayante pour les communications à grande échelle, voire publiques. Il est ainsi possible d'établir des conversations de groupe avec des milliers de membres, où chacun peut exprimer son opinion et poser des questions. Cela donne à ces membres un sentiment d'appartenance et leur permet de voir que d'autres individus partagent leurs points de vue (Brown & Korff, 2009). De surcroît, chaque groupe ou individu peut lancer une discussion publique qui peut être suivie par n'importe qui, une fonction qui fait de Telegram le nouveau « Twitter » (Stalinsky & Sosnow, 3 janvier 2017).

35. Jusqu'ici, seul un nombre restreint de communications externes ont été effectuées depuis le *dark web*. L'attrait de ce réseau pour la propagande est sans doute limité, en raison de sa difficulté d'accès pour la plupart des gens. En particulier, « les novices peuvent avoir peur de faire d'emblée un pas vers « l'illicite », par opposition à de simples recherches effectuées sur Google par curiosité » (Moore & Rid, 2016). La plupart des sites du *dark web* requièrent une invitation et des identifiants de connexion. De plus, ils ne sont pas aussi faciles à trouver que les sites du web visible car il n'existe pas de répertoire stable et centralisé des sites. C'est la raison pour laquelle, sur de nombreux forums en ligne, extrémistes et terroristes ont suggéré la création d'un « djihadwiki » (Weimann, 2015). Cela dit, comme indiqué plus haut, un grand nombre de listes d'indexation, de forums et de moteurs de recherche ont fait leur apparition ces dernières années et facilitent l'exploration du *dark web*.

36. Parallèlement, le *dark web* est utilisé de façon croissante pour abriter du matériel de propagande. Après les attentats de Paris en 2015, Daech a annoncé que le site *Isdarat*, qui contient toute la propagande de l'organisation, allait être déplacé sur le *dark web* en raison de la pression croissante qu'il subissait sur le web visible (Insite, 2015). Bien que le site soit désormais hébergé sur le *dark web*, tous ses contenus sont encore accessibles via des sites du web visible, comme par exemple Google Vidéo.

37. Dans de nombreux cas, le processus de **radicalisation** est le suivant : les sympathisants font de premières rencontres dans la vraie vie ou sur le web visible, puis ils font connaissance avec d'autres individus ou de petits groupes via des applications de messagerie instantanée. Ils sont ensuite progressivement endoctrinés et mis en contact avec d'autres individus qui peuvent les tester et les conduire encore plus loin sur le chemin de la radicalisation. Un grand avantage de ce processus est qu'un individu qui se montre intéressé peut être « testé », devenir membre de l'organisation et même effectuer une mission sans avoir eu de contact physique direct avec les autres membres (Magdy, 2016).

38. Les services de messagerie cryptée sont beaucoup utilisés par des groupes comme Daech ou al-Qaida dans la péninsule arabique (AQPA) pour leurs **communications internes et les tâches de commandement et de contrôle**. Le fait de pouvoir communiquer rapidement et secrètement avec différentes parties du monde permet aux groupes terroristes d'effectuer des formations ainsi que de planifier et de mener à bien des attentats. On dit par exemple que Daech, l'AQPA, Ansar al-Charia en Libye et l'ancien Front al-Nosra en Syrie font une utilisation intensive des communications cryptées sur Telegram (Barak, 2016).

39. Bien que plus difficile d'accès, le *dark web* peut être – et est – utilisé pour des communications ainsi que des tâches de commandement et de contrôle plus ciblées. En 2013, des communications cryptées ont été interceptées par la NSA (l'agence nationale de sécurité des États-Unis) entre le chef d'al-Qaida, Ayman al-Zawahiri, et celui de l'AQPA, Wasser al-Washishi. On a ensuite découvert que ces échanges avaient eu lieu sur le *dark web*. Les espaces de discussion hébergés sur Tor (comme The Hub et OnionChat), les outils de messagerie personnelle (comme Tor Messenger, Bitmessage et Ricochet), qui fonctionnent comme des applications de messagerie depuis le *dark web*, sont quelques-unes des options dont disposent les individus qui ont besoin de communiquer avec un degré supplémentaire d'anonymat et de solides systèmes d'authentification. Certains experts indiquent cependant que ces services dissimulés sur le *dark web* « sont souvent trop peu stables ou trop difficilement accessibles pour une communication efficace » (Moore & Rid, 2016).

B. ACQUISITION D'ARMES ET AUTRES BIENS ILLICITES

40. Selon une analyse effectuée par Europol en 2016, Internet et les médias sociaux sont actuellement utilisés par Daech pour se procurer des biens tels que des armes et de faux documents d'identité nécessaires pour commettre des attentats (Europol, 2016). Bien que les extrémistes et les terroristes n'aient aucun moyen d'être vraiment sûrs de ne pas être repérés, les identités secrètes, boîtes postales anonymes et autres astuces simples permettant de dissimuler leur identité rendent ces acquisitions possibles. Europol a noté en particulier que les applications cryptées comme WhatsApp, Skype ou Viber offrent aux terroristes un moyen relativement sûr de se procurer ces biens sans être repérés par les agences de renseignement ou les services de police.

41. Le *dark web* – et en particulier les services cachés du logiciel Tor – est un lieu bien connu des acteurs mal intentionnés car ils peuvent s'y procurer toutes sortes de biens illicites. Il existe à ce jour peu d'études approfondies sur la façon dont les extrémistes, terroristes et autres malfaiteurs utilisent le *dark web* pour y effectuer des achats illicites. Seuls des éléments épars sont en fait disponibles. Après les attentats de Paris en 2015, il a été dit que les terroristes s'étaient procuré leurs armes sur Internet, mais ces allégations n'ont pas été confirmées (Persi Paoli et al, 2017). En revanche, il a été établi avec certitude qu'un adolescent qui a tué plusieurs personnes à Munich en juillet 2016 avait acheté son arme sur le marché du *dark web*. Les Nations unies ont également fait savoir que certains groupes terroristes recherchaient sur le *dark web* des renseignements sur les armes de destruction massive (Besheer, 2017).

42. Pour l'heure, ce sont les experts de l'institut RAND qui ont réalisé l'étude la plus fouillée concernant le marché des armes sur le *dark web*, même si la capture qu'elle fournit ne s'étend que sur une semaine (Persi Paoli et al., 2017). Au cours de cette période d'observation, les analystes ont estimé que 52 marchands d'armes étaient actifs sur le *dark web* avec un catalogue de 811 produits. Les pistolets sont, de loin, les produits les plus courants. Un constat intéressant est que les articles numériques (par exemple les manuels de fabrication d'armes à feu et d'explosifs artisanaux, ou encore les plans d'impression des armes en 3D) représentent la deuxième catégorie de produits les plus vendus (évidemment, un grand nombre de ces produits numériques se trouvent également sans difficulté sur le web visible). Les analystes ont déduit par extrapolation que 136 ventes – d'un montant total de quelque 80 000 dollars US – étaient effectuées chaque mois sur ce réseau. Cela est peu comparé au commerce d'armes illicites qui a lieu dans le monde réel. En fait, le marché du *dark Web* a une portée limitée et ne semble être une solution viable que pour les petits groupes ou les individus isolés. Qui plus est, la communauté qui fréquente ce réseau est prudente – voire suspicieuse – quant à la viabilité du marché des armes du *dark Web* en raison « des escroqueries, de l'intensification de la surveillance policière et du faible volume des ventes ». Pour autant, les experts du RAND estiment que globalement, « le volume des ventes d'armes peut être considéré comme suffisamment élevé pour constituer une source de préoccupation pour les responsables politiques et les services de police ».

43. L'utilisation de cryptomonnaies – à l'aide d'un pseudonyme ou sous couvert d'anonymat – faciliterait l'achat de biens illicites par les terroristes. En effet, toutes les transactions effectuées sur le *dark Web* le sont avec des cryptomonnaies. Cela dit, même dans le monde réel, les transactions légales effectuées en cryptomonnaies augmentent ce qui pourrait représenter un risque (Goldman et al, 2017). Ainsi, des particuliers vivant au Texas peuvent tout à fait s'échanger des armes à feu sans qu'il n'y ait aucun contrôle d'antécédents (Brill & Keene, 2014).

C. FINANCEMENT DU TERRORISME

44. Le financement du terrorisme prend toutes sortes de formes. Le système financier international, très interconnecté, présente des failles que les groupes extrémistes et terroristes ne cessent d'exploiter. De surcroît, à une échelle moindre, les terroristes utilisent toutes sortes de sources de financement : prêts bancaires, allocations sociales, cartes cadeau, transferts d'espèces de la main à la main ou virements électroniques (Goldman et al, 2017 ; Keatinge & Keen, 2017).

45. Sur Internet, les extrémistes et les terroristes se livrent à la cybercriminalité pour s'enrichir, par exemple en commettant des attaques assorties de demandes de rançon. Les experts estiment cependant que la part de ces actes criminels commis en soutien à des causes extrémistes ou terroristes est encore relativement faible. Ils constatent en outre dans les services de messagerie cryptée une tendance aux appels aux dons et à la vente de toutes sortes de produits (Stalinsky & Sosnow, 12 septembre 2017). Il est par ailleurs possible que les terroristes essaient d'accéder – ou accèdent déjà – aux marchés illicites du *dark web* pour trouver des financements, par exemple en vendant des drogues illicites, des documents d'identité ou des données de cartes bancaires.

46. Il existe dans le monde réel toutes sortes de possibilités de financement mais, comme l'ont souligné les pouvoirs publics et les experts, les cryptomonnaies pourraient ouvrir de nouvelles perspectives aux terroristes. Le fait que ces monnaies puissent être utilisées anonymement, leur portée mondiale ainsi que le flou des cadres réglementaires constituent autant d'avantages (Goldman et al, 2017). Il y a effectivement un certain nombre d'années que les instances de réglementation ont appelé l'attention sur les risques soulevés par ces monnaies. L'Autorité bancaire européenne a par exemple émis un avis concernant le risque élevé que les monnaies virtuelles ne soient utilisées pour financer le terrorisme (*European Banking Authority*, 2014).

47. Bien que certains cas aient été médiatisés et que les organisations terroristes et extrémistes aient parfois fait l'apologie des cryptomonnaies, celles-ci ne sont pas encore utilisées de manière intensive par al-Qaida, Daech ou d'autres groupes. Cela peut s'expliquer par toutes sortes de facteurs. Premièrement, il faudrait un perfectionnement technologique majeur pour que les cryptomonnaies existantes soient utilisées à grande échelle avec le degré d'anonymat souhaité. Deuxièmement, dans nombre de zones où les groupes terroristes sont présents, la pénétration d'Internet est faible et les cyber infrastructures peu développées. Troisièmement, dans la mesure où les terroristes cherchent, en définitive, à avoir un impact dans le monde réel, il faudrait qu'ils amènent les cryptomonnaies dans le monde réel, or cela « introduit un facteur de complexité inutile et menace davantage le caractère déstabilisateur de leurs opérations ». Un point extrêmement important est que les extrémistes et les terroristes disposent de nombreuses alternatives aux cryptomonnaies. En fait, ces groupes ont toujours « la possibilité de contourner les règles mondiales qui régissent le financement du terrorisme avec suffisamment de facilité et de régularité, ce qui rend l'utilisation des monnaies virtuelles inutile ». En d'autres termes, les cryptomonnaies « ne deviennent une menace stratégique dans le domaine de la lutte antiterroriste que lorsqu'elles peuvent rivaliser avec les espèces et d'autres sources de financement faciles à se procurer, et acquièrent la même portée » (Goldman et al, 2017).

48. Au vu de ces analyses, la plupart des entités gouvernementales, des instances de réglementation et même des experts n'ont toujours pas de certitude concernant les niveaux de risque. Ainsi, dans leur évaluation nationale de 2015 sur les risques en matière de financement du terrorisme, les États-Unis indiquaient que le risque n'était pas clairement établi (*US Office of Terrorist*

Financing and Financial Crimes, 2015). De leur côté, les autorités britanniques n'ont relevé aucune utilisation illicite avérée de cryptomonnaie au Royaume-Uni, et précisent que ce risque « va probablement très peu augmenter dans les cinq prochaines années » (*UK HM Treasury & Home Office*, 2017). Un expert met en garde contre la surestimation des risques : « Le financement du terrorisme au moyen des cryptomonnaies est un risque qui pourrait s'accroître avec le temps, mais c'est un risque qui nécessite une réponse mesurée » (Carlisle, 2018).

IV. POLITIQUES ACTUELLES ET OPTIONS POUR L'AVENIR

49. L'utilisation des technologies de chiffrement par les extrémistes, les terroristes et autres acteurs malveillants est une source de défis multiples pour les responsables politiques, les services de police, les agences de renseignement, les entreprises, les particuliers et bien d'autres. Des politiques diverses ont été mises en œuvre et des options existent pour l'avenir. Néanmoins, il n'y a pas de solutions miracles et un grand nombre de ces options pourraient engendrer de nouveaux problèmes ou supposer des arbitrages politiques difficiles. Bien que non exhaustive, cette section abordera les principaux points et débats de fond sur la voie à suivre.

A. SURVEILLANCE, SIGNALEMENT ET PERTURBATIONS PAR LES MILITANTS, LES CITOYENS ET LES OPÉRATEURS

50. Comme dans la vraie vie, les citoyens constatant dans l'univers numérique des comportements, contenus ou messages inquiétants doivent le signaler aux opérateurs ou aux autorités compétentes. Depuis plusieurs années, les médias sociaux – dont les services de messagerie cryptée – sont critiqués pour la trop grande quantité de contenus illicites qui demeurent sur leurs plateformes pendant très longtemps. La situation a commencé à changer récemment, sous l'influence des pouvoirs publics ou de l'adoption par ces derniers de lois contraignantes. En conséquence, de nombreux systèmes de détection et de notification ont été améliorés. À l'avenir, les nouvelles technologies (par exemple l'apprentissage automatique/ l'intelligence artificielle et l'analytique des données massives) devraient permettre d'améliorer encore la détection et le retrait automatiques des contenus litigieux.

51. Outre le signalement opéré par les utilisateurs et le retrait effectué par les opérateurs, un certain nombre de groupes de militants mènent volontairement des actions de surveillance, de signalement et de perturbation, protégés par l'anonymat que permettent les technologies de chiffrement modernes (Solon, 2017). Le collectif hacktiviste *Anonymous* cible depuis longtemps les opérations de Daech et a même « déclaré la guerre » à l'organisation après les attentats de Paris en 2015. Les autres groupes militants sont notamment *Ghost Security Group*, *Di5s3nSi0N*, *Daeshgram*, *KDK* et le *Hellfire Club*. Certains coopèrent avec les services de police et les agences de renseignement pour lutter contre l'extrémisme et le terrorisme. D'autres, plus controversés, s'attaquent eux-mêmes de façon directe aux agissements radicaux et terroristes.

52. Le débat concernant les actions de surveillance, de signalement et de perturbation qu'il convient de mener à l'égard des contenus extrémistes ou terroristes est à la fois complexe et très politique mais suscite aussi des questions difficiles. Quelle est la frontière entre un contenu illicite qui doit être retiré et un autre considéré comme légitime en vertu de la liberté d'expression ? Qui décide de retirer des contenus : l'État, les citoyens ou les militants politiques ? Lorsque des contenus sont retirés, ceux qui ont procédé au retrait doivent-ils en informer les services de police ou les agences de renseignement, ou au moins conserver une copie des contenus à des fins de preuve ? L'État doit-il encourager les citoyens et les militants à jouer ce rôle, voire parrainer des pirates « éthiques » ou des « soldats » du cyberespace indépendants, ou cela serait-il assimilé à une justice populaire ? Si la réponse est affirmative, l'État doit-il les encourager à être simplement réactifs ou à pénétrer activement les réseaux extrémistes et terroristes ? Pour résumer, ce débat de fond n'est toujours pas tranché.

B. OPÉRATIONS DES SERVICES DE POLICE ET DES AGENCES DE RENSEIGNEMENT

53. Les services de police et les agences de renseignement possèdent déjà de nombreux outils pour faire obstacle aux activités menées par les groupes extrémistes et terroristes au moyen des technologies de chiffrement. Ils doivent encourager – et encouragent déjà – le signalement d'activités suspectes, mais ils doivent aussi organiser des opérations musclées pour surveiller et faire échouer les activités en question, ainsi que pour démanteler les réseaux extrémistes et terroristes.

54. Comme dans n'importe quelle enquête, les services de police peuvent essayer de **contraindre les entreprises privées à travailler avec eux**, **en vertu des lois et des réglementations existantes**. Le plus important, c'est que ces services puissent obtenir un accès aux données ou métadonnées se rapportant aux suspects et à leurs activités. Le succès de cette approche dépend tout d'abord de la disponibilité des données et/ou métadonnées auprès de l'entreprise concernée. En effet, à mesure que les applications adoptent des technologies de chiffrement hautement sécurisées, de moins en moins de données et de métadonnées sont accessibles, même si les sociétés privées sont disposées à coopérer. Dans d'autres cas, les entreprises refusent de répondre aux demandes des services de l'État : certaines pour des raisons idéologiques ou professionnelles ; d'autres parce que leur siège se trouve dans un autre pays et que l'administration locale ne peut – ou ne veut – pas apporter de l'aide. Malgré les difficultés, les services de l'État doivent exploiter toutes les possibilités offertes par la loi.

55. Le **travail de police** portant sur les services de messagerie cryptée et le *dark web* ainsi que sur les transactions financières effectuées en cryptomonnaies est forcément plus complexe que les enquêtes menées sur le web visible. À titre d'exemple, les récentes opérations qui ont été menées sur le *dark web* pour mettre au jour les principaux marchés illicites ont été longues et complexes, et ont requis des investigations à la fois en ligne et hors ligne. Toutefois, les progrès technologiques relatifs à la surveillance, l'analyse, l'accès et la perturbation de l'utilisation du chiffrement par les extrémistes et les terroristes – associés à l'anonymat que ces avancées procurent également aux services de police – devraient progressivement faciliter le travail des enquêteurs (Jardine, 2014 ; Chertoff & Simon, 2014). Comme le soulignent par exemple deux experts : « Une idée fausse très répandue est que Tor est protégé contre la surveillance des services de l'État et que ses utilisateurs peuvent donc agir en toute impunité. En réalité, toute entité dotée de ressources suffisantes peut lancer une attaque avec un haut degré de réussite tout en courant un minimum de risques d'être détectée » (Owen & Savage, 2015). Dotés d'une formation, d'effectifs et de ressources appropriés, les forces de police et d'autres entités peuvent bloquer ou contrôler des nœuds du réseau, démasquer les utilisateurs de Tor et attaquer des sites du *dark Web* (Owen & Savage, 2015 ; Moore & Rid, 2016).

56. Une autre action plus controversée des services de l'État est qu'ils peuvent (et nombre d'entre eux s'y attèlent) **s'attaquer aux systèmes de chiffrement en s'y infiltrant**. Ils pourraient, par exemple, détecter les failles de systèmes et les utiliser le moment opportun pour atteindre certains individus ou certains groupes. Les services de police et les agences de renseignement pourraient chercher à secrètement s'infiltrer pour accéder à certaines données ou métadonnées, mais ils pourraient également accéder au système lui-même et ainsi, aux machines ou même aux sites du *dark web* dans leur ensemble (Buchanan, 2016). De cette façon, ils pourraient lire les messages texte au fur et à mesure qu'ils sont saisis, enregistrer en direct les appels téléphoniques et surveiller d'autres activités. Le problème est que franchir une telle ligne équivaudrait à une escalade eu égard aux écoutes téléphoniques classiques, car cela nécessiterait l'installation d'un logiciel spécialement conçu à des fins malveillantes. On passerait alors d'une collecte passive d'informations à une surveillance active. La légitimité et la légalité de telles actions seraient variables d'un pays à l'autre et dépendraient des cibles : ressortissants nationaux ou étrangers. Le plus inquiétant peut-être est que cela exposerait les systèmes de chiffrement à des risques : si les services de l'État peuvent trouver leurs points faibles, des acteurs malveillants peuvent en faire de même. De surcroît, il peut

arriver que les outils utilisés et les vulnérabilités exploitées par les services gouvernementaux soient divulgués, que ce soit de manière intentionnelle ou par accident. L'affaire *Shadow Brokers*, par exemple, est connue comme l'un des pires cas de violation de la sécurité d'une agence de renseignement des États-Unis. En 2016, le groupe se faisant appeler *Shadow Brokers* a rendu public une multitude d'outils de piratage ultra-puissants utilisés par l'agence états-unienne, outils aujourd'hui facilement accessibles pour des acteurs mal intentionnés.

57. Les services de police cherchent par ailleurs à **repérer et combler les failles en matière de sécurité** des technologies de chiffrement. Par exemple, bien que le code du bitcoin soit conçu pour protéger cette monnaie contre tout piratage, une faille pourrait l'exposer à des menaces numériques. Fin 2017, Interpol et la société Kaspersky, spécialisées dans la cybersécurité, ont découvert dans le grand livre comptable du bitcoin une faille susceptible d'être exploitée à des fins malveillantes. En réaction, un projet conjoint a été mis sur pied par Interpol et les services de police européens pour analyser les composantes du bitcoin qui facilitent sa non-détection par les forces de l'ordre, tout en respectant la protection de la vie privée des utilisateurs de bitcoins.

58. Un autre volet très utile de la lutte contre l'utilisation illicite des technologies de chiffrement serait d'intensifier la **coopération internationale** à tous les niveaux de l'État et dans de nombreux domaines de travail, notamment les enquêtes, les poursuites judiciaires et les processus opérationnels. Il est par exemple important d'actualiser et d'adapter les traités d'entraide judiciaire (TEJ). Ces traités sont des accords (unilatéraux ou multilatéraux) conclus entre plusieurs États pour échanger des informations se rapportant à une enquête. Les Alliés devraient également essayer de conclure des TEJ avec les pays qui suscitent des inquiétudes, même si la tâche sera difficile lorsque les pays en question ne partagent pas le même sentiment d'urgence ou les mêmes valeurs en ce qui concerne le contrôle des technologies de chiffrement.

C. NOUVELLES LOIS ET RÉGLEMENTATIONS

59. Dans un contexte où la menace et la technologie évoluent, les gouvernements doivent passer en revue leurs lois et leurs réglementations et, le cas échéant, en adopter de **nouvelles** concernant les services de messagerie cryptée, le *dark web* ou les cryptomonnaies.

60. Dans l'ensemble des pays de l'Alliance, des débats animés ont lieu au sujet des lois sur la **conservation des données et des métadonnées**. Cette question est source de nombreuses divergences politiques. Elle oppose fréquemment les partisans d'une forte protection de la vie privée et ceux qui considèrent que la sécurité de l'État peut et doit être renforcée en demandant aux sociétés privées de conserver des données ou des métadonnées (en plus grande quantité) sur leurs serveurs – même sous forme cryptée – et de les rendre plus facilement accessibles par les services de l'État, par exemple lors d'enquêtes. En règle générale, ces sociétés ont beaucoup de mal à accepter ce qu'on leur demande. D'une part, elles craignent de perdre leurs clients qui se dirigeraient vers des services similaires mais plus sécurisés, en particulier celles qui sont implantées dans d'autres pays que celui qui impose la réglementation. D'autre part, un grand nombre des sociétés de haute technologie sont plus favorables à une forte protection de la vie privée et s'opposent aux nouvelles lois et réglementations qui sont adoptées dans ce domaine. Malgré la complexité des débats, les responsables politiques ne doivent pas les éviter compte tenu des risques et des menaces posés par l'extrémisme et le terrorisme.

61. Tandis que le phénomène du bitcoin poursuit son essor, les questions de fond sur la façon de **réglementer les cryptomonnaies** ne sont pas encore réglées. Il existe déjà dans les législations nationales, dans le secteur financier et dans le droit international des outils permettant de lutter efficacement contre le financement du terrorisme et il convient d'en faire la plus large utilisation possible. Cela dit, les possibilités d'adapter le cadre réglementaire et d'inciter les sociétés et les organisations du secteur des cryptomonnaies à réglementer leurs propres activités ne manquent pas. Des débats politiques ont lieu dans toute l'Alliance sur la question de l'adaptation des lois actuelles et de l'adoption de nouveaux textes en vue de réduire l'utilisation abusive des

cryptomonnaies pour le blanchiment de fonds et le financement du terrorisme. Les pays peuvent s'inspirer de ce qu'ont fait les pionniers en la matière. En dehors de l'Alliance, le Japon a globalement accepté les cryptomonnaies et il a été l'un des premiers pays à changer sa législation. Il a notamment introduit une obligation d'audit annuel, des exigences en matière de fonds propres pour les échanges en cryptomonnaies, ainsi que d'autres mesures pour lutter contre le blanchiment de fonds. De nombreux Alliés ainsi que l'Union européenne ne cessent quant à eux d'intensifier leurs efforts en la matière.

62. **Le blocage ou l'interdiction de certains services, voire d'un ensemble de technologies** (par exemple les cryptomonnaies), est une autre option parfois suggérée. Toutefois, une telle approche ne serait sans doute pas viable au-delà du court terme. Pour les individus recherchant des services de chiffrement à toute épreuve, de nombreuses alternatives existent. Lorsque la pression s'accroît sur certaines plateformes, les extrémistes et les terroristes tendent à s'adapter rapidement à la situation. Dans l'univers des services de messagerie cryptée, par exemple, « lorsqu'une plateforme devient moins avenante pour les terroristes, ces derniers migrent vers une autre plus sûre » (Stalinsky & Sosnow, 3 Janvier 2017). Au vu de ces éléments, certains experts ont préconisé la mise en place de normes ou de codes de conduite dans l'ensemble du secteur (Stalinsky & Sosnow, 3 Janvier 2017). Cependant, là aussi des problèmes apparaissent : il y aura toujours des personnes – physiques ou morales – pour répondre aux besoins des extrémistes et des terroristes. Certains États autoritaires (notamment la Chine et son « grand pare-feu ») ont essayé de se protéger complètement contre certains services, mais la méthode n'a pas fait montre de beaucoup d'efficacité et ne serait certainement pas considérée comme légale ou légitime dans les pays de l'Alliance (Buchanan, 2016).

D. AFFAIBLISSEMENT OU CIBLAGE DES TECHNOLOGIES DE CHIFFREMENT

63. Des options plus radicales et plus controversées sont parfois proposées. Une possibilité serait par exemple de **réglementer la puissance du chiffrement** en la limitant sur le marché civil tout en la maintenant à un niveau élevé dans son utilisation par les instances gouvernementales. Dans la première moitié des années 1990, les États-Unis ont utilisé pendant une courte période un système à deux volets (Buchanan, 2016) : les normes de chiffrement de haut niveau étaient légalement autorisées, mais seuls les protocoles les moins puissants pouvaient être exportés. Dans un monde où la puissance de calcul des ordinateurs et le nombre d'utilisateurs étaient faibles, un certain contrôle des technologies de chiffrement très sophistiquées était possible. En revanche, avec le développement du numérique et la mondialisation, le contrôle des logiciels de chiffrement et des algorithmes bien connus qui les sous-tendent n'est plus envisageable. Il est difficile d'imaginer comment, aujourd'hui, un tel système pourrait être efficace, réalisable et même politiquement acceptable. Cela est particulièrement vrai à mesure que les technologies émergentes ou transhorizon comme l'intelligence artificielle, l'analytique des données massives et l'informatique quantique faciliteront la mise en échec des technologies de chiffrement actuelles les plus puissantes.

64. Une autre option plus intrusive serait d'exiger que les **protocoles de chiffrement soient dotés d'une « porte dérobée »** pouvant être utilisée par les services de l'État en cas d'attaque par des malfaiteurs ou des terroristes. En théorie, lorsque les citoyens peuvent être sûrs que l'État n'abusera pas de ses pouvoirs et que les clés donnant accès à la porte dérobée – qui sont en sa possession – sont en sécurité, les utilisateurs peuvent continuer à bénéficier d'une bonne protection cryptographique (Buchanan, 2016). Cette option pourrait cependant se heurter à des difficultés insurmontables. Tout d'abord, elle requiert une très grande confiance dans les instances gouvernementales. Il est peu probable que l'opinion publique des pays de l'Alliance accepte une telle approche, qui soulève d'importantes questions concernant la protection de la vie privée. Ensuite, du point de vue technologique, il n'est pas sûr qu'un tel système puisse fonctionner. Selon certains experts, il est mathématiquement impossible d'introduire délibérément des défaillances tout en maintenant un haut niveau de sécurité. Même si c'était possible, la mise en place de portes dérobées accroît la complexité des protocoles de chiffrement, les rendant ainsi très vulnérables face à des pirates (étatiques ou non) et exposant par conséquent les citoyens à de plus grands risques

de la part de cyber malfaiteurs et de gouvernements hostiles (Buchanan, 2016). Par ailleurs, dans une telle situation, les développeurs tenteraient sans doute rapidement de concevoir de nouvelles techniques de chiffrement pour répondre à la demande croissante d'applications plus sécurisées (Moore & Rid, 2016).

V. CONCLUSIONS

65. L'objectif de ce rapport est de montrer quelles utilisations les extrémistes et les terroristes peuvent faire – et font déjà – des services de messageries cryptée, du *dark web* et des cryptomonnaies. Comme nous l'avons vu, les technologies de chiffrement présentent des avantages importants pour une grande variété d'acteurs, depuis les particuliers jusqu'à la communauté internationale dans son ensemble. Cela dit, elles ont rapidement été détournées de leur usage par des acteurs aux intentions malveillantes. Le rôle des responsables politiques et autres décideurs est donc de développer au maximum les bienfaits de ces technologies émergentes, tout en réduisant au maximum leurs risques.

66. À mesure que le paysage numérique évolue, il est indispensable que l'ensemble des parties prenantes comprennent mieux les nouvelles utilisations qui sont faites des technologies de chiffrement, ainsi que les possibilités et les dangers qu'elles présentent. Une campagne de sensibilisation et une approche proactive de la cybersécurité doivent être mises en œuvre à l'égard de l'ensemble des citoyens. Les gouvernements peuvent aider l'ensemble des parties prenantes intervenant dans ce processus avec plus de communication, de coopération et d'incitations. Par ailleurs, outre la prise de conscience, les entités qui, au sein des pouvoirs publics, des organisations ou des entreprises, sont responsables de ces questions doivent avoir suffisamment de ressources, d'équipements et de formations pour pouvoir s'adapter aux changements suscités par lesdites technologies.

67. Une surveillance policière rigoureuse et des réglementations strictes des technologies de chiffrement sont nécessaires. Toutefois, la grande difficulté dans ce contexte est, pour les démocraties libérales, de continuer à préserver les droits humains fondamentaux – comme la protection de la vie privée et la liberté d'expression – tout en relevant le défi d'assurer la protection des citoyens. Le rapporteur est d'accord avec ceux qui préconisent « une évaluation de la technologie et du chiffrement régie par des principes, mais demeurant réaliste » (Moore & Rid, 2016). Les responsables politiques doivent prendre leurs décisions en s'appuyant sur des principes de base rationnels, sur les faits et sur les possibilités / limites des technologies.

68. Le rapporteur note qu'il existe de grandes divergences politiques au sein de l'Alliance quant à une stratégie acceptable pour toute démocratie libérale sur ces questions. Il espère néanmoins que ce rapport pourra susciter un débat qui permettra de s'accorder sur un certain nombre de principes de base à adopter pour une réponse transatlantique aux défis des technologies de chiffrement. Fondamentalement, ces questions doivent toutefois être débattues au niveau national. Il n'empêche que le dialogue et la coopération à l'échelle internationale se sont avérés essentiels pour gérer certains des risques liés à ces technologies.

69. Le rapporteur souhaite émettre un ensemble de recommandations d'action concrètes à l'intention des gouvernements et des parlements des pays de l'Alliance atlantique.

- Dans toutes les réponses qui sont proposées, les droits, pouvoirs et libertés dont jouissent les citoyens doivent être reconnus, garantis, protégés et en permanence respectés.

- Les principes de proportionnalité et de gouvernement limité doivent toujours être appliqués. La vie des gens ordinaires ne doit pas être rendue impossible par des mesures disproportionnées visant à contrôler toujours plus la société au sens large.

- Toute mesure visant à empêcher les extrémistes et les terroristes d'utiliser les technologies de chiffrement doit strictement se limiter au champ de la lutte antiterroriste.

- Ces politiques doivent s'inscrire dans le cadre plus général de la lutte contre l'extrémisme violent et contre le terrorisme.

- Toutes les parties prenantes doivent posséder une bonne connaissance de la situation et des risques. Les campagnes publiques de sensibilisation et le travail gouvernemental auprès des citoyens, des militants (comme les pirates éthiques), des entreprises, des organisations, des organismes publics et d'autres acteurs sont à cet égard essentiels.

- Les parties prenantes doivent continuer à surveiller et à supprimer les contenus extrémistes et terroristes à la fois sur les services de messagerie et sur le *dark web*. La suppression d'un groupe, d'une plateforme ou d'un site internet risque de laisser place à d'autres, mais c'est la nature même du maintien de l'ordre dans les sociétés libres.

- Les services de police et les agences de renseignement doivent mener des enquêtes et des opérations poussées pour surveiller et ébranler les activités des groupes extrémistes et terroristes, et pour démanteler ces réseaux.

- Les travaux de recherche et de développement doivent être intensifiés afin de trouver des solutions technologiques permettant d'assurer une utilisation raisonnable des technologies de chiffrement, en particulier dans le domaine de l'intelligence artificielle et de l'analytique des données massives.

- L'affaiblissement systématique des techniques de chiffrement n'est pas une stratégie viable pour l'avenir, car cela mettrait en péril la sécurité de tous.

- Le dialogue et la coopération entre les services de police et les agences de renseignement doivent être intensifiés au niveau international, notamment en ce qui concerne les échanges d'informations, les enquêtes, les poursuites judiciaires et les processus opérationnels.

- Les pouvoirs des instances gouvernementales – notamment ceux des services de police, des agences de renseignement et des services de sécurité –, ainsi que leur utilisation par lesdites instances doivent faire l'objet d'un contrôle démocratique efficace et efficient, et des comptes doivent être rendus à l'opinion publique.

- L'Alliance dans son ensemble doit renoncer catégoriquement à toute activité subversive (par action ou par omission) de ses services gouvernementaux, de renseignement et de sécurité, que ce soit au niveau national, international ou supranational (par exemple en collusion avec le crime organisé et d'autres entités malveillantes, ou par le truchement d'intermédiaires nouvellement créés), qui viserait délibérément à créer, entretenir et/ou tolérer des risques ou des menaces pour la sécurité, des acteurs malveillants artificiels, des dialectiques « problème-solution » préétablies, des opérations psychologiques, des infiltrations, des faux signalements, etc. – pour quel que motif que ce soit. En d'autres termes, la fin ne doit pas justifier les moyens et cela peut en soi réduire considérablement l'ampleur des problèmes de sécurité auxquels nos citoyens et nos populations sont confrontés.

BIBLIOGRAPHIE CHOISIE

(Pour des informations plus exhaustives sur les ressources utilisées, veuillez-vous adresser au directeur de la commission des sciences et des technologies au secrétariat international de l'AP-OTAN)

Barak, Michael, *The Telegram Chat Software as an Arena of Activity to Encourage the "Lone Wolf" Phenomenon*, International Institute for Counter-Terrorism, 24 mai 2016

Bartlett, James, *The Dark Net: Inside the Digital Underworld*, London: William Heinemann, 2014

Bergman, Michael K., "White Paper: The Deep Web: Surfacing Hidden Value", in *Journal of Electronic Publishing*, vol. 7, no. 1, 2001

Besheer, Margaret, "UN: Terrorists Using 'Dark Web' in Pursuit of WMDs", *Voice of America*, 28 juin 2017

Brill, Alan & Keene, Lonnie, "Cryptocurrencies: The next Generation of Terrorist Financing?" *Defence Against Terrorism Review*, vol. 6, no. 1, 2014

Brown, Ian & Korff, Douwe,, "Terrorism and the Proportionality of Internet Surveillance", *European Journal of Criminology*, vol. 6, no. 2, 2009

Buchanan, Ben, "Cryptography and Sovereignty", *Survival*, vol. 58, no.5, 2016

Carlisle, David, *Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic*, RUSI, 2 mars 2017

Chertoff, Michael & Simon, Tobby, "Chapter Two: The Impact of the Dark Web on Internet Governance and Cyber Security", in *Cyber Security in a Volatile World*, Global Commission on Internet Governance, 2014,

Coinmarketcap, *Cryptocurrency Market Capitalizations*, n.d.,

Cypher Research Laboratories, *A Brief History of Cryptography*, 2014

Driscoll, Scott, *How Bitcoin Works Under the Hood*, Imponderable Things (Scott Driscoll's Blog), 14 juillet 2013

European Banking Authority, EBA Opinion on 'virtual currencies', 4 juillet 2014

Europol, *Changes in Modus Operandi of Islamic State Terrorist Attacks*, Europol, 18 janvier 2016

FinCEN, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, 2013

Goldman, Zachary et al., *Terrorist Use of Virtual Currencies: Containing the Potential Threat*, Centre for a New American Security, 2017

Greenberg, Andy, "Hacker Lexicon: What is Perfect Forward Secrecy?", *Wired*, 28 novembre 2016

Insite Site Staff, *IS Shifts Propaganda Archive to the Dark Web*, Insite Blog on Terrorism & Extremism, 18 novembre 2015

Jardine, Eric, "Chapter Three: The Dark Web Dilemma: TOR, Anonymity, and Online Policing", in *Cyber Security in a Volatile World*, Global Commission on Internet Governance, 2014,

Keatinge, Tom & Keen Florence, *Lone-Actor and Small Cell Terrorist Attacks: A New Front in Counter-Terrorist Finance?*, RUSI, 2017, au 7 mars 2018

Lee, Alex, *"Theresa May's Crackdown on the Internet Will Let Terror in the Backdoor"*, *The Guardian*, 20 juin 2017

Magdy, Sarah, "A Safe Space for Terrorists", *The British Journalism Review*, vol. 27, no. 4, 2016

Marr, Bernard, "A Short History Of Bitcoin And Crypto Currency Everyone Should Read", *Forbes*, 6 décembre 2017

Microsoft, *Journey Through the World Wide Web*, Microsoft, 19 juillet 2016

Moore, Daniel & Rid, Thomas, "Cryptopolitik and the Darknet", *Survival*, vol. 58, no. 1, 2016

Niglia,A., Al Sabaileh, A. , & Hammad, A., *Countering Terrorism, Preventing Radicalization and Protecting Cultural Heritage: The Role of Human Factors and Technology*, NATO, Brussels: NATO Science for Peace and Security Series, 2017

Noack, Rick, "France's Latest 'Terrorist Attack' Exposes Dark Side of Social Media", The Washington Post, 14 juin 2016

Owen, Gareth & Savage, Nick, "Chapter Four: The Tor Dark Net", in *Cyber Security in a Volatile World*, Global Commission on Internet Governance, 2015

Persi Paoli, Giacomo et al., *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web*, RAND Europe, 2017

Rosner, Yotam, London, Sean & Mendelboim, Aviad, "Backdoor Plots: The Darknet as a Field for Terrorism", *INSS Insight*, vol. 464, no. 1, 2013

Solon, Olivia, "Global Network of 'Hunters' Aim to Take Down Terrorists on the Internet", *The Guardian*, 21 juillet 2017

Stalinsky, Steven & Sosnow, R., *Germany-Based Encrypted Messaging App Telegram Emerges as Jihadis Preferred Communications Platform*, Middle East Media Research Institute, 3 janvier 2017

Stalinsky, Steven & Sosnow, R., *Jihadi Use of Encrypted Messaging App WhatsApp*, Middle East Media Research Institute, 12 septembre 2017

Stalinsky, Steven & Sosnow, R., *Switzerland-Based Encrypted ProtonMail Emerges As Popular Jihadi Platform – Especially Among ISIS Hacking Groups*, Middle East Media Research Institute, 26 octobre 2017

Statista, *Number of Monthly Active WhatsApp Users Worldwide from April 2013 to December 2017 (in Millions)*, Statista, 2018

Tor Metrics, *Servers*, Tor Metrics, 2018

UK HM Treasury & Home Office, National Risk Assessment of Money Laundering and Terrorist Financing 2017, UK HM Treasury & Home Office, 2017

US Office of Terrorist Financing and Financial Crimes, *National Terrorist Financing Risk Assessment 2015*, US Department of the Treasury, 2015

Weimann, Gabriel, "Going Dark: Terrorism on the Dark Web", *Studies in Conflict & Terrorism*, vol. 39, no.3, 2015