Trafic d'armes sur le Darkweb

LE RENOUVEAU DES MENACES INTERNATIONALES
À L'ÈRE DU NUMÉRIQUE

CATHERINE CONVERT - 2019 / 2020

SOUS LA DIRECTION DE MONSIEUR JEAN-YVES HAINE

INSTITUT LIBRE D'ÉTUDE DES RELATIONS INTERNATIONALES

ILERI
L'ECOLE DES RELATIONS INTERNATIONALES
A PARIS DEPUIS 1948

Les opinions émises dans ce mémoire sont propres à son auteur et n'engagent en rien la responsabilité de l'Institut d'Etude des Relations Internationales

Je souhaiterais remercier mon directeur de mémoire, Monsieur Jean-Yves Haine, docteur en sciences politiques et professeur à l'ILERI pour ses conseils et ses corrections pour la rédaction de ce mémoire,

Monsieur Nicolas Florquin, coordinateur de recherches au Small Arms Survey, pour son avis constructif concernant la place du Darkweb dans le trafic d'armes international,

Monsieur Giacomo Persi Paoli, responsable du programme des Nations Unies pour la sécurité et la technologie à l'UNIDIR, de m'avoir accordé de son temps pour répondre à mes questions sur l'impact du cybertrafic d'armes pour la sécurité internationale,

Monsieur Stijn Hoorens, directeur de bureau chez RAND Corporation, de m'avoir mise en relation avec des experts et chercheurs concernant le cyberespace,

Monsieur Laurent Gayard, auteur et chroniqueur, de m'avoir permis de mieux comprendre les enjeux géopolitiques et économiques du Darknet et des cryptomonnaies,

Page laissée volontairement blanche

SOMMAIRE :

LEXIQUE :

ACLU	Union Américaine pour les Libertés Civiles
AEW	Acoustic Expension Weapon (arme à expansion acoustique)
ALPC	Arme Légère et de Petit Calibre
ARPAC	Association pour le Rétablissement du Port d'Arme Citoyen
AOAV	Action On Armed Violence (Action contre la Violence Armée)
COSI	Comité permanent de coopération opérationnelle en matière de Sécurité Intérieure
DNRED	Direction Nationale du Renseignement et des Enquêtes Douanières
ECOSOC	Conseil Économique et Social
UE	Union Européenne
FBI	Federal Bureau of Investigation (Bureau Fédéral des Enquêtes)
IANSA	International Action Network on Small Arms (Réseau d'action international sur les armes légères)
IARMS	Illicit Arms Records and tracing Management System (Système de gestion des registres et du traçage des armes illicites)
IBAN	International Bank Account
ICSR	Centre International pour l'Étude de la Radicalisation et de Violence Politique
JAD	Journées d'Action Commune
NHTCU	National Hi-Tech Crime Unit
NSA	National Security Agency
OSCE	Organisation pour la Sécurité et la Coopération en Europe
PIB	Produit Intérieur Brut
SIA	Système d'Information sur les Armes
TFUE	Traité sur le Fonctionnement de l'UE
TOR	The Onion Router (Le Routeur Oignon)
UFA	Union Française des Amateurs d'Armes
VPN	Virtual Private Network (Réseau Privé Virtuel)

Page laissée volontairement blanche

INTRODUCTION

Difficile d'imaginer qu'un trafic aussi historique que celui des armes puisse être encore d'actualité, pourtant, s'il n'est pas encore répandu et reconnu comme un danger de premier plan, le cyber trafic d'armes pointe du doigt quelques vérités sur la sécurité internationale.

En 2013, Edward Snowden va mettre en place les prémices d'un cyberespace anonyme et incontrôlable. Les scandales de surveillance de masse qu'il dénonce vont lentement orienter les utilisateurs vers des réseaux cryptés et anonymes pour échapper au contrôle des autorités. Le Darknet naît de cette envie d'échapper à une surveillance massive avec le navigateur Tor par exemple. Comme tout outil possède ses dérivés nocifs, le Darknet ne va pas échapper à la règle et va devenir une gigantesque place de marché noir en plus d'être le symbole de la « cyber liberté ».

Les autorités vont alors se heurter à plusieurs obstacles dans la gestion de ce trafic d'armes : l'opinion public favorable à l'anonymat sur internet, l'expansion des réseaux internet dans les différentes régions du monde et la délocalisation de l'offre et de la demande. Le trafic d'armes sur internet devient alors une affaire de sociologie au service du maintien de l'ordre.

En effet, le XXIème siècle voit apparaître un genre de menace nouveau. Entre le terrorisme et la cybercriminalité, les guerres « non réglées » remplacent les guerres « réglées » que Christian Malis décrivait comme inscrite dans un calendrier précis, dans un territoire précis. Il n'est plus nécessaire de revenir sur les particularités de la menace terroriste, qu'on connaît trop bien pour son caractère imprévisible et difficilement localisable, à l'image des cyberattaques. La description du trafic d'armes reprend, dans les grandes lignes, les caractéristiques citées plus tôt, à la différence du profil type d'un trafiquant. S'il a été possible d'analyser en partie les profils des terroristes et d'identifier les victimes potentielles de cyberattaques, aujourd'hui, il n'est pas réellement aisé d'identifier avec exactitude le profil type d'un vendeur ou d'un acheteur d'arme illégale. En effet, que ce soit les fusillades perpétrées par des adolescents aux États-Unis, ou encore les réseaux de trafic d'armes démantelés à Torcy en Île-de-France, la gestion des trafics se fait ponctuellement, avec un retard sur les flux de marchandises, qui finissent par se perdre dans la nature, aux dépends des sécurités nationales. Il faut aussi prendre en compte le type de marchandises retrouvées sur le Darkweb, qui empêchent tout soupçon de par leur légalité dans certaines régions du monde ou encore les modifications apportées illégalement après achat par les trafiquants.

Si aujourd'hui, le cyber trafic semble concerner en grande majorité les puissances occidentales, il faut absolument être capable de lier l'expansion du numérique et les questions de droit de la population mondiale de bénéficier d'une connexion avec les différents travers que pourrait offrir ce droit dans des États instables. En effet, l'Europe se présente comme une « couveuse » de ce qui pourrait s'apparenter aux externalités négatives d'un marché numérique globalisé, en concordance avec une promotion des monnaies virtuelles. Le trafic d'armes bénéficie d'une trêve de la part des instances internationales et des autorités nationales à cause de son histoire, qu'on attribue à tort à un marché passé. La vérité montre qu'un marché illégal historique de la Guerre Froide a laissé sa place à un marché innovant qui a su exploiter les connaissances d'une nouvelle génération sur les nouvelles technologies, qui mettent en avant une transition dans laquelle les autorités traditionnelles commencent tout juste à s'atteler.

La méthodologie d'étude du trafic d'armes sur le Darknet devrait alors davantage se rapprocher de l'analyse d'une cyberattaque, en se détachant des anciennes méthodes employées dans le trafic d'armes traditionnel, hérité des années post Guerre-Froide. Il est essentiel, à l'image des nouvelles menaces, de comprendre l'intérêt d'un travail d'identification optimal exercé en amont.
Afin d'introduire à la notion de commerce sur l'internet anonyme, il convient d'expliquer trois notions principales : le Darknet, le Darkweb et le Deepweb. La définition du site Tor-Browser explique que « le deepweb est la somme de toutes les pages web qui ne sont pas trouvables par les moteurs de recherche classiques, tandis que le darkweb est la partie du deepweb qui est cachée et que seules des navigateurs darknet (comme TOR BROWSER) pourront accéder. »
Le Darknet ressemble donc à un navigateur spécial, à l'image de Google, Yahoo ou Bing, à la seule différence qu'il est le seul à donner accès à des sites web cachés, qu'on qualifie de deepweb (Wikileaks, Hiddenwiki). Le Darkweb est accessible par des liens très précis, accessibles uniquement via des navigateurs Darknet. Les sites DeepDotWeb ou Hiddenwiki donnent justement accès à ces liens précis.

Il faudra alors se demander si le trafic d'armes sur le Darknet peut représenter une nouvelle menace internationale et la manière avec laquelle il peut modifier l'identification des risques internationaux.

Ce travail de recherche va alors exposer les raisons pour lesquelles le Darknet représente une place de marché idéale pour les trafiquants, et les difficultés rencontrées par les autorités pour

le réguler. Afin d'appuyer sur l'importance de cette menace, ce mémoire va expliquer l'impact du cyber trafic d'armes dans le monde, et tenter de comprendre les raisons pour lesquelles l'Europe semble en être le plus fervent client. Il s'agira en dernier lieu de comprendre les tenants socio-économiques de ces trafics et les solutions pour y remédier.

I/ Un accès facilité aux armes illégales par le dark web :

Les réseaux cryptés et l'évolution de l'internet vont devenir des questions centrales dans le traitement des cyber menaces. Dans le cas du trafic d'armes, sa compréhension est cruciale et toute lacune peut compromettre la bonne étude d'un dossier. Que ce soient la question des monnaies virtuelles ou les nouvelles technologies permettant de rendre une adresse IP anonyme, le trafic sur le Darknet n'a jamais été autant d'actualité.

I.1 Le renouveau des transactions

Au-delà de l'évolution même des outils informatiques, il convient de revenir sur une nouvelle variante clé du trafic d'armes nouvelle génération, qui vient modifier la lecture traditionnelle de l'économie souterraine.

I.1.1 Paiement anonyme

I.1.1.1 *Bitcoin, monnaies virtuelles :*

La question des monnaies virtuelles a déjà été largement traitée dans les études contemporaines de l'économie et des risques liés au cyberespace. Pour autant, pour une lecture facilitée des points à venir, il convient de réexpliquer brièvement les raisons pour lesquelles le bitcoin et les monnaies virtuelles viennent « révolutionner » le commerce illégal, principalement dans le trafic d'armes. L'apparition de monnaies cryptées et leur usage à grande échelle date d'à peu près 2011, bien que le concept apparût en 1989 avec l'entreprise DigiCash de David Chaum. La criminalité liée aux trafics avant 2011 existait bel et bien, il s'agissait donc pour les intéressés de trouver des fraudes habiles pour brouiller les pistes des autorités. Viktor Bout, condamné le 5 avril 2012 à une peine de 25 ans, démontre bien la complexité et l'organisation irréprochable derrière le commerce illégal. Entre sociétés écrans et acquisition de compagnies aériennes pour le transport de marchandises, un tel trafic n'était pas à la portée de tous. Il

demandait trois composants essentiels : du personnel, des fonds et des contacts. Le Darknet ne finançait pas les conflits au Sierra Leone, Liberia, Afghanistan comme pouvait le faire Bout, ce qui pourrait laisser penser que le trafic d'armes requiert, aujourd'hui, moins d'attention. Pourtant, les composants fondamentaux du réseau de trafic traditionnel se modernise : le Darkweb donne accès à un réseau d'utilisateurs intéressés, où les transactions ne nécessitent plus de stratégie et de ruse particulière. Le Bitcoin, monnaie privilégiée de ces transactions, se caractérise de base par un système de chiffrage perfectionné. Tout utilisateur bénéficiant d'un compte bancaire a la possibilité d'acquérir cette monnaie, qui par la suite sera utilisée à des fins légales ou non. En plus d'assurer un anonymat lors des transactions, qui ne seront d'ailleurs jamais contrôlées par une autorité monétaire, leur acquisition se fait également en tout anonymat, bien que le fonctionnement de la blockchain[1] permette une traçabilité des transactions. Lors de la constitution d'un portefeuille BTC, le propriétaire reçoit une clé publique et une clé privée. La première, communiquée lors des transactions, pourrait se comparer à l'IBAN (International Bank Account Number) ; voici un exemple de clé publique, aujourd'hui inactif : 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa. Les clés privées, comme leur nom l'indique, ne sont connues que par le propriétaire du « brain wallet » (autre appellation du portefeuille Bitcoin). En 2011 et 2012 par exemple, Clifton Collins, alors vendeur et cultivateur de cannabis, avait eu la possibilité d'acquérir 6000 BTC. Encore à ses débuts, le BTC ne valait que 4 à 6 dollars, contre 9 271,90 dollars en juillet 2020, et en perdant l'accès à ses « brain wallet », ce sont environ 55 millions de dollars qui se volatilisent.

Une fois le portefeuille BTC constitué (ou d'une autre cryptomonnaie que préférerait le vendeur comme Monero, Ether, Ripple ou Litecoin), les achats sur le Darkweb s'apparentent à un achat sur eBay. Pour assurer la viabilité de la transaction, il est demandé au client de s'enregistrer sur le site. Une fois le montant versé, les sites de commerce du Dark Web (Cryptomarket) font appel à des services tels que Escrow[2], qui sont un tiers partie pour assurer du respect des conditions de transaction. Si le client n'a pas reçu sa commande, les fonds sont retenus par le tiers partie et le vendeur n'est pas payé. Cette procédure permet de rassurer le client sur la marchandise reçue, et permet de confirmer la fiabilité du vendeur sur les différents forums du Darkweb, où les éventuels clients peuvent échanger sur leurs préférences de fournisseurs et conseiller les novices. D'autres moyens de transaction permettent de rassurer le client sur le

[1] *« Mode de stockage et de transmission de données sous forme de blocs liés les uns aux autres et protégés contre toute modification », Blockchain France, https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/*

[2] Annexe 1

sérieux du vendeur comme, par exemple, les transactions multisignatures, de plus en plus courantes sur les cryptomarkets référencés sur l'ancien portail[3] Deepdotweb (13 Cryptomarkets sur 21 utilisent cette technologie). Il s'agit d'une technique de chiffrage demandant plusieurs entrées de clés privées pour chaque mouvement de fonds. Dans la vie courante, une telle technologie est déjà utilisée pour les transactions légales. Les banques utilisent de plus en plus la technologie d'authentification à deux-facteurs, où le propriétaire de compte est appelé à valider un virement sur son portable en plus de l'avoir validé une première fois sur son ordinateur.

La concurrence sur le Darkweb est élevée, et le manque de visibilité peut être un handicap pour les vendeurs, qui doivent alors miser sur leur réputation sur les forums dédiés. La partie la plus difficile d'une transaction sur le Darkweb, pour un novice, réside alors dans le premier achat de cryptomonnaie. Ils sont cependant assez bien aiguillés dans ces mêmes forums, qui procurent des conseils aux amateurs.

I.1.1.2 *Réseaux cryptés, difficulté de localisation :*

Le premier problème des autorités réside dans l'impossible localisation des adresses IP (Internet Protocol) ou d'un quelconque indice d'identification des vendeurs. Le Darknet, comme expliqué plus tôt, s'accède via des navigateurs qui brouillent l'identité d'un ordinateur connecté au réseau. Il est possible de faire l'expérience de la précision d'une localisation par adresse IP en se rendant sur le site *https://www.hostip.fr* par exemple. Une fois l'adresse IP modifiée à l'aide d'un VPN (Réseau Privé Virtuel), l'utilisateur reçoit une autre identification IP, qui peut le localiser dans n'importe quelle autre région du monde. Le VPN est un outil de plus en plus utilisé pour des activités même légales, pour protéger sa vie privée, ou pour tout simplement avoir accès à des sites web interdits ou inaccessibles dans le pays d'origine. On estime l'utilisation du Darknet pour des activités légales à hauteur de 97% contre seulement 3% d'activité illégales. Selon Jean-Philippe Rennard, le contrôle du Darknet et sa fermeture serait donc « illusoire »[4]. Avant d'être considéré comme une place de marché dangereuse, c'est aussi un outil permettant d'échapper aux différents contrôles : Tor est utilisé en Chine, malgré le pouvoir autoritaire en place et les différentes tentatives gouvernementales visant à contrôler la libre expression sur le Web. Pour résumer brièvement, le Darknet utilise un système d' « open source », correspondant à un « réseau collaboratif mondial ». Ce réseau est créé grâce à des

[3] Site web donnant accès à des sites du Darkweb et à des marchés illicites, clôturé en mai 2019

[4] « Vouloir fermer le Darknet est illusoire », Le Parisien, novembre 2016, https://www.leparisien.fr/societe/vouloir-fermer-le-darknet-est-illusoire-01-11-2016-6274134.php

utilisateurs partageant leurs machines et contribuant au développement de ce réseau. [5] Selon Eric Filiol, directeur de virologie et de cryptologie opérationnelles à l'ESIA, le Darknet devrait avant tout être considéré comme un internet parallèle, comprenant des protocoles différents de l'internet que l'on connaît : le routage en oignon. Les différentes machines évoquées par monsieur Rennard, servent de proxy, un serveur relais qui chiffre le message initial, qui sera ensuite décodé par un autre proxy. De ce fait, une connexion sur Tor peut être retracée, mais l'identité de l'utilisateur à l'origine de la recherche reste inconnue. Le Darknet fonctionne donc *grosso modo* de la même manière que la blockchain, précédemment expliquée pour les transactions en crypto monnaies.

L'autre difficulté, au-delà de la conception même de cet internet parallèle, est l'activisme des bénévoles, militant pour un anonymat sur internet. La participation de particuliers est donc l'élément central du bon fonctionnement du Darknet, que ce soient pour l'hébergement de proxy ou pour la longévité même du réseau. Certains grands organismes comme le NSA (National Security Agency) peuvent en effet héberger des serveurs Tor et devenir ainsi des proxys afin de retracer une connexion. Dans ces cas-là, des bénévoles agissant contre la surveillance de masse peuvent identifier ces proxys pour tenter de les fermer. Le NSA avait d'ailleurs estimé que toute personne utilisant le réseau Tor pouvait être considéré comme « extrémiste » selon Laurent Gayard. Parmi les différents « nœuds » des réseaux Darknet, on avait d'ailleurs pu identifier quelques machines émanant d'autorités gouvernementales, comme le NSA. Ces machines étaient donc rapidement identifiées et détournées. Cependant, le routage en oignon a pu être contourné pour l'arrestation de Eric Marques en 2013, ce qui montre que les autorités ne manquent pas tant de moyens de contrôle mais de légitimité politique à s'en prendre à un tel réseau, utilisé en majeure partie, pour des activités légales. Pour identifier Marques, le FBI avait lancé une quantité importante de logiciels malveillants, affectant un grand nombre de machines utilisées comme proxy pour le Darknet. Une technique efficace mais qui a été largement critiquée par l'ACLU (Union Américaine pour les Libertés Civiles). Le FBI préfère garder le secret des logiciels utilisés, bien qu'ils aient affecté des machines civiles sans discernement. Une telle mesure ne peut donc être employée qu'en cas extrême, avec un suspect identifié et reconnu pour son activité illégale, comme Eric Marques. Lorsqu'on en vient au trafic d'armes, on se heurte pourtant à des vendeurs particuliers pour qui une mesure de rupture de l'anonymat semblable à celle du FBI serait politiquement discutable.

[5] Annexe 2

I.1.1.3 *Fournisseurs indépendants promus par des plateformes de vente*

Il faut être objectif quant aux vendeurs retrouvés sur le Darkweb. Si Ross Ulbricht, fondateur de la célèbre plateforme SilkRoad, a été arrêté, ses usagers en revanche peuvent toujours jouir d'une liberté complète. De même que Eric Marques dirigeait l'entreprise cybercriminelle Freedom Hosting, à l'origine de la diffusion d'images pédopornographiques, de piratages de masse ou de conseils en blanchiment d'argent était déjà ciblé par les autorités après sa création de 2008.

Sur le Darkweb, il existe à la fois des cryptomarkets, mettant en relation plusieurs vendeurs avec une communauté de clients, comparables aux eBay et Amazon de l'internet « clair ». Généralement ces vendeurs ne possèdent pas de boutiques, et peuvent vendre occasionnellement sur le site, sans avoir de commerce illégal en tant que tel (il s'agirait d'un stock de moins de cinq armes/munitions). Ces cryptomarkets apportent un service client et une fiabilité bien plus accrue que les sites de vendeurs indépendants. Cette sécurité peut être à la fois une bonne et une mauvaise chose : elle incite les vendeurs et les acheteurs à se retrouver sur une même plateforme, comme SilkRoad, Black Hand, French Deep Market ou Freedom Hosting. L'inconvénient reste pourtant la fermeture de ces plateformes qui laissent les vendeurs s'éparpiller dans la nature sans possibilité de les retrouver dans l'immensité anonyme du Darkweb. Ce sont généralement les cryptomarkets qui vont être les premières cibles des autorités. Ross Ulbricht, simple créateur de la plateforme SilkRoad a ainsi été accusé de vente de produits illicites, face une multitude de réels vendeurs d'armes non identifiés. Il devient alors compliqué de vendre sur le Darkweb sur de grandes plateformes, ce qui peut pousser les vendeurs à vouloir créer leur propre site de vente, EuroArms, the French Armory, Alphabay, Hansa, Black Hand (démantelé en 2018) etc. [6] L'autre raison pour laquelle ces plateformes sont la principale cible est, logiquement, leur utilisation par des amateurs, pour qui l'accès à ces grands noms du commerce illégal est bien plus simple que de trouver un vendeur moins connu avec un site particulier. Il y a alors sur les cryptomarkets plus de chances de retrouver des consommateurs novices, qui n'ont pas pleinement connaissance du fonctionnement ou des adresses de confiance sur le Darkweb. On peut alors légitimement se demander la quantité de vendeurs inconnus des radars, ayant des adresses de sites non indexés et partagés à comités restreints et de confiance. Une problématique qui n'a pas encore été résolue par les autorités, qui ne peuvent pour l'instant s'atteler qu'au démantèlement de grosses plateformes. Ce travail n'est toutefois pas négligeable car il permet de dévier toutes tentatives de novices qui

[6] D'après une enquête de terrain sur le Darkweb, à travers le navigateur Tor sur le site HiddenWiki, donnant accès à des liens pour accéder à des sites non indexés.

souhaiteraient acquérir des armes. En revanche, ce n'est qu'une résolution partielle et limitée étant donné qu'on estime l'ouverture de 5 nouveaux sites pour chaque site du Darkweb démantelé.

Les « single-vendor markets », permettent aux vendeurs de ne payer aucune commission sur les gros cryptomarkets et permettent d'éviter une retenue de fonds par des services d'Escrow. Ils font généralement leur réputation sur les cryptomarkets afin de créer une clientèle solide pour créer leur propre commerce. Après la clôture de SilkRoad, la confiance des acheteurs et des vendeurs a été largement remise en question par l'émergence de fraudes bien plus que par le travail des mesures juridiques. Le développement des monnaies virtuelles et leur valorisation a mené des délinquants à demander des sommes importantes sans envoyer de commandes. Rien qu'en juillet 2020, on peut voir que les arnaques de monnaies virtuelles prennent une ampleur conséquente même sur le web « clair », comme le hack massif de comptes de personnalités publiques (comptes de Barack Obama, Bill Gates, Elon Musk). Les fraudes sur le Darkweb sont donc d'autant plus plausibles.

1.1.2 Livraison des marchandises

La question qui peut revenir assez régulièrement concernant les marchés illégaux sur le Darkweb serait alors les moyens de transport et de livraison, est-il véritablement aussi simple d'envoyer une carabine à chargement automatique Torun turque ou un fusil à chargement automatique AR-M9 libyen vers la France ?

1.1.2.1 *Moyens de transport privilégiés*

Comme expliqué plus tôt, la communication entre le vendeur et l'acheteur est largement facilitée par les forums. Généralement, le vendeur donne la possibilité à l'acheteur de choisir les services de livraison standards ou des services de dépôt à une location précise. Ce dernier éviterait à l'acheteur de passer par les services de poste et de renseigner son identité. De plus, la taille des colis implique forcément le déplacement du client vers un service de poste, qui pourrait l'exposer aux systèmes de surveillance (CCTV). Le client pourrait être tenté de renseigner une fausse identité pour la réception d'un colis, mais une telle démarche pourrait attirer l'attention sur un colis potentiellement suspect, signalé par les services postiers. Les vendeurs alertent également sur le risque d'un colis bénéficiant d'un suivi, qui pourrait donner

aux autorités de maintien de l'ordre la possibilité d'une enquête à grande échelle ou encore d'organiser des audits sur les suivis de colis pour tenter de localiser les vendeurs.

Le moyen de livraison privilégié devient donc le « dead drop ». Ce service implique l'intervention d'une personne supplémentaire dans la transaction, ce qui peut également menacer l'identité du vendeur. Le « dropman » livre un colis préalablement emballé, afin qu'il n'ait aucune connaissance du contenu du colis, dans un lieu hors connexion, sans système de surveillance et plutôt discret. Il lui suffit alors simplement de communiquer les coordonnées GPS exactes de l'emplacement de la marchandise. L'acheteur paye alors une commission pour le dropman sur les services escrow une fois la marchandise récupérée. L'ampleur de l'utilisation de ce mode de livraison est encore inconnue, mais il est possible qu'il s'étende à mesure que les autorités contrôlent les douanes et services de poste. Il est également utile dans le cadre d'une vente d'arme volumineuse ou d'armes à feu, plus lourdes et davantage repérable que l'envoi de drogues par la poste.

Le système de « dead drop » est optimal si le vendeur et l'acheteur sont sur un même territoire. Dans le cas d'une transaction internationale, les marchandises sont transportées par fret maritime. Les vendeurs peuvent, par exemple, cacher leurs armes dans les containers de consoles de jeu, de disques durs, de télévisions ou de nourriture. Le vendeur enveloppe à chaque fois les produits dans du plastique puis dans des sacs en Mylar avant de les déguiser dans des emballages alimentaires. Il est indispensable pour le vendeur d'avoir des contacts et un réseau pour prendre en charge les marchandises et les acheminer sans encombre jusqu'au client.

Le trafic d'armes par voie aérienne concerne avant tout le trafic de pièce détachées, avec le perfectionnement des technologies de sécurité douanière le transit d'armes complètes seraient vain. De nombreux colis sont saisis dans les plateformes de frets aériens pour des pièces de rechange, notamment à Roissy où les autorités ont pu intercepter trois colis contenant trente culasses, guides, tiges guides et ressorts récupérateurs de pistolet Beretta 92 S en février-mars 2019. Si à l'aube du trafic d'armes, à partir de 1947 en Europe jusque dans les années 1990-2000, le trafic d'armes de masse pouvait opérer librement sans subir de pression des autorités, aujourd'hui, selon Jean-Charles Antoine, le contrôle des frontières et des services postiers oblige une adaptation des vendeurs. Cette actualisation du trafic d'armes concerne essentiellement le mode de livraison et les techniques de transport. On privilégie ainsi l'envoi de plusieurs colis plutôt qu'un seul. [7]

[7] Antoine. J-C, « Frontières et trafic d'armes », Diploweb, mars 2015, https://www.diploweb.com/Frontieres-et-trafic-d-armes.html

1.1.2.2 *Contrôles de douane et repérage des frontières accessibles*

Si des progrès ont été faits en termes de livraison, il ne faut pas non plus négliger l'importance de contacts physiques dans le trafic d'armes en Europe. La prise de contact sur le Darknet ne suffit pas à assurer la globalité d'une transaction. Ainsi Jean-Charles Antoine explique la place qu'occupe toujours la corruption dans le trafic en Europe[8]. Dans les années 1990, la guerre en Bosnie-Herzégovine ou encore le conflit au Kosovo ont largement contribué à l'effacement de frontières et au passage de marchandises illégales, des armes à feu et des munitions, qui se retrouvaient alors en grande quantité au sein des populations croates, kosovares, serbes, bosniaques et albanaises. Bien que les Balkans ne fissent pas partie de l'espace Schengen, ces marchandises ont pu l'intégrer sans trop de problèmes grâce à l'importante diaspora qui s'était développée en Europe. La création de trafic d'armes remonte donc du passé conflictuel aux Balkans et au développement de la délinquance dans les banlieues de l'Europe Occidentale pour le trafic de drogues. Un scénario similaire s'est développé en territoire africain, dans la région sahélienne mais aussi avec l'émergence des Printemps Arabes qui ont fait augmenter la demande d'armes en développant le « gangsterterrorisme »[9]. Il faut aussi noter l'absence de contrôles aux frontières dans ces régions conflictuelles qui ont permis l'émergence de convois routiers transportant d'importantes quantités d'armes d'un pays à l'autre. Parallèlement au développement de diasporas en Europe Occidentale issus de régions conflictuelles, le développement du commerce international, du flux d'individus et de marchandises ont permis de quintupler la quantité de marchandises échangées dans le monde par voies maritime et aérienne. Ainsi, en 1990 on estimait le commerce maritime à 4 milliards de tonnes par an de marchandise, contre environ 15 milliards de tonnes aux alentours de 2020 selon Florent Detroy. Au-delà de l'impact des diasporas et du développement du commerce international, il faut également comprendre l'impact de la corruption dans le recel d'armes en Europe. Selon le Rapport Transparency International 2009, la perception de la corruption est particulièrement marquée en Ukraine, Biélorussie, Lituanie, Moldavie et Rouamanie. C'est aussi dans ces régions que le rapport souligne l'existence de services douaniers faisant preuve d'une corruption active ou passive importante. On relève plusieurs frontières donnant directement accès aux États de l'Union Européenne. La frontière ukrainienne est l'une des plus importantes frontières corrompues en Europe et on y identifie plusieurs flux illégaux dissimulant des trafics d'armes légères et de petit calibre (ALPC) vers la Pologne, la République tchèque et la Hongrie.

[8] Annexe 3

[9] Antoine. J-C, « Frontières et trafic d'armes », Diploweb, mars 2015, https://www.diploweb.com/Frontieres-et-trafic-d-armes.html

Il faut aussi noter la porosité des frontières entre l'Ukraine, la Moldavie et la Roumanie, bien que le rapport ne fasse aucune mention de flux massifs d'ALPC entre ces trois pays. Une fois les armes entrées en Europe, le rapport énumère plusieurs agglomérations sujettes à une taux important de corruption. En Ukraine d'abord avec Kiev, Odessa et Lviv, les villes roumaines et bulgares Constanta, Varna et Sofia, Istanbul en Turquie, Vlora en Albanie, Milan en Italie, puis enfin les villes françaises Ajaccio, Grenoble et Marseille. Le rapport fait mention de flux d'ALPC allant d'Istanbul jusqu'à la France en prenant l'itinéraire Vlora-Bari-Milan-Marseille ou Sofia-Nis-Milan-Marseille. Lors de perquisition et de démantèlement de trafics français, la majorité des armes confisquées seront d'origine italienne et turque.

I.1.2.3 *Service de livraison privilégié*

Le recours à des services postiers n'est plus aussi simple que dans le début des années 2000. De nombreuses législations pour le transport de produits dangereux de la part des groupes privés et les technologies de détection de ces mêmes produits empêchent les vendeurs d'avoir recours aux services de UPS, GLS, Chronopost, Fedex et TNT si facilement. Les vendeurs doivent faire usage de techniques perfectionnées pour échapper aux dépistages des services postaux. Les techniques de dissimulation sont généralement à l'initiative du vendeur et comprennent l'envoi en plusieurs paquet ou une dissimulation efficace dans un emballage de produits électronique lourds, comme un carton de télévision ou de produit électroménager. Pour ce qui est de l'envoi de grenades ou de munitions, le vendeur fixe une quantité maximale par colis afin que le colis ne soit pas trop lourd pour sa taille. Ils limitent donc généralement l'envoi de trois grenades en une fois. Pour les armes envoyées en une fois, la technique privilégiée sera d'envoyer la marchandise dans une caisse d'instrument de musique par exemple. Dans d'autres cas, le vendeur demande si l'acheteur accepte que le vendeur endommage volontairement l'arme ou la démonte pour faciliter son transport. Le client doit alors accepter de recevoir une arme endommagée qui pourra servir moins longtemps qu'une arme envoyée avec plus de risques. Les armes de type Kalachnikov sont très populaires pour la façon avec laquelle elles peuvent être remontées et démontées sans problèmes et leur facilité d'entretien générale. Certains vendeurs vont également jouer sur des prix de groupe en proposant d'envoyer de la drogue et davantage de munitions dans un même colis. Selon un article du Telegram, la majorité des armes envoyées au Royaume-Uni arrivent en pièces détachées. Cette technique permet de contourner les législations des services postiers, refusant l'envoi d'armes entières et complètes sans permis adéquat, cette « faille » permet de passer outre le contrôle des douanes et de la

surveillance des services de livraison. Beaucoup de pièces détachées d'armes peuvent ainsi transiter grâce aux services de livraison comme la Poste.

I.2 Mondialisation des télécommunications

L'autre variable essentielle au commerce illégal est l'établissement d'un contact et d'une confiance de la part des deux partis. Que ce soit l'acheteur souhaitant dépenser ses bitcoins et recevoir sa marchandise ou le vendeur qui peut soupçonner un agent du maintien de l'ordre, la correspondance doit convaincre chacune des partie-prenante.

I.2.1 Communication acheteur/vendeur

La communication va représenter une part importante du trafic illégal d'armes sur le Darknet. C'est aussi au travers d'autres outils comme les réseaux sociaux et plateformes de communication que les acheteurs vont pouvoir entrer en contact avec des vendeurs. Il n'y plus besoin de se déplacer de son salon pour obtenir des armes, drogues, munitions sur internet.

I.2.1.1 *Réseaux privilégiés de mise en vente : Facebook, Whatsapp, Snapchat, Telegram, Silk Road*

Lorsque Jean-Philippe Rennard expliquait que la fermeture du Darknet serait illusoire, c'est aussi en raison de l'importance de l'internet clair dans l'établissement du trafic d'armes. S'il faut fermer le Darknet à cause du commerce illégal, il faudrait appliquer la même sanction à Facebook, Snapachat, Instagram ou encore Whatsapp, ce qui serait difficilement explicable à la majorité d'utilisateurs innocents et ignorant les autres usages de ces plateformes. Facebook représente une place de marché monumentale, contre laquelle les autorités américaines ont tenté d'apporter une réponse en collaboration avec la société américaine sans pouvoir réellement apporter de solution durable. Le cas de la Libye est intéressant dans le rôle de Facebook dans le trafic d'armes. Pendant le gouvernement de Kadhafi, celui-ci régulait le commerce d'armes sur son territoire tout comme il contrôlait et interdisait les trafics illégaux. Les sanctions des Nations Unies ont également mis un frein aux exportations légales d'armes libyennes entre 1992 et 2003, ce qui a contribué à augmenter la quantité d'armes inutilisées en Libye et donc leur stockage. Le besoin important du gouvernement de Kadhafi en armes après l'embargo lui a valu plusieurs contrats avec la France ou encore la Belgique à partir de 2004. En 2008 la France décroche un contrat de 168 millions d'euros pour la fourniture de missiles antichar

Milan : « Les Libyens vont dépenser quelques centaines de millions d'euro pour faire fonctionner les entreprises en France, qu'est-ce qu'on me reproche ? De trouver des contrats ? » disait Nicolas Sarkozy le 6 août 2007 sur Journal Télévisé France 2. En Belgique, 3000 armes étaient stockées dans des entrepôts belges après que le gouvernement ait interdit toute exportation d'armes vers la Libye, craignant la vente d'armes vers des pays subissant des embargos ou vers des bandes irrégulières. A la suite de la chute du régime de Kadhafi en 2011, l'utilisation des réseaux sociaux explose, notamment celle de Facebook. La création de groupes fermés ou secrets sur Facebook empêche les autorités ou parfois même Facebook de s'introduire dans ces réseaux, dont le contrôle repose généralement sur les signalements d'autres utilisateurs. D'autres exemples de l'impact de Facebook dans la revente d'armes devraient montrer que le Darkweb n'est pas le seul responsable du trafic, comme tentait de le montrer deux journalistes américains en 2014, parvenant à acquérir une arme illégalement sur un groupe tel que « Guns for Sale », « I Love Guns » ou « Guns, Ammo & Blades », ouverts au public après demande d'adhésion, aujourd'hui signalés et fermés. Rien n'empêche par la suite de revendre ces armes dans des « cryptomarkets », où elles pourront être achetées en tout anonymat via des monnaies virtuelles et des porte-monnaie anonymes sans avoir besoin de se rencontrer pour une transaction en liquide.) D'autres « vitrines » pouvaient être visibles sur Instagram, des comptes privés qui servaient également à exposer les articles à vendre, comprenant des mitrailleuses, des Kalachnikov, des missiles antichars, des lance-roquette. Les transactions se faisaient via Bictoin comme sur le Darkweb. A l'heure actuelle, on peut également se questionner sur la suite du trafic d'armes vers la Libye depuis la Turquie, que l'Union Européenne tente d'enrayer grâce à une opération navale en Méditerranée. Quel sera l'avenir de toutes ces armes turques envoyées illégalement par voie routière ou navale vers la Libye ?

D'autres réseaux servent à la vente d'armes comme Whatsapp, dont l'interception de discussions par la police ont permis d'arrêter en 2019 un vendeur d'armes à Tourcoing. Une perquisition qui avait mené à la confiscation d'un pistolet 9 millimètres et un fusil de calibre 222. Plus récemment en mai 2020, un trafic d'armes à également pu être démantelé à Fort-de-France, où le vendeur se servait de Whatsapp avec son entourage proche et d'autres individus intéressés sur une conversation privée, pour vendre des armes. Lors de la saisie de son véhicule, on y découvre des armes légères, des munitions et cartouches de catégorie B et autre matériel. Ce trafic était en partie dû à l'activité d'armurier clandestine d'un des prévenus.

Si ces réseaux sont autant privilégiés, c'est parce qu'ils permettent de faire rencontrer l'offre et la demande. Sur Facebook en Libye, l'offre importante rencontrait également une demande

élevée, qui n'aurait été possible que par bouche à oreille dans le cas d'un marché noir physique. Si Whatsapp, Snapchat et Telegram, des services de messagerie, appellent à la discrétion des vendeurs et permettent de ne communiquer qu'avec des intéressés, rien n'empêche par la suite à ces vendeurs de prendre le Darkweb en main et d'y vendre leurs marchandises sur les cryptomarkets. D'autres pays suivent le même modèle que la Libye comme la Syrie, l'Irak, le Yémen. Une façon de toucher une clientèle internationale et de prendre facilement contact avec les acheteurs pour le règlement des détails connexes (mode de livraison privilégié, adresse, modalités de paiement, conditions de vente et service après-vente, options de remboursement etc.)

I.2.1.2 *Communication facilitée par les nouvelles applications chiffrées*

Les commerces illégaux sont largement facilités par les applications. Le principe de « story » Snapchat par exemple permet de faire disparaître une publication en vingt-quatre heures, et visible facilement par tous les contacts du compte. Pour le cas de Whatsapp et Telegram, les autorités se heurtent à la technologie de chiffrement de bout en bout (End-to-end encryption, ou E2EE). Au même titre que la popularité grandissante du Darknet pour l'anonymat qu'il confère, des services de messagerie tels que Signal (utilisé et promu par Edward Snowden) deviennent de plus en plus utilisés. Ces applications en open source permettent à tous les utilisateurs de comprendre son fonctionnement et avoir accès aux codes sources, facilitant ainsi l'identification de failles par les utilisateurs et empêche les autorités d'intercepter une conversation avec des méthodes simples. En comparaison, Whatsapp ne permet d'accéder qu'à une partie du code de l'application, ce qui laisse plus de possibilités aux forces de police. De plus en plus d'applications chiffrées se développement après les scandales relatifs à la vie privée des utilisateurs. Signal a été créée par le cofondateur de Whatsapp, qui était en désaccord avec Mark Zuckerberg sur les questions de vie privée. Aujourd'hui, des applications comme Wire, Keybase, Protonmail, Telegram voient le jour avec des codes sources régulièrement audité par des experts en cybersécurité. Si de telles applications sont cruciales pour la protection des données et de la vie privée, elles créent un instrument parfait pour la prolifération de commerces illégaux. On assiste à une concurrence de plus en plus accrue pour la vente de drogue, obligeant les vendeurs à travailler leur communication. Le trafic d'armes voit également la concurrence émerger, coïncidant avec le besoin des délinquants de protéger leur activité des rivaux. Le trafic d'armes est intimement lié au trafic de drogues, et les moyens employés pour promouvoir les marchandises sont comparables en tout point, à la différence d'une demande moins importante pour les armes.

I.2.1.3 *Marketing et ciblage de clientèle par les vendeurs*

S'attaquer aux services de messagerie pour enrayer le trafic devient alors une stratégie habile. Que ce soient les publications éphémères ou chiffrées, les trafiquants trouvent bien plus leur bonheur dans les nouveaux modes de communication que les autorités, qui tentent de s'adapter à une « ubérisation » du trafic, consistant à mettre professionnels et clients en contact direct. Une stratégie marketing de plus en plus utilisée dans les commerces licites, mais largement maîtrisée par les vendeurs de drogues ou d'armes. Maître Céline Tavenard, avocate d'un des prévenus dans l'affaire « Shit and Co », expliquait à quel point les réseaux sociaux permettaient à ces « entrepreneurs » de créer des micro structures, reprenant trait pour trait la structure d'une jeune entreprise dynamique : « comme dans une société classique, il y avait un secrétariat, un service de ressources humaines et de communication ». Une organisation qui permet de faire grimper les chiffres d'affaire jusqu'à 50 000 euros par mois[10]. Ces petites structures sont également tenues par des jeunes adultes de moins de 30 ans, ce qui explique l'adaptabilité de leur commerce et leur portée. La multiplication des services de messagerie et la démocratisation des nouvelles technologies confrontent les trafics illégaux aux mêmes défis que les commerces classiques, avec une offre de plus en plus grande pour une demande de plus en plus grande. L'affaire Shit & Co montre une stratégie marketing imparable nécessitant une étude de marché assidue ainsi qu'une approche commerciale offensive, pouvant souvent mener à des insécurités dans les régions pivots des trafics. De fil en aiguille, la demande d'armes légères augmente pour remédier à la concurrence que les réseaux créent.

I.2.2 Expansion des connexions internet : un enjeu du cyberespace

Le développement des nouvelles technologies et l'écart générationnel qu'elles créent dans l'approche du maintien de l'ordre rendent la gestion du trafic d'armes difficile. C'est aussi les modifications qu'elle apportent dans les comportements et les sociologies qui pourraient inquiéter sur l'avenir des trafics illégaux et leur popularité dans les différents milieux et couches sociales.

[10] Paolini E, Lepoivre A, « Snapchat, Whatsapp : les nouveaux codes du deal 2.0 », BFMTV, août 2019, https://www.bfmtv.com/police-justice/snapchat-whats-app-les-nouveaux-codes-du-deal-2-0_AV-201908020036.html

I.2.2.1 *Marché criminel accessible aux mineurs*

Il faut tout d'abord mentionner l'accès facilité aux technologies pour les mineurs, qui peuvent se retrouver, par curiosité, sur des sites de vente de drogues ou d'armes sur les réseaux sociaux ou encore en ayant accès au Darkweb. On estime qu'un enfant ira s'aventurer sur le web entre 12 ans et 15 ans[11], pour finir par être sensibilisé et accoutumé au fonctionnement du commerce illégal. A partir de 16 ans, un mineur peut, avec l'autorisation de ses parents, ouvrir un compte en banque. C'est donc à partir de cet âge qu'un mineur peut avoir accès à ses premiers Bitcoins, en étant accompagné sur différents forums du Darknet, sur lesquels il aura déjà pu s'informer des procédures à suivre pour l'acquisition d'une telle monnaie. Si les dernières années n'ont pas permis de démontrer l'impact des réseaux cryptés sur les activités des jeunes sur le Darkweb, on peut s'attendre dans les prochaines années à une meilleure connaissance des technologies de Blockchain et de monnaies virtuelles, qui pourraient représenter une menace dans la sécurité de ces jeunes utilisateurs. Comme l'explique Jean-Paul Pinte, Maître de conférence à l'Université Catholique de Lille, le Darkweb pourrait représenter « un défi pouvant faire monter en eux une certaine forme d'excitation, d'un pouvoir de toute puissance. Pouvoir se fournir en drogues sur le Dark Web en représente l'apothéose. » En d'autres termes, les mineurs ayant accès à ces sites peuvent être motivés par des pressions de groupe, en n'ayant pas encore connaissance des risques de telles transactions. La promotion faite des monnaies virtuelles peut alors empêcher ces jeunes à comprendre les risques d'arnaque, de piratage ou de tout simplement ignorer la qualité douteuse d'une marchandise achetée. Il peut alors sembler important de comprendre et expliquer la curiosité des jeunes pour les nouvelles technologies afin de les guider intelligemment dans leur comportement sur le web. Le risque principal serait un déséquilibre entre la connaissance des jeunes des réseaux face à un corps de police davantage basé sur la répression de comportements illégaux plutôt que leur explication. Les questions relatives à la protection de la vie privée, qui étaient abordées dans les années 2010 avec l'expansion de Facebook, devrait aujourd'hui se moderniser et s'adapter à de nouveaux outils qui tendent à se propager dans les différentes tranches d'âge. S'il est impossible d'interdire l'accès au réseau Tor, on peut néanmoins expliquer comment l'utiliser sans s'exposer à un danger.

[11] Pinte, J-P. « Les jeunes et le Dark Web », *Terminal*, décembre 2018, consulté le 24 juillet 2020, http://journals.openedition.org/terminal/3278 ; DOI : https://doi.org/10.4000/terminal.3278

1.2.2.2 *Impact des communications transnationales sur le sentiment d'insécurité*

Si Jean-Paul Pinte explique que le trafic de drogue sur le Darkweb concerne avant tout une clientèle nationale, le trafic d'armes répond à une logique différente. Comme évoqué plus tôt, les armes du trafic viennent d'Europe de l'Est, de Libye, Syrie et autres régions marquées par des conflits armés. En ce qui concerne les membres de l'Union Européenne, et plus particulièrement la France, l'Allemagne, l'Italie et l'Espagne, l'absence de conflits armés et le contrôle assidu des stocks d'armes empêche l'exportation d'armes européennes vers les autres pays frontaliers. L'Europe est avant tout importatrice, ce qui implique une communication internationale avec des vendeurs d'armes par des particuliers.

Dans le cas du terrorisme en Europe, l'utilisation des réseaux sociaux et des messageries a sans aucun doute joué en la faveur de l'acquisition d'armes de la part de jeunes radicalisés, qui ont en grande partie été abordés par ces mêmes réseaux dans le cadre de leur radicalisation. Dans le cas du trafic d'armes sur le Darkweb, la communication transfrontalière devient un composant clé, dont la portée croit à mesure que de nouvelles possibilités de communication voient le jour. On peut voir des systèmes de messagerie sur différentes plateformes de jeux en ligne ou encore des forums avec système de messagerie privée facilitant une prise de contact directe avec des jeunes fragilisés. S'il ne faut pas considérer chaque communication comme une tare de la mondialisation, il est vraisemblable que la mise en relation d'individus de régions différentes amène des problématiques nouvelles impliquant la répercussion d'une insécurité dans un pays vers un autre. Selon Isabelle Veyrat-Masson, le sentiment d'insécurité naît depuis les années 1970 avec la diffusion de faits divers. La diffusion de nouvelles images du monde entier, concernant le terrorisme, la criminalité peut également faire monter un sentiment d'insécurité en Europe. En 2015 et 2016 les attentats successifs en France et Royaume-Unis ont accentué un sentiment d'insécurité bien que les attentats existassent déjà depuis les années 1960 et 1970 en Europe. Comme Grégory Derville l'explique dans *Le pouvoir des médias : mythes et réalités*, les médias ont contribué à la « création [d'une] réalité »[12] en présentant un danger omniprésent en Europe. Charlie Hebdo, par exemple, a donc poussé les Français à s'intéresser à l'acquisition d'une arme sur le Darkweb. Les déclarations de Alain Marsaud en janvier 2016 sur le plateau de iTélé, admettant posséder une arme pour ne pas laisser les « assassins » être seuls possesseurs d'armes à feu a pu être partagé par son électorat. Les réseaux sociaux sont également un milieu faiblement régulé, qui a vu de nombreuses incitations à la haine se développer ainsi que la propagation d'informations infondées et fausses, contribuant à un

[12] Derville G, *Le pouvoir des médias : mythes et réalités*, *2ème édition revue et augmentée*, PUG, 2005, pp. 69

sentiment général d'insécurité, pouvant pousser à un intérêt pour les armes. En 2016, on observe un intérêt croissant des Français pour les armes à feu, augmentant la fréquentation de stands de tir de 40%[13]. La popularité de l'ARPAC (Association pour le Rétablissement du Port d'Arme Citoyen) témoigne également d'une volonté de réarmer les citoyens en passant de 15000 adhérants sur la page Facebook en 2016[14] à plus de 40 000 en 2020.

1.2.2.3 *Cour des Droits de l'Homme : démocratiser l'usage d'internet et garantie d'accès aux réseaux pour toute la population*

Si l'accès aux armes est facilité par l'accès au web, on pourrait se demander si les récents progrès en termes de législation de l'accès internet ne faciliterait pas encore davantage ces acquisitions. En 2019, les agences We Are Social et Hootsuite publient un rapport annuel sur la part de population connectée à internet (via téléphones portables ou ordinateurs), et estiment à 57% la part de la population mondiale y ayant accès[15]. L'étude de Max Roser, Hannah Ritchie et Esteban Ortiz Ospina pour Our World in Data montre également des connexions internet en expansion, surtout dans les pays en voie de développement[1617]. Face à cette évolution des connexions, la législation évolue tout comme la notion de Droit de l'Homme appliqué à l'accès internet. Une évolution nécessaire au vu du récent projet Starlink d'Elon Musk, censé également apporter une connexion viable aux régions reculées.

En juillet 2016, le Conseil des Droits de l'Homme « condamne les restrictions à l'accès à l'information sur internet ». Une étape clé dans le développement de l'accès à Tor et au Darkweb, dans la mesure où de nombreux États incluant la Chine, la Russie, le Bangladesh, le Kenya, l'Inde, l'Indonésie, l'Afrique du Sud, le Burundi, Cuba ou encore le Qatar ont semblé émettre des réserves sur une telle résolution. Ces positions questionnent sur la proportion de la population étant capable de se rendre sur le Darkweb sans y être autorisé légalement par la politique de leur pays. Un droit international prônant alors le libre accès à l'information suggérerait davantage de liberté sur le web et donc une plus grande utilisation de sites web cryptés, potentiellement revendeurs d'armes à travers des navigateurs anonymes interdits.

---

[13] « Enquête sur ces Français qui veulent s'armer », L'Obs, octobre 2016, https://www.nouvelobs.com/societe/20161031.OBS0569/enquete-sur-ces-francais-qui-veulent-s-armer.html

[14] E.Paolini, « Ces Français qui revendiquent leur droit à disposer d'une arme à feu », le Figaro, novembre 2016, https://www.lefigaro.fr/actualite-france/2016/11/15/01016-20161115ARTFIG00108-ces-francais-qui-revendiquent-leur-droit-a-disposer-d-une-arme-a-feu.php

[15] « Digital 2020 : global digital overveiw », We Are Social et Hootsuite, janvier 2020, https://datareportal.com/reports/digital-2019-global-digital-overview

[16] Annexe 4

[17] Roser M, Ritchie H, Ortiz-Ospina E, « internet », Our World in Data, 2020, https://ourworldindata.org/internet#citation

En France, le code de l'action sociale et des familles ainsi que la loi du 31 mars 1990 sont également révisés avec la loi pour le numérique adoptée par le Sénat le mercredi 28 septembre 2016, visant à maintenir les connexions internet des utilisateurs même s'ils ne sont plus en mesure de le payer. Bien que les connexions se multiplient, il existe bien un « fossé numérique » qui, accentue les inégalités entre les pays riches et les pays pauvres, selon la Banque Mondiale. Kaushik Basu, chef économique de la Banque Mondiale en 2016, met alors en garde sur le risque de la création d'une « nouvelle classe socialement marginalisée » du fait des retards du numériques dans certaines régions.[18] La décennie 2020-2030 pourrait être dédiée au développement d'une ère numérique, en étroite collaboration avec des entrepreneurs comme Elon Musk. Il faudrait alors s'interroger sur les outils que possèdent les autorités concernant le contrôle de la cybercriminalité et les violations des lois qui pourraient en découler. Un accès global et brutal à internet des 40% restant pourrait avoir d'importantes conséquences sur la régulation du cyberespace.

Avec le développement de l'accès internet et des cryptomonnaies, il faudrait comprendre à quelles marchandises la population peut avoir accès et les raisons pour lesquelles elles peuvent représenter une menace non négligeable dans les pays en développement et développés.

II/ Estimation du marché de l'armement illégal sur le Darkweb

Le seul danger du Darkweb ne réside pas uniquement dans sa facilité d'accès ou la dangerosité des armes qu'on peut y trouver. Ce qui tend à inquiéter les chercheurs spécialisés en trafic d'armes comme Jean-Charles Antoine se trouve davantage dans la légalité des armes retrouvées lors des perquisitions, ou encore la reconversion d'armes considérées comme de simples objets d'art/collection par la loi.

II.1 Identification des armes échangées et de leur clientèle

II.1.1 Les différents types d'armes retrouvées sur le marché

[18] « Plus de 4 milliards de personnes n'ont pas accès à Internet », le Figaro, janvier 2016, https://www.lefigaro.fr/secteur/high-tech/2016/01/14/32001-20160114ARTFIG00078-plus-de-4-milliards-de-personnes-n-ont-pas-acces-a-internet.php

Le mythe selon lequel n'importe quel particulier pourrait se procurer une AK-47 ou un FAMAS sur le Darkweb n'est pas à considérer comme une réalité absolue. Ces armes circulent bien sur différents réseaux de vente, mais ce ne sont pas les principales marchandises qu'un individu chercherait à se procurer. Lorsqu'on souhaite acheter sur le Darkweb, le mot d'ordre est avant tout la discrétion, ce qui rend la livraison d'une arme volumineuse non neutralisée risquée.

II.1.1.1 *Armes non létales reconverties*

En plus des traditionnelles Kalachnikov, issues des Balkans, le choix des utilisateurs va se porter sur des armes non létales, accessibles sur des sites de l'internet « clair ». On retrouvera sur le Darkweb des armes d'airsoft reconverties à des fins létales. On retrouvera par exemple des pistolets à air comprimé, qui sont avant tout considérés comme des jouets dans de nombreux pays où ils sont commercialisés. Contrairement aux modèles, ces armes d'airsoft sont principalement composées de plastique, qui pourraient devenir dangereux pour les utilisateurs et les individus visés par l'arme. Une simple modification au niveau de la boîte de culasse est nécessaire, exécutée avec des pièces détachées d'armes létales, dont la circulation hors-frontières n'est pas toujours régulée, tout comme la carcasse d'armes létales. On trouve d'ailleurs beaucoup de boîtier de culasse d'occasion d'une variété d'armes conséquente (carabines Wintchester, Magnum, fusil Berthier etc) sur des sites tels que NaturaBuy, qui ne fait même pas partie du Darkweb. De plus, la montée en popularité des sports d'airsoft poussent les fabriquant à perfectionner leurs répliques, y ajoutant des pièces métalliques ou se rapprochant de plus en plus de véritables armes. C'était le cas d'AR-15 factices produits en Chine, où les pièces anciennement en plastique de la partie inférieure de la boîte de culasse étaient devenues métalliques. Les modifications pour en faire des armes létales deviennent alors moindres.

Il y aura également certains pistolets d'alarmes, principalement turcs et italiens, qui ont été reconnus pour être facilement modulables et modifiables pour en faire de véritables armes d'appoint. Parmi les modèles fréquemment identifiés, on retrouve le Tanfoglio GT 28, le Kimar, le Ekol Tuna, Volga, Jackal Dual[19]. Ces derniers sont bien plus susceptibles d'être convertis étant donné qu'elles sont censées imiter à la perfection une arme létale. Ils sont donc confectionnés avec les matériaux d'une véritable arme, avec un mécanisme modifié pour qu'il ne puisse pas tirer de munitions. Les armes « front-venting » sont particulièrement prisées vu

[19] Florquin N, King B, « Quand le légal devient létal : les armes à feu converties en Europe », Rapport, Small Arms Survey, avril 2018

qu'elles sont utilisées dans le monde du cinéma, mais ne sont pas facilement accessible au public. Elles évacuent les gaz par le canon et les fabricants, soucieux de leur conversion, dévient le canon de la chambre. En 2015, un Allemand avait procédé à la modification d'armes d'alarme qu'il avait par la suite vendu sur internet[20]. Après la perquisition du domicile du vendeur, un lien a pu être établi avec les armes utilisées dans les attentats de Paris la même année. Ce type d'armes est d'ailleurs en vogue chez les petits délinquants, qui privilégieront un réseau clos et de confiance pour pouvoir convertir des armes en toute discrétion et les distribuer à des contacts de confiance. Ces armes arrivent alors rarement sur le Darkweb bien que leur présence ne soit pas exclue, comme en témoigne l'enquête saisie par le parquet de Stuttgart et le vendeur de 24 ans Sascha W.

II.1.1.2 *Armes létales neutralisées reconditionnées*

L'autre point d'inquiétude des autorités en matière de trafic concerne les capacités des délinquants à reconditionner des armes anciennes, qui peuvent alors franchir les frontières en étant considérées comme objets d'antiquité ou de collection. Comme l'explique Virginie Rozière, eurodéputée s'exprimant sur la directive de l'Union Européenne sur les armes à feu, il existe des lacunes dans les textes de lois. Il faudrait améliorer la traçabilité des armes, aujourd'hui obligatoire que pendant 20 ans, en la rendant obligatoire jusqu'à la destruction de l'arme.[21] Une telle législation permettrait de résoudre le problème des armes anciennes. En 2012, la perquisition du domicile de Mohamed Merah permet d'identifier un pistolet mitrailleur datant de la Deuxième Guerre Mondiale et un pistolet Remington fabriqué en 1942. Il en va de même pour l'attentat Charlie Hebdo, où des fusils d'assaut des années 1960 et des pistolets des années 1950 ont été identifiés.[22]Ce sont des armes pouvant être acquises par voie légale, bien que la neutralisation soit une condition de vente d'armes à feu. En revanche, la « retroconversion »[23] d'armes anciennes représente une importante part de marchandises retrouvées sur le Darkweb. D'après la proposition de directive du Parlement Européen et du Conseil relative au contrôle de l'acquisition et de la détention d'armes du 19 février 2020, peut

[20] « Attentats de Paris : des armes utilisées ont été achetées en Allemagne », Le Point, novembre 2015, https://www.lepoint.fr/monde/attentats-de-paris-des-armes-utilisees-ont-ete-achetees-en-allemagne-27-11-2015-1985382_24.php

[21] Gardette H, « Comment les armes se retrouvent-elles dans les mains des terroristes », émission Du Grain à Moudre du 25 mars 2016, France Culture, https://www.franceculture.fr/emissions/du-grain-moudre/comment-les-armes-se-retrouvent-elles-dans-les-mains-des-terroristes

[22] « Vendre et acheter des armes en Europe : où en est-on ? », France Inter, émission du 24 mars 2016, https://www.franceinter.fr/emissions/l-eco-du-matin/l-eco-du-matin-24-mars-2016

[23] Florquin N, King B, « Quand le légal devient létal : les armes à feu converties en Europe », Rapport, Small Arms Survey, avril 2018

être considéré comme « armes à feu neutralisées » « les armes à feu qui ont été mises hors d'usage par une neutralisation, qui assure que toutes les parties essentielles de l'arme à feu en question ont été rendues définitivement inutilisables et impossibles à enlever, remplacer ou modifier en vue d'une réactivation quelconque de l'arme à feu »[24]. Les mesures de neutralisation présentent une grande disparité parmi les membres de l'Union Européenne, ce qui rendrait une retroconversion bien moins laborieuse que la neutralisation elle-même. Cette disparité de contrôle prend des proportions sécuritaires importantes. En premier lieu, cette mesure permet aux États d'inciter les civils à acheter des armes et ainsi épuiser les stocks d'armes en excédent dans les forces armées et les forces de police. Une mauvaise neutralisation rend donc ces armes légales sur le marché et facilement dangereuses pour la population. Si une majorité des particuliers faisant acquisition de ces armes les utilisent honnêtement afin de les exposer dans des musées ou pour des collections personnelles, leur commercialisation sur des sites de vente d'objet d'art ou de vente de particulier à particulier empêche un suivi précautionneux. Dans la catégorie des armes neutralisées, on retrouve les armes à expansion acoustique (AEW), qui sont les plus simples à rendre létales de nouveau. Au même titre que les armes d'alarme, elles sont en mesure de tirer des munitions à blanc, pendant que les autres armes neutralisées subissent des modifications importantes empêchant toute expulsion de projectile. Les AEW sont toutefois bien plus dangereuses et prisées que les armes d'alarmes étant donné qu'il s'agit initialement de véritables armes neutralisées, ayant donc une confection résistante, permettant d'assurer la sécurité du tireur. On retrouvera en général des produits excédentaires de l'ancienne armée tchécoslovaque comme le pistolet-mitrailleur Skorpion vz.61 ou le fusil automatique vz.58. Il y a également des armes légères comme les pistolets Glock, Makarov et PS97 Arrow. De nombreux attentats ont été perpétrés par ce type d'armes, en janvier 2015 à Paris avec l'utilisation de fusil AEW convertis, en juillet 2016 lors de l'attentat de Munich avec un pistolet réactivé. En 2017, Europol va également déclarer que cette forme d'armes est l'une des principales sources d'approvisionnement en armes illicites, ce qui se vérifie en Somalie par exemple, avec la saisie de 25 000 armes, dont une partie n'a pas pu être confisquée et circule dans un nombre important d'États africains.[25]

Une grande quantité d'armes sont converties pour s'adapter aux calibres Flobert qui sont principalement utilisées pour le tir à la cible. Beaucoup d'armes converties sont d'ailleurs

[24] *Proposition de directive du Parlement Européen et du Conseil relative au contrôle de l'acquisition et de la détention d'armes (codification)*, 26 février 2020, Sénat, http://www.senat.fr/europe/textes_europeens/e14635.pdf

[25] Florquin N, King B, « Quand le légal devient létal : les armes à feu converties en Europe », Rapport, Small Arms Survey, avril 2018

modifiées pour s'adapter aux munitions de calibre Flobert. C'est également une arme à feu étant faiblement soumise à des restrictions de possession, en Espagne elle fait même partie des armes pouvant être détenues par des civils en quantité illimitée. Les munitions de calibre Flobert sont donc beaucoup moins contrôlées et viennent presque toutes de Slovaquie, invitant les revendeurs à convertir des fusils automatiques à ce calibre. On retrouvera donc des Walthers p99 (pistolet semi-automatique fabriqué en Allemagne dans les années 1990) de ce calibre en Slovaquie et aux Pays-Bas.

II.1.1.3 *Fabrication clandestine et usage de nouvelles technologies*

La dernière inquiétude en matière de création d'armes à feu réside dans les nouvelles technologies de production, comme l'impression 3D. Comme le souligne Jean-Charles Antoine, les technologies utilisées ne sont jamais illégales, mais leur exportation ne suit pas nécessairement la législation de tous les États. En 2013, Cody Wilson, citoyen américain, souhaite mettre en ligne les plans de son arme « Liberator » en open source, afin que tout le monde puisse imprimer une arme. Son entreprise va rapidement être empêchée par la justice américaine. En 2015, il gagne le procès contre le gouvernement, il déclare : « cette victoire est à considérer comme le véritable commencement de l'ère des armes à feu téléchargeables. Les pistolets et fusils sont tout aussi téléchargeables que la musique. Il y aura même des services de streaming pour les semi-automatiques ». Il n'a pas fallu beaucoup de temps avant que ces plans se retrouvent partagés à l'international sur le Darkweb, même si les impressions restent contrôlées. Le 9 octobre 2019 par exemple, l'attentat de Yom Kippour à Halle-sur-Saale par l'extrémiste de droite Stephen Balliet impliquait l'utilisation d'armes imprimées en 3D. Bien que le nombre de victimes ne soit pas suffisamment significatif pour que les autorités s'y attèlent sérieusement, comme le déplore Rajan Basra, chercheur au Centre International pour l'Étude de la Radicalisation et de Violence Politique (ICSR), cet attentat fera au moins office d'avertissement concernant l'usage d'armes en impression 3D dans des attaques terroristes. Balliet, dans un message, évoquait d'ailleurs la simplicité d'une telle acquisition : « tout ce dont vous avez besoin est d'un weekend entier et de 50$ de matériels ».[26] L'adoption de ces nouvelles techniques de production par des extrémistes d'extrême droite implique une suppression impossible de tous les fichiers menant à la création d'armes 3D. Encore une fois,

[26] Dearden L, « Use of 3D printed guns in German synagogue shooting must act as warning to security services, expert say », The Independant, octobre 2019, https://www.independent.co.uk/news/world/europe/3d-gun-print-germany-synagogue-shooting-stephan-balliet-neo-nazi-a9152746.html

l'aide des utilisateurs d'internet en termes de signalement d'activités illégales est encouragée par les chercheurs et les autorités.

D'autres techniques de fabrication d'armes clandestines peuvent se retrouver sur le Darkweb ou même sur Facebook. C'est le cas d'un grand nombre de guides pour la fabrication artisanale de bombes. Le site *The Big Book of Mischief* par exemple donnait accès en quelques clics à la recette de fabrication d'une bombe au fulminate de mercure, avant d'être clôturé et que le propriétaire du site ne soit arrêté.[27] En 2017, l'attentat de la Manchester Arena par Salman Abedi aurait également été causé par une bombe artisanale dont l'auteur aurait trouvé la recette sur internet. Que ce soit sur Facebook, où une présentation de 30 diapositives a été retrouvée ou suite à la publication d'Al-Quaida « comment fabriquer une bombe dans la cuisine de maman » (« Make a bomb in the Kitchen of your Mom »)[28] en 2010, il était très simple de pouvoir rassembler des ingrédients dangereux. Bien que des explosifs comme le Semtex ne sont pas accessibles à la vente pour des particuliers, de nombreux autres produits alternatifs pouvaient être utilisés comme de l'engrais ou même certains produits pour les cheveux. Cependant, pour l'expert du contre-terrorisme au Royal United Services for Defence and Security Studies Raffaello Pantucci faire une bombe peut ressembler à un jeu d'enfant mais son fonctionnement et son explosion relèvent de compétences particulières, qui ne sont pas à la portée de tous, en faisant référence à de nombreux attentats à la bombe ayant échoué au Royaume-Uni.[29] Si de tels guides ont pu être trouvés sur internet et Facebook entre 2010 et 2014, leur suppression des plateformes n'a certainement pas empêché à ces guides de fuiter sur des forums du Darknet, qui sont encore accessibles aujourd'hui à travers des liens spécifiques.

II.1.2 Proportions des armes vendues par région/pays

Étant donné que le Darkweb s'apparente à une véritable « boîte noire » difficile à saisir par les autorités[30], il devient alors fondamental d'identifier les axes de passages ainsi que les

[27] Yeazel B « Bomb Making Manuals on the Internet : Maneuvring a solution through First Amendment Jurisdprudene », Notre Dame Journal of Law, Ethics & Public Policy, février 2014, http://scholarship.law.nd.edu/ndjlepp/vol16/iss1/12

[28] Annexe

[29] MacAskill E, Hopkins N, « Bomb-making guides are online, but getting them to work is not easy », The Guardian, mai 2017, https://www.theguardian.com/uk-news/2017/may/23/bomb-making-guides-are-online-but-getting-them-to-work-is-not-easy

[30] « Trafic d'armes : internet, « boîte noire » difficile à pénétrer pour les autorités », l'Obs, novembre 2015, https://www.nouvelobs.com/societe/20151111.AFP6194/trafic-d-armes-internet-boite-noire-difficile-a-penetrer-pour-les-autorites.html

principaux revendeurs d'armes sur les réseaux, pour pouvoir agir physiquement et non plus uniquement virtuellement, sur l'émergence de ce trafic.

II.1.2.1 *Les plus grands vendeurs : États-Unis*

Il s'agit dans un premier temps d'analyser la provenance des armes perquisitionnées aux frontières ou dans les domiciles. Comme le disait Jean-Charles Antoine lors d'une interview sur RTL, la plupart des armes retrouvées sur le Darkweb viennent principalement du cadre légal, ce qui implique une commercialisation plus importante d'armes légales légères acquise légalement par des citoyens américains ou des armes à feu issues d'anciens conflits d'Europe de l'Est, dont la neutralisation a pour vocation de les rendre légales et autorise leur libre circulation à des fins d'exposition.

Premièrement, il faut savoir que le trafic d'armes nord-américaines est connu des différentes autorités des Amériques. Selon les experts en trafic d'armes Sarah Kinosian et Eugenio Weigend, les criminels et mafias mexicains obtiennent généralement des armes grâce à un contact pouvant en obtenir de manière légale, pour les revendre ensuite sur le marché noir à un prix plus élevé.[31]C'est un procédé courant qui permet d'assurer le fonds de commerce de certains petits commerçants. Entre les continents américains, les experts s'accordent à dire que le trafic représente une activité à moindre risque, en partie grâce au laxisme des autorités fédérales concernant la circulation des armes sur le territoire, participant au financement de la guerre de la drogue au Mexique par exemple. En 2017, l'enquête de RAND Europe et de l'Université de Manchester montre que les armes américaines représentent également 60% des armes à feu retrouvées sur le Darkweb[32]. Il s'agira majoritairement d'ALPC, étant donné que ce sont les plus simples à se procurer, que ce soit de manière légale ou illégale, surtout si elles doivent traverser l'Océan. La présence d'armes américaines sur les marchés noirs s'explique également par l'assistance militaire américaine en Syrie, Irak ou encore en Afghanistan, qui consiste à fournir des gouvernements ou des acteurs non étatiques en armes, comme par exemple des fusils d'assaut M16 et M4, des lance-grenades, des mitrailleuses lourdes, des lunettes de visée thermiques ainsi que des gilets pare-balles[33]. Le retrait rapide des troupes américaines de Syrie avait d'ailleurs interrogé sur la possibilité d'une « révolution industrielle » dans le terrorisme, tant la quantité d'armes laissées était conséquente. En 2019, des avions de

[31] Shepp J, « The American Gun Glut Is a Problem for the Entire Worid », New York Mag, février 2018, https://nymag.com/intelligencer/2018/02/the-american-gun-glut-is-a-problem-for-the-entire-world.html

[32] Persi Paoli. G, Aldridge. J, Ryan. N, Warnes. R, « Behind the Curtain, the illicit trade of firearms, explosives and ammunition on the dark web », RAND Europe, 2017

[33] Annexe 5

combat F-15R Strike Eagle ont exécuté une frappe aérienne de précision, commanditée par le Pentagone afin de détruire une importante cachette de munitions américaines logée dans une ancienne cimenterie, convertie en base d'opérations spéciales américaines et en camp d'entraînement kurde. Il s'agissait de « réduire l'utilité militaire de l'installation ».[34] Une partie du matériel utilisé par les troupes américaines n'a pu être récupérée ou détruite, il sera alors retrouvé sur le Darkweb mais également sur les différents services de messagerie cryptée comme Telegram, contrôlée par des militants affiliés à Al-Qaïda ou alors sur Facebook dans des groupes secrets. Selon le journaliste d'investigation Christopher John Chivers, les États-Unis auraient perdu la trace de centaine de milliers d'armes en Iraq et en Afghanistan[35]. Comme le montre Iain Overton dans le cadre de l'association Action on Armed Violence (AOAV), dont il est le directeur, le Pentagone a déclaré avoir des registres pour seulement 48% des armes que les États-Unis ont fourni à différents alliés, soit environ 700 000 armes légères.[36]

II.1.2.2 *Les plus grands vendeurs : L'Europe*

À l'image des armes en provenance des États-Unis, l'Europe possède également son lot d'armes légales revendues sur le darkweb. Elles sont généralement issues de vols à des particuliers ayant une licence de chasse ou se rendant en stand de tir. Selon une étude du Flemish Peace Institute, une grande partie des armes européennes retrouvées sur le darkweb proviennent de Belgique, Croatie, Danemark, France, Italie, Pays-Bas, Roumanie et du Royaume-Uni. Ce sont dans ces pays qu'une grande quantité de vols d'armes à feu ont été perpétrés, engendrant le vol d'au moins 827 armes en Belgique à des possesseur légaux, des fabricants, des trafiquants, des stocks de l'État ainsi que sur des sites de destruction rien qu'en 2015 contre 10 572 en France la même année. Au Danemark, ce sont plus de 1000 armes volées entre 2012 et 2016, 300 aux Pays-Bas et environ 692 au Royaume-Uni entre 2015 et 2016. La majorité des armes volées à des particuliers sont issues de cambriolages aux domiciles des possesseurs. En Belgique, des producteurs d'armes à feu ont subi de nombreux cambriolages comme l'entreprise FN Herstal, principalement de la part de ses salariés tout comme en Bulgarie où deux employés d'une entreprise de production d'armes à feu ont été arrêtés pour trafic d'armes dans la région de Stara

[34] Keller J, « The Weapons America is Leaving Behind in Syria », The Soapbox, octobre 2019, https://newrepublic.com/article/155471/weapons-america-leaving-behind-syria

[35] Chivers J-C, « How Many Guns Did the US Lose Track of in Iraq and Afghanistan ? Hundreds of Thousands. », The New York Times Magazine, août 2016, https://www.nytimes.com/2016/08/23/magazine/how-many-guns-did-the-us-lose-track-of-in-iraq-and-afghanistan-hundreds-of-thousands.html

[36] Overton I, Jarvis-Norse A, Dathan J, Lombardi M, « US Department of Defence spend on guns in « War on Terror » revealed », Action on Armed Violence (AOAV), août 2016, https://aoav.org.uk/2016/us-department-of-defence-spend-on-guns-and-ammunition-in-the-war-on-terror-revealed/

Zagora. Le trafic d'armes émanant d'Europe est donc en partie dû au développement de l'industrie militaire dans ces différents pays. Certaines entreprises ont tout de même pris les devants en investissant dans des systèmes de sécurité perfectionnés, qui ont dissuadé tout braquage, comme les entreprises croates par exemple. Le vol d'établissements de vente ou d'entrainement sont également fréquemment enregistrés en Europe. En France, les autorités ont estimé à environ 300 armes volées par an à des commerces professionnels (stands de tir et vendeurs avec licence). La question de la mauvaise neutralisation d'armes induit également la vente de fusil d'assaut de type AK-57, des mitraillettes PPSH41, pistolets et fusils stockés par des sociétés de cinéma. [37]

Bien sûr, la législation concernant le port d'armes dans chaque État européen modifie les provenances d'armes sur le Darkweb. Au Danemark par exemple, l'inscription en stand de tir est ouverte à tous les citoyens, sans regarder les passifs des inscrits. Les criminels sont donc susceptibles de fréquenter des stands de tir, ce qui explique la raison pour laquelle la police danoise semble confrontée à des criminels maniant des armes à feu avec dextérité et précision. Cette ouverture des stands de tirs à un public aussi large donne aussi la possibilité de faire des repérages réguliers pour en prévoir le vol.

Les sites de destruction européens sont également sujets à des trafics, comme en 2016 lorsque le directeur du banc d'essai d'armes à feu de Liège a été arrêté à cause de la disparition des registres de 260 armes censées partir en destruction. Comme expliqué plus tôt, la part d'armes sujettes à une reconversion ou à une retroconversion est également conséquente en Europe, avec les armes utilisées par l'ex-armée yougoslave, les défauts de neutralisation d'armes en Slovaquie etc. La fusillade de Munich du 22 juillet 2016 avait été commise par un jeune de 17 ans, s'étant procuré un pistolet au calibre Flobert ainsi que des munitions pour l'équivalent de 4 500€ tout compris sur le darkweb. La part des ventes sur le Darkweb n'est évidemment pas l'unique moyen employé par les gros trafiquants pour vendre leur marchandise, le trafic physique et la contrebande gardent un avantage pécuniaire en raison de l'importance des transactions et des cargaisons.

[37] Duquet N, Goris K, « Firearms acquisition by terrorists in Europe : research findings and policy recommendations of Project SAFTE », Flemish Peace Institute, avril 2018, https://www.flemishpeaceinstitute.eu/safte/files/vrede_syntheserapport_safte_lr.pdf

II.2 Réponse internationale et nationales

II.2.1 Mesures et succès des autorités dans le contrôle des trafics

Face à l'importante variété de sources du trafic d'armes, on pourrait légitimement se questionner sur l'efficacité des autorités compétentes, pourtant il serait erroné de ne leur attribuer aucun mérite quant à la gestion d'une telle menace à la sécurité internationale. En effet, depuis 2016, une part importante de plateformes clés du trafic de drogue et d'armes sur le Darkweb a pu être clôturée grâce aux autorités nationales mais aussi grâce à des institutions internationales.

II.2.1.1 *Démantèlement de plateformes de vente du darkweb (Silk Road, French Deep Market etc)*

Premièrement, la répression du commerce illégal passe par le démantèlement des places de marché virtuelles. La clôture de la célèbre plateforme de vente SilkRoad mais aussi de la quantité astronomique de sites de vente sur le Darkweb contribue à chaque fois à lutter l'avance technologique de vendeurs et de plateformes sur le Darkweb. Rien qu'en France, des démantèlements de grosses plateformes de vente (Black Hand et French Deep Market) ont nécessité une mobilisation exceptionnelle d'agents de la DNRED (Direction Nationale du Renseignement et des Enquêtes Douanières) ainsi que des experts techniques. Dans le cas de la DNRD, lutter contre le trafic d'armes sur internet entre dans sa mission de lutte « contre les grands réseaux internationaux de contrebande (stupéfiants, tabac, armes, biens culturels, contrefaçons) en mettant en œuvre, si les enjeux le justifient, des techniques d'investigation spécialisées ». [38] La teneur exacte des opérations menées par la DNRED ne sont pas communiquées, mais elles consistaient à la saisie massive de données ainsi qu'un accès au serveur de Black Hand[39] pour finalement remonter jusqu'aux administrateurs principaux du site. L'historique de démantèlements de différents réseaux comme Hansa, Freedom Hosting, French Deep Market, the Wall Street Market montrent que les techniques ne sont jamais les mêmes. Dans le cas de Freedom Hosting avec Eric Marques, le FBI a choisi une technique de rupture de l'anonymat sur Tor, une technique nécessitant des cybers experts et dont le coût peut

[38] « L'essentiel de la douane », Portail de la Direction Générale des douanes et droits indirects, Portail de l'Économie, des Finances, de l'Action et des Comptes Publics, https://www.douane.gouv.fr/la-douane/qui-sommes-nous/lessentiel-de-la-douane

[39] Planques M, « Comment le forum du « dark web » vient d'être démantelé en France », RTL, juin 2018, https://www.rtl.fr/actu/futur/comment-le-forum-du-dark-web-vient-d-etre-demantele-en-france-7793777376

être conséquent (implantation de machines du FBI en tant que routeurs de Tor et hackers pour mettre fin à l'anonymat)[40]. Les autorités allemandes, dans le cas de la fermeture de Wall Street Market, ont préféré s'atteler à la fermeture massive de comptes Escrow et les portefeuilles de monnaie virutelles, valant en tout 11 millions de dollars. Cette saisie a été en partie due grâce à l'affût massif de vendeurs sur la plateforme après la fermeture par les autorités finlandaises du réseau Silkkitie (Valhalla)[41]. Une autre technique qui a pu être menée à bien a nécessité le concours d'Europol et de la société de sécurité sur Internet Bitdefender pour le cas du site Hansa. Cette coopération a permis à Europol de fournir des informations clés sur les administrateurs du site aux autorités néerlandaises, qui ont pu alors remonter jusqu'aux coupables en Allemagne et permettre la saisie des serveurs situés aux Pays-Bas, en Allemagne et en Lituanie. La saisie massive de données a été permise grâce à l'autorisation judiciaire néerlandaise, qui a permis de collecter des adresses, transmises aux forces de police et à Europol. Ce succès a été permis grâce à l'Operation Bayonet, une opération multinationale qui a également servi à la fermeture du site AlphaBay, avec la contribution du FBI.[42] Encore une fois, les détails concernant les moyens employés par le FBI ou Europol ne sont pas renseignés. Dans le cas de AlphaBay, un simple mail (pimp_alex_91@hotmail.com) renseigné sur le message de bienvenue sur le site a permis aux autorités de trouver son compte PayPal lié à une certaine société EBX Technologies, située à Bangkok en Thaïlande, où la police locale a alors procédé à une enquête au domicile de Caze pour pouvoir le démasquer[43].

II.2.1.2 *Démantèlement de réseaux physiques en Europe*

Les démantèlements de trafics physiques, qui sont maintenant aidés par des compétences de la part des experts en cyber, ne sont pas récents et explosent en 2015 avec l'inquiétude d'une réitération d'attentats en France et en Europe. En 2019, un trafic d'armes international est démantelé en France pour des armes vendues d'origine américaine. Les coupables, installés en Seine-et-Marne, étaient associés avec un homme qui se rendait régulièrement aux États-Unis pour y acquérir des armes de manière légale. Les gendarmes de la section de recherche d'Angers

[40] Howell O'Neill P, « A dark web tycoon pleads guilty. But how was he caught ? », MIT Technology Review, février 2020, https://www.technologyreview.com/2020/02/08/349016/a-dark-web-tycoon-pleads-guilty-but-how-was-he-caught/

[41] « German police shuts down one of world's biggest dark web site », The Guardian, mai 2019, https://www.theguardian.com/world/2019/may/03/german-police-close-down-dark-web-marketplace

[42] « Massive Blow to Criminal Dark Web Activities after Globally Coordinated Operation », Europol, juillet 2017, https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

[43] Greenberg A, « Global Police Spring a Trap on Thousands of Dark Web Users », Wired, juillet 2017, https://www.wired.com/story/alphabay-hansa-takedown-dark-web-trap/

vont alors contacter des partenaires au HSI (Homeland Security Investigations) aux États-Unis pour une coopération dans l'opération de démantèlement du réseau. Cette opération permet de mettre la main sur des culasses, des carcasses de pistolets-mitrailleurs (à des fins de reconversion d'autres armes), des pièces détachées de pistolet Beretta, des carabines et autres armes d'épaule, des explosifs (bâtons de dynamite ainsi que des grenades) dont le motif d'utilisation est encore inconnu[44]. Toutes ces colis ont pu être interceptés à l'aéroport de Roissy. Cette perquisition a également permis d'identifier un vaste trafic sur tout le territoire Français, notamment en Savoie, dans le Loiret, la Nièvre, en Val-de-Marne et Seine-et-Marne. C'est d'ailleurs dans ce département qu'un important atelier de confection d'armes va être évacué, à Nemours[45].

En juin 2020, l'un des plus gros trafics d'armes est démantelé en Espagne, en provenance de Malaga. Ce ne sont pas moins de 731 armes à feu de saisies, certaines répondant d'ailleurs à la qualification d'armes de guerre. Les produits retrouvés étaient des armes factices pouvant être rendues létales, des armes neutralisées pouvant être reconditionnées et des armes qui destinées à une reconstruction à partir de pièces détachées (concept de « cannibalisation », visant à reconstruire une arme à partir de pièces détachées provenant d'autres)[46]. Étant donné que l'Espagne fait partie des principales sources d'armes sur le Darkweb (en provenance d'Europe), il se pourrait que cette intervention réduise drastiquement la quantité d'armes disponibles sur les plateformes de vente du Darkweb. Ces démantèlements de gros réseaux répondent avant tout à un travail d'investigation de plus en plus perfectionné, où les forces de police agissent à la fois sur le terrain mais sont également positionnées sur les réseaux sociaux et sites de vente afin de repérer les activités illégales. Les saisies de 2019 et 2020 en France et en Espagne ne sont pas les seules perquisitions importantes faites en Europe ces dernières années. Elles font suite à une série de succès des autorités pour l'identification de trafiquants, principalement des petites mains des réseau.

En mars 2019, un autre réseau important a pu être démantelé grâce à la coopération de l'Italie et de l'Autriche ainsi que d'Eurojust. Un succès majeur vu la part d'armes italiennes en vente sur le Darkweb. Le rapport d'Eurojust recense 22 arrestations, 1600 saisies de munitions et

[44] Annexe 6

[45] Chevillard T, « Angers : un trafic international d'armes à feu provenant des États-Unis démantelé », 20 minutes, mars 2019, https://www.20minutes.fr/faits_divers/2466627-20190306-angers-trafic-international-armes-feu-provenant-etats-unis-demantele

[46] Taylor L, « Police Dismantle One of The Largest Gun Trafficking Networks in Spain With Origins in Costa del Sol's Malaga », Euro Weekly News, juin 2020, https://www.euroweeklynews.com/2020/06/24/police-dismantle-one-of-the-largest-gun-trafficking-networks-in-spain-with-origins-in-costa-del-sols-malaga/

d'explosifs et 139 armes à feu[47]. Parmi les arrestations, deux autrichiens étaient à l'origine de la vente de 800 pistolets et 50 kalachnikovs à des groupes de crimes organisés ainsi que sur les réseaux. Cette importante vente d'armes était en partie due à l'expansion de la mafia Ndrangheta. En Italie, cette perquisition n'était pas rendue facile à cause de la présence de la mafia dans les cercles politiques et dans les administrations, ce qui a obligé la police italienne a récourir à une « police blitz », se résumant au déploiement de 3000 policiers dans 12 régions italiennes pour procéder aux arrestations de manière groupée. Le chef de la Ndrangheta, Luigi Mancuso a également été arrêté ainsi qu'un ancien parlementaire du gouvernement de Silvio Berlusconi, accusés d'avoir travaillé avec le groupe mafieux[48]. Des arrestations qui pourraient radicalement diminuer la présence italienne dans le trafic d'armes.

II.2.1.3 *Identification des points de passage*

Cependant, bien que ces saisies représentent une avancée majeure dans la lutte contre le trafic d'armes, celles commercialisées sur le Darkweb n'ont pas disparu pour autant. Il devient alors important de pouvoir identifier les voies utilisées pour leur livraison, tout en innovant les techniques de contrôle. Sur le continent européen, les saisies dans les aéroports ou l'interception de colis peut parfois se montrer inefficaces à cause de stratégies d'évitement bien rodées.

Les cryptomarkets et leus vendeurs précisent la provenance des marchandises (à l'image des sites de vente comme ebay), ce qui permet de se mettre d'accord sur les moyens de livraison entre l'acheteur et le vendeur. Les autorités pensaient alors utiliser la recherche par pays pour tenter d'identifier les différentes provenances. Cependant cette technique s'est avérée inefficace. Par exemple, des vendeurs de drogue néerlandais spécifiaient leur location mais préféraient faire appel à des intermédiaires pour envoyer le colis en toute confiance sans passer par les services de poste. La popularité de la drogue en Europe a déjà permis de perfectionner les systèmes de contrôle de colis au Pays-Bas. De plus, les vendeurs se gardent souvent d'indiquer le pays où se trouve la marchandise, préférant spécifier une région ou un continent. Dans ce sens, beaucoup de vendeurs vont tout simplement dire qu'ils expédient du monde entier pour empêcher de trouver un quelconque indice sur leur localisation, bien que certains préfèreront être honnêtes et jouer la carte de la transparence pour attirer plus de clients. Selon le rapport de RAND Europe « Behind the Curtain », les États-Unis représentent un revenu de

[47] « Massive arms trafficking ring dismantled by Italian and Austrian action, coordinated by Eurojust », Eurojust, mars 2019, http://www.eurojust.europa.eu/press/PressReleases/Pages/2019/2019-03-26.aspx

[48] Povoledo E, « Italian Police Arrests Over 300 in Raids on Organized Crime », The New York Times, décembre 2019, https://www.nytimes.com/2019/12/19/world/europe/ndrangheta-arrests-police-mafia.html

24 987 dollars par mois contre 29 526 dollars par mois pour des provenances inconnues. Les Pays-Bas et le Royaume-Uni se placent même avant l'Europe avec des revenus respectifs de 8 088 dollars par mois et 5 043 dollars par mois en 2017. Cependant, grâce au travail d'investigation des experts de RAND Europe, il a été déterminé que sur un total de 74 733 dollars par mois, 68 561 dollars d'armes sont envoyés dans le monde entier, sans précision de la destination. Les profils de vendeurs précisant un envoi dans le monde entier ont donc bien plus de chances de trouver preneur qu'un vendeur qui préciseraient des destinations de prédilection. L'Europe représente 4 154 dollars à elle seule, sans compter les livraisons faites en Europe au travers la qualification « Worldwide shipping »[49]. Cependant, il apparaît logique que les États-Unis soient les principaux vendeurs envoyant vers le monde entier, en raison de la politique nationale sur le port d'arme[50]. Une grande partie des transactions reste pourtant opaque concernant les destinations exactes en Europe, étant donné que les données la présente comme principale réceptrice. Seuls le Danemark, les Pays-Bas et l'Allemagne précisent plus ouvertement leur localisation. Bien que ces informations donnent une vue générale sur la tendance du trafic sur le web, elle ne permet pas de mener des opérations de lutte anti-trafic efficaces, à part l'identification d'un vaste trafic entre les États-Unis et l'Europe.

II.2.2 Les innovations de la scène internationale pour la lecture de ces trafics

La vague d'attentats de 2015 et 2016 a indubitablement modifié le jugement de la scène internationale concernant l'état du trafic d'armes dans le monde et en Europe. De nombreux think tanks, réunions intergouvernementales ou encore des politiques multinationales ont été menées afin d'endiguer une menace accentuée par la popularité du Darkweb.

II.2.2.1 *Projets de lois et initiative relatifs au trafic d'armes en Europe*

En 2018, l'Union Européenne lance une stratégie concernant les ALPC, censée intégrer chaque membre européen à la lutte contre la prolifération d'armes en Europe et réfléchir à un désarmement progressif de la population européenne. Le Think Tank sur la non-prolifération et le désarmement a proposé un article en avril 2019, rédigé par Nils Duquet. Ce texte proposait, en plus de fournir un aperçu détaillé de la situation du trafic d'armes en Europe, des recommandations visant à sensibiliser les États Européens aux mesures de contrôle possibles

[49] Persi Paoli. G, Aldridge. J, Ryan. N, Warnes. R, « Behind the Curtain, the illicit trade of firearms, explosives and ammunition on the dark web », RAND Europe, 2017
[50] Annexe 7

sur leur territoire.[51] Parallèlement, les chefs d'États se sont entendus sur le risque que représente le trafic d'armes à feu en provenance des Balkans (trafics physiques ou virtuel). En 2018, les ministres des affaires étrangères français et allemands Jean-Yves Le Drian et Heiko Mass président la première réunion de haut niveau de lutte contre les trafcis d'armes à feu dans les Balkans Occidentaux, à l'initiative des deux gouvernements. [52]Cette mesure permettrait de coordonner davantage l'action des gouvernements de l'Union Européenne et des Balkans afin de stabiliser la région, surtout face à une menace terroriste encore présente. Étant donné que le trafic d'armes en Europe s'exporte également dans les autres régions du monde, l'initiative est rejointe par des partenaires internationaux. Cette politique établit une feuille de route à destination des pays des Balkans sur des objectifs à atteindre avant 2024. En 2016, Europol avait estimé entre 3 et 6 millions la quantité d'armes en circulation dans la région, avec seulement 44 000 armes légères détruites. Certaines dispositions concrètes ont été prises, comme l'aide financière française et allemande pour la conception de logiciels d'identification et de traçage balistique ainsi que la production d'équipement adapté. Un travail sera également fait du côté des ambassades, avec par exemple l'ouverture d'un poste de coopérant chargé de la lutte contre les trafics d'armes à feu, qui prendra ses fonctions dans l'ambassade française à Belgrade en Bosnie Herzégovine.[53] Un poste censé se charger de l'efficacité des autorités aux frontières ainsi que leur contrôle plus assidu. D'autres postes similaires devraient voir le jour dans les années à suivre pour permettre d'atteindre l'objectif 2024. Les sept objectifs énumérés dans la feuille de route sont :

- « OBJECTIF 1. D'ici 2023, veiller à ce que la législation sur le contrôle des armements soit en place, pleinement harmonisée avec le cadre réglementaire de l'UE et des autres obligations internationales connexes et normalisée dans toute la région.
- OBJECTIF 2. D'ici 2024, veiller à ce que les politiques et pratiques de contrôle des armements dans les Balkans occidentaux soient fondées sur des preuves et fondées sur le renseignement.

[51] « The 2018 EU SALW Strategy : Towards an Integrated and Comprehensive Approach », Non Proliferation and Disarmement Consortium, 2018, https://www.nonproliferation.eu/2018-eu-salw-strategy/
[52] « Lutte contre les trafics illicites d'armes à feu dans les Balkans occidentaux – Déclaration à la presse de M.Jean-Yves Le Drian (Paris, 11.12.2018) », France Diplomatie, décembre 2018, https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/desarmement-et-non-proliferation/elimination-et-maitrise-des-armements-classiques/article/lutte-contre-les-trafics-illicites-d-armes-a-feu-dans-les-balkans-occidentaux
[53] « Lutte contre les trafics illicites d'armes à feu dans les Balkans occidentaux – Déclaration à la presse de M.Jean-Yves Le Drian (Paris, 11.12.2018) », France Diplomatie, décembre 2018, https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/desarmement-et-non-proliferation/elimination-et-maitrise-des-armements-classiques/article/lutte-contre-les-trafics-illicites-d-armes-a-feu-dans-les-balkans-occidentaux

- OBJECTIF 3. D'ici 2024, réduire considérablement les flux illicites d'armes à feu, de munitions et d'explosifs vers, à l'intérieur et au-delà des Balkans occidentaux.
- OBJECTIF 4. D'ici 2024, réduire considérablement l'offre, la demande et l'utilisation abusive des armes à feu en augmentant la sensibilisation, l'éducation, l'aide et le plaidoyer.
- OBJECTIF 5. D'ici 2024, réduire considérablement le nombre estimé d'armes à feu en possession illicite dans les Balkans occidentaux.
- OBJECTIF 6. Diminuer systématiquement les excédents et détruire les armes légères et de petit calibre saisies et leurs munitions.
- OBJECTIF 7. Réduire considérablement le risque de prolifération et de détournement d'armes à feu, de munitions et d'explosifs. » [54]

Ce sommet vient compléter les directives européennes déjà existantes concernant le trafic d'armes en Europe, la première version a été révisée en 2008 pour être encore complétée en 2017 (Directive 2008/51/EC et 2017/853/EC), qui permettait d'ajouter les nouvelles techniques de conversion et de création d'armes à feu ainsi que des précisions quant aux nouveaux types de munitions, calibre et pièces détachées interdites à la vente légale et assure la requalification de certaines armes anciennement jugées comme objet d'art[55]. Cet amendement permet aussi d'intégrer pour la première fois internet dans un texte de loi officiel relatif au trafic d'armes, bien qu'il n'évoque pas encore l'implication conséquente du Darkweb dans la propagation d'armes en Europe.

II.2.2.2 *Mesures multilatérales et internationales*

En 2017, le Conseil de Sécurité publie un rapport rédigé par la Secrétaire Générale adjointe et Haute Représentante du désarmement Izumi Nakamitsu faisait le lien entre le trafic d'armes et les obstacles au développement, qui inclue la Darkweb comme un des enjeux croissants de la sécurité internationale.[56] En 2015, le gouvernement français parle de la mise en place de « cyber-patrouilles » pour la lutte contre la détention illégale d'armes et leur vente[57]. Sur le plan européen, de nombreuses avancées on été permises grâce aux stratégies d'Europol et ses

[54] Extrait de la feuille de route présentée et adoptée par les chefs d'États de gouvernement lors du Sommet de Londres sur les Balkans Occidentaux du 9 au 10 juillet 2018, https://www.france-allemagne.fr/IMG/pdf/roadmap-final_version_july_2018.pdf
[55] « Directive (EU) 2017/853 of the European Parliament and of the Council of 17 May 2017 amending Council Directive 91477/EEC on control of the acquisition and possession of weapons », Official
[56] « S/2017/1025 : Small Arms and Light Weapons : report of the Secretary-General », United Nations Security Council, décembre 2017, https://undocs.org/S/2017/1025
[57] « Plan National de Lutte contre les Armes Illégalement Détenues », Ministère de l'Intérieur, 2015

différents programmes de contrôle de la sécurité intérieure de la région. En 2016, Europol lance l'opération Ciconia Alba, censée lutter contre le cybercrime et le trafic d'armes[58] dans le cadre du cycle politique EMPACT, d'une durée de 4 ans (2018-2021, faisant suite au programme de 2010-2014). Cette politique internationale organisée par l'Union Européenne et épaulée par des partenaires en dehors de la zone, permet de s'atteler aux crimes majeurs relatifs à la cybercriminalité, trafic de drogue, l'immigration illégale, crime organisé, trafic d'humains, blanchiment d'argent, trafic d'armes, crime environnemental, fraude de documents. L'opération Ciconia Alba regruope 52 États participants incluant tous les membres de l'UE, on retrouve entre autres les États-Unis, le Canada, le Brésil, la Colombie, Hong Kong, le Nigéria, la Thailande, le Qatar ou encore les Émirats Arabes Unis, en plus de partenaires comme Eurojust, Frontex, le Centre Opérationnel du Renseignement Maritime pour les Stupéfiants et Interpol. Elle vise à rassembler les organismes d'application de la loi, les institutions et organismes européens ainsi que tout autre partenaire pertinent[59]. Cette politique a été aiguillée par le Comité permanent de coopération opérationnelle en matière de sécurité intérieure (COSI), dont le fonctionnement est introduit dans l'article 71 du traité sur le fonctionnement de l'UE (TFUE). Ce comité permet de coordonner « l'action des autorités compétentes des États membres »[60]. En 2017, l'Opération Dragon fait suite à l'Opération Ciconia Alba en devenant la quatrième série des journées d'action commune (JAD), où des officiers des forces de l'ordre travaillent sur le terrain et reçoivent un support opérationnel de la part du centre de coordination d'Europol situé à la Haye, 24/7. Les officiers de liaison des États membres ainsi que leurs collègues d'autres partenaires internationaux (cités plus haut) coordonnent l'échange d'informations et de renseignement avec les services de maintien de l'ordre nationaux. Les spécialistes et analystes d'Europol fournissent une assistance depuis le siège mais également sur place[61].

L'autre projet d'ampleur mettait en scène une coopération américaine, allemande, britannique et néerlandaise ainsi que d'autres participants à l'international. La mission n'était plus seulement de clôturer des réseaux étant donné que d'autres se recréaient immédiatement derrière, mais d' « endommager la confiance dans le système complet », comme l'explique Marinus Boekelo, enquêteur à la National Hi-Tech Crime Unit des forces de police britanniques

[58] Annexe 8
[59] « EU Policy Cycle – EMPACT », Europol, https://www.europol.europa.eu/empact
[60] Extrait de l'article 71 du TFUE
[61] « Worldwide operation Dragon sees 52 countries teaming up to thwart organised crime », Europol, juin 2017, https://www.europol.europa.eu/newsroom/news/worldwide-operation-dragon-sees-52-countries-teaming-to-thwart-organised-crime

en s'attaquant au site Hansa[62] Une opération qui a montré l'évolution des forces de police dans leur gestion des cybercrimes avec des méthodes nouvelles et adaptées.
Enfin, en juin 2017, toujours grâce à Europol, l'organisation de « cyber patrouilles » (cyber-patrolling week) d'une semaine permet d'intercepter des échanges d'armes, drogues et trafics d'humains, grâce au travail d'enquêteurs spécialisés dans les différents types de cybercrime.[63] Cette semaine dédiée à l'identification d'activités illégales comprenait les mêmes partenaires étatiques que l'Opération Ciconia Alba. Seul Eurojust en tant que tiers partenaire, prenait part à l'opération.

III/ Conséquences du cyber trafic d'armes

Au-delà des efforts réalisés par la scène internationale pour le contrôle du trafic d'armes et plus récemment son expansion sur le web, il faut tout de même souligner les effets d'un tel commerce sur la géopolitique, l'économie ou encore sur les sociétés. Il y a en effet un véritable travail sociologique à fournir concernant les profils des utilisateurs du Darkweb qui sembleraient bien plus hétérogènes que les clients traditionnels du trafic d'armes dans le cadre du crime organisé ou des grands groupes terroristes.

III.1 Conséquences géopolitiques

III.1.1 Création de nouveaux « hubs terrestres » du trafic d'armes en Europe et aux États-Unis

La nouvelle nature du trafic d'armes sur internet ne dispense pas les réseaux criminels ou la corruption d'agir sur le terrain ou de faciliter ces transactions. Le développement des trafics par le biais du Darknet continue de modifier les territoires et les dynamiques de groupe, sans oublier que le trafic d'ALPC a largement augmenté des suites d'une hausse de la demande en drogue, ce qui a exacerbé des rivalités.

[62] Greenberg A, « Operation Bayonet : Inside the Sting That Hijacked an Entire Dark Web Drug Market », Wired, août 2018, https://www.wired.com/story/hansa-dutch-police-sting-operation/
[63] « Cyber-patrolling week », Europol, https://www.europol.europa.eu/activities-services/europol-in-action/operations/cyber-patrolling-week

III.1.1.1 *Corruption*

En 2019, Antonio Guterres mentionnait le danger d'une corruption toujours active dans les trafics d'armes, d'enfants et de drogue. Lors de la Journée contre la Corruption à l'ONU, il déclare que « des milliers de milliards de dollars, soit plus de 5% du PIB mondial, disparaissent dans des pots-de-vin ou d'autres pratiques de corruption »[64]. En attendant la session de l'Assemblée Générale, censée se tenir en 2021 afin d'examiner les progrès des États dans leur lutte contre la corruption, il convient d'analyser la responsabilité de cette corruption dans la propagation d'armes auprès de particuliers européens. Selon Andrew Feinstein, ancien membre du Congrès National Africain, le taux de corruption pour le trafic d'armes s'élèverait à 40% de la corruption totale. Il faut pourtant pouvoir diviser la corruption entre des acteurs transnationaux et nationaux, de la corruption plutôt locale, permettant de faire passer des armes discrètement aux frontières ou dans les services postiers et de fret. Selon une étude sur la corruption aux frontières, dirigée par Marie Chêne en 2018, l'Union Européenne, par sa géographie et sa disparité économique, est propice à la corruption des gardes-frontières. Pour les grands points de passage, les frontières sont généralement bien équipées avec des systèmes de surveillance perfectionnés et une coopération entre gardes-frontières de chaque côté de la frontière plus importante, ce qui n'est pas le cas dans les postes moins importants, à l'écart des grandes villes[65]. Selon le Centre d'Étude de la Démocratie, ces postes et leurs gardes-frontières sont plus enclins à la corruption, que ce soit pour aider la famille ou des amis, ou tout simplement suite à la pression de groupe des autres gardes. L'organisation des équipes en « unités cohésives » rend alors la lutte contre la corruption plus complexe. Selon Marie Chêne, il n'est pas rare qu'un petit poste devienne complètement corrompu de cette manière. Il ne faut pas non plus négliger la forte pression des collègues de travail dans la cadre de ces agissements qui peuvent nuire à la qualité de vie et de travail de celui qui s'y opposerait, comme l'expliquent les chercheurs Carlos Ferreira, Michael Engelschalk et William Melville.[66] La collusion du crime organisé avec des agents des douanes corrompus pose un risque majeur pour la sécurité, car elle compromet non seulement la détection du commerce illicite de drogues, mais également celle des marchandises à haut risque et interdites telles que les armes et les explosifs. Par

[64] « Journée contre la corruption : le Secrétaire Général appelle à s'unir pour mettre fin au détournement des ressources par les flux d'argent illicites », SG/SM/19901-OBV/1945, Nations Unies, décembre 2019, https://www.un.org/press/fr/2019/sgsm19101.doc.htm

[65] Chêne M, « Corruption at borders », CHR Michelsen Institute, 2018, pp 2 https://www.u4.no/publications/corruption-at-borders.pdf

[66] Ferreira C, Engelschalk M, Mayville W, *The Many Faces of Corruption : Tracking Vulnerabilities at the Sector Level,* « The Challenge of Combating Corruption in Customs Administrations », World Bank Group Publications, 2011, pp. 367-386

exemple, un appareil à rayons X de haute technologie utilisé dans un poste de douane corrompu peut entraver tous les efforts visant à détecter d'éventuelles activités terroristes.

Le problème de vol de matériel directement dans des bases militaires contre des sommes élevées soulèvent également un problème de corruption important. C'était le cas du caporal-chef opérant à la base de l'armée de l'air à Istres qui aurait fourni plusieurs fusils d'assaut (notamment des FAMAS) ainsi que des caisses contenant différentes carcasses, matériels techniques et autres armes de poing en plein état d'urgence militaire[67]. Une transaction d'autant plus étonnante dans une base aussi surveillée.

III.1.1.2 *Restructurations territoriales clandestines/criminelles : l'exemple de la Seine-Saint-Denis*

Pour donner un aperçu de la géopolitique du trafic d'armes, Jean-Charles Antoine avait judicieusement choisi d'aborder le cas de la Seine-Saint-Denis, en évoquant l'histoire de la commune mais aussi son développement, notamment en termes d'accessibilité pour la revue Hérodote de 2016[68]. Cette analyse permet de mettre en évidence des causes socio-économiques permettant le développement de trafics illégaux dans certaines régions européennes. Le même portrait peut être dressé dans d'autres États membres de l'Union Européenne, qui pourrait expliquer la circulation massive d'armes dans la zone. Il précise néanmoins que le cas de cette commune ne doit pas, et ne peut pas, être comparé avec les autres communes abritant des trafics d'armes, comme Marseille, Grenoble, Lyon, Toulouse ou encore Lille. Les axes routiers ne sont pas les mêmes, les connexions sont moins nombreuses et l'histoire des communes font également varier leur importance dans le trafic d'armes en France et en Europe. La première particularité de la Seine-Saint-Denis est sa connexion a des axes routiers importants ainsi que son rôle de terminal de cars internationaux. Ainsi, Jean-Charles Antoine explique que ces lignes, souvent nocturnes et soumises à de moindres contrôles, favorisent le transport de Kalachnikov M70AB2 venant de Serbie, des pistolets mitrailleurs Skorpio de République Tchèque et de Slovaquie et des munitions. Ces cars prennent généralement le même itinéraire : Autriche-Allemagne-Alsace-Reims pour arriver dans la périphérie de la capitale, à Porte de Bagnolet. À cela s'ajoute d'autres axes comme les nationales 2, 3 et 4 ainsi que l'autoroute A4.

[67] « Vol d'armes sur une base militaire d'Istres. Quatre suspects écroués », Ouest France, septembre 2016, https://www.ouest-france.fr/societe/justice/vol-darmes-sur-une-base-militaire-distres-quatre-suspects-ecroues-4519296

[68] « Le trafic d'armes en Seine-Saint-Denis : aspects géopolitiques et enjeux », Hérodote, n°162, mars 2016, https://www.cairn.info/revue-herodote-2016-3-page-73.htm, pp. 73-84

Avant même l'intégration du Darkweb dans la région, il y avait donc déjà une présence de réseaux bosniaques, albanophones, belges et serbes qui assuraient l'approvisionnement en armes du territoire depuis la porte de Bagnolet. L'histoire industrielle du département dans les années 1860-1890 jusque dans les années 1940 explique également la disparité de la population comme dans la ville d'Aubervilliers. La variété de population dans les débuts des Trente Glorieuses avec l'accueil de travailleurs d'Afrique du Nord et d'Europe du Sud a pu exacerber certaines rivalités, en y ajoutant le chômage massif qui a été causé lors des différentes récessions, ce qui a laissé une place importante aux activités illégales. Aujourd'hui, ces différents éléments expliquent les causes d'une région de plus en plus sujette à des rivalités ou à de la violence, notamment dans le commerce de drogue, où la Seine-Saint-Denis est bien plus exposée à la concurrence que les régions marseillaise et toulousaine, du fait de la grande connexion de la commune avec d'autres villes clés du trafic (Le Raincy, Bobigny, Bondy, Clichy-sous-bois, Sevran, Alnay-sous-Bois), sans compter les interconnexions avec les départements voisins du Val-d'Oise et de la Seine-et-Marne[69]. L'afflux d'armes par les différentes filiales d'Europe de l'Est et de Belgique ont alors permis de transformer la Seine-Saint-Denis ainsi que les départements voisins en véritable réserve d'ALPC. Néanmoins, il s'avère que la criminalité en Seine-Saint-Denis est davantage liée à des rivalités entre clans, aboutissant le moins souvent à des fusillades, comme il peut y en avoir à Marseille comme par exemple la récente fusillade par une arme de type Kalachnikov du 3 août 2020 sur l'autoroute A7, tuant l'un des conducteurs de 19 ans[70] ou encore celle de juillet 2020 à la rue Consolat[71] de la ville. Il est donc nécessaire de traiter la question du trafic d'armes de manière ciblée et adaptée aux situations des départements visés. En Seine-Saint-Denis, il s'agira avant tout de règlement de compte et de « jambisation » (inspiré de l'expression des mafias italiennes « gambizzazioni »), permettant surtout d'asseoir une autorité sur la « main d'œuvre ».

III.1.2 « Cyber économie souterraine »

Au-delà des conséquences sociales du trafic d'armes, il ne faut pas oublier les tenants économiques d'un tel trafic, considéré comme l'un des plus lucratif après le trafic de drogue.

[69] « Le trafic d'armes en Seine-Saint-Denis : aspects géopolitiques et enjeux », Hérodote, n°162, mars 2016, https://www.cairn.info/revue-herodote-2016-3-page-73.htm, pp. 73-84

[70] « Marseille. Après une fusillade sur l'autoroute A7 et une sortie de route, un homme de 19 ans est mort », Ouest France, août 2020, https://www.ouest-france.fr/provence-alpes-cote-dazur/marseille-13000/marseille-apres-une-fusillade-sur-l-autoroute-a7-et-une-sortie-de-route-un-homme-de-19-ans-est-mort-6926707

[71] Miguet E, « Marseille : trois personnes, dont une jeune femme de manière collatérale, blessés par balles dans la nuit », La Provence, juillet 2020, https://www.laprovence.com/actu/en-direct/6051921/.html

La saisie de portefeuille virtuels ainsi que la fermeture de sites de vente, représentant parfois des millions d'euros, peuvent avoir des répercussions importantes sur l'économie.

III.1.2.1 *Estimation de la valeur du trafic d'armes illégal sur le Darkweb*

L'estimation de la valeur du marché du Darkweb est soumise à certains obstacles, notamment la quantité de plateformes de vente, où le prix peut être différent, mais aussi les différentes techniques de vendeurs consistant à fixer un prix de vente très élevé en cas de rupture de stock ou d'indisponibilité du vendeur pour l'envoi pour pouvoir laisser l'annonce en ligne (on les qualifie d'« holding price »). Cependant, les ventes d'armes mises à part ne génèrent pas autant de revenus que l'achat de données de carte de crédit, d'images pédopornographiques et surtout de drogues. L'activité la plus lucrative revient surtout au trafic d'armes plus traditionnel, qui fonctionne uniquement via des réseaux criminels bien ancrés, des hommes politiques et des industriels de l'armement. Pour dresser un tableau plus précis des sommes engagées pour l'achat d'une arme sur le Darkweb, il a fallu que des chercheurs de RAND Europe récoltent les données de 12 cryptomarkets, afin d'en dégager une valeur moyenne par type d'armes puis par marque d'armes. Étant donné que les ALPC sont bien plus populaires du point de vue de l'offre mais surtout de la demande, il est bien plus facile d'en acquérir une à prix avantageux. Premièrement, les chercheurs ont réparti les ventes d'armes par types, armes à balles réelles, répliques, neuves ou usées et non spécifié. Encore une fois les résultats sont faussés, les vendeurs mettant bien plus en avant les types d'armes à feu à balles réelles que les armes neutralisées, reconverties, ou les armes d'alarme. Dans le cas d'une véritable arme, sur un total de 74 733 dollars de revenus mensuels sur les 12 plateformes, 64 224 dollars reviennent à la vente de pistolets, 2 586 dollars pour les pistolets mitrailleurs et 7 923 dollars pour les carabines. Ils en ont conclu que les modèles les plus vendus étaient des pistolets Glock, Sig Sauer et Taurus (ce dernier étant moins cher) pour des revenus mensuels respectifs de 24 882 dollars, 11 045 dollars et 4 860 dollars. Entre la vente de produits digitaux, de munitions, d'explosifs et d'armes à feu, ces dernières représentent 90% des revenus mensuels du trafic d'armes sur le Darkweb[72]. Cependant, les chercheurs affirment leur limite dans une estimation précise du poids du trafic d'armes sur le Darkweb, étant donné qu'ils ne prennent pas en compte les sites de vendeurs indépendants ainsi que d'autres cryptomarkets nationaux. En effet, comme French Deep Market, French Armory ou encore la plateforme finlandaise Sikklitie, certains

[72] Persi Paoli. G, Aldridge. J, Ryan. N, Warnes. R, « Behind the Curtain, the illicit trade of firearms, explosives and ammunition on the dark web », RAND Europe, 2017, pp 44

produits ont pu passer entre les mailles du filet. La quantification des transactions, certainement sous-estimée, paraît étonnante surtout après qu'Europol ait estimé la quantité d'armes en circulation de 3 à 6 millions, seulement en Europe. Ces transactions peuvent également paraître mineures, mais si on établit la clientèle principale du Darkweb, il ne s'agit pas de transactions mondiales mais régionales, principalement européenne, à l'exception de l'Australie qui compte pour une part infime des transactions totales. Ainsi, ce sont plusieurs centaines d'armes à feu et de munitions par mois, qui sont vendues grâce à un Darkweb qui ne cesse de gagner du terrain à mesure que les régions se développent. C'est ce dernier point qui a également inquiété l'ancienne Secrétaire Générale adjointe et Haute représentante pour les affaires de désarmement Izumi Nakamitsu, concernant le développement du numérique dans des régions animées par des conflits et de la pauvreté, qui pourraient profiter à la popularité des ALPC sur le Darkweb. Il est encore difficile de donner un chiffre précis au cybertrafic d'armes, mais les nouvelles compétences d'enquête, les nouveaux outils ainsi que le développement d'une population sensibilisée pourrait permettre de mieux quantifier et évaluer l'importance du cybertrafic d'armes, dont l'estimation devient de plus en plus importante pour l'élaboration d'opérations internationales concrètes.

Une sous-estimation qui ne se démontre rien qu'avec une analyse approfondie du cas français. La société Trend Micro s'est intéressé de près à la cybercriminalité française, et y a identifié environ 40 000 vendeurs. On peut y retrouver des produits à des prix bien plus compétitifs que ceux repérés dans les différents cryptomarkets internationaux. Les produits iront de 10 à 150 euros pour des armes blanches discrètes comme des stylo-pistolets, teasers, points américains ou des couteux de petits format, mais aussi des kits d'impression 3D pour une bouchée de pain ainsi que des armes lourdes allant de 650 euros à près de 2000 euros.[73] On y estime un chiffre d'affaire allant de 5 à 10 millions d'euros par mois, une part négligée dans l'étude de l'économie souterraine dans le PIB national.

III.1.2.2 *Influence du Darkweb sur l'économie*

L'économie souterraine a longtemps bénéficié de l'étude d'économistes afin d'en comprendre la teneur et l'importance dans les économies. En 2017, l'Institut National des Statistiques a estimé qu'elle représentait 19,5% du Produit Intérieur Brut (PIB) en Italie et 12% du PIB en France en 2019 selon le Conseiller d'Orientation pour l'Emploi, qui ne prennent même pas en

[73] S. Rolland, « Cybercriminalité : qui sont les escrocs du darknet français ? », La Tribune, septembre 2016, https://www.latribune.fr/technos-medias/cybercriminalite-qui-sont-les-escrocs-du-darknet-francais-599111.html

compte les transactions illégales du Darkweb. Le Darkweb en France rapporte entre 5 et 10 millions par mois à environ 40 000 revendeurs (il faut néanmoins prendre en compte la disparité des vendeurs sur le darkweb, certains amateurs auront tendance à disparaître sous une concurrence accrue, il se peut que quelques centaines de vendeurs sur le 40 000 estimés détiennent la majorité de ces revenus). En 2018, le marché noir de la drogue prend une ampleur telle que la l'INSEE souhaitait intégrer les ventes du type dans le PIB national. Ce changement permettrait d'augmenter le PIB français de quelques milliards d'euros (une augmentation de 0,1 point contre une augmentation du PIB britannique de 10,9 milliards d'euros en 2013). [74] Cette prise en compte permettrait par exemple d'augmenter sensiblement le budget accordé par la France à l'Union Européenne. Le Darkweb sera également amené à être étudié avec plus de précision, comme le demandait le Secrétaire Générale des Nations Unies et l'adjoint du Secrétaire Général, comme peut en témoigner les missions de cyberpatrouilles déployées de façon régulière sur les plateformes. Même si le Darkweb et ses places de marché redoublent d'ingéniosité pour échapper aux autorités, les innovations en matière de cyber espace et de cybersécurité pourrait permettre d'apporter des chiffres plus précis sur l'économie souterraine représentée par le Darkweb. Il est également possible d'avoir un ordre d'idée sur l'importance du Darkweb via le cours du Bitcoin, bien que cette information soit limitée avec l'utilisation d'autres crypto-monnaies telles que Monero, Dash ou ZCash. Rien que pour la monnaie Bitcoin, des chercheurs de l'Université de Sydney et l'Université de Technologie de Sydney ont démontré que 44% des transactions Bitcoin étaient associées à des activités légales, principalement sur le Darkweb, ce qui pourrait représenter environ 24 millions de participants au marché Bitcoin[75]. Les différentes saisies des autorités de portefeuille Bitcoin pourrait également conduire à un désintérêt pour les cybercriminels pour cette monnaie, qui privilégieraient des alternatives.[76] La valeur du Bitcoin serait alors impactée de manière conséquente. Sa valeur a connu un pic en 2018 (16 721 euros = 1 bitcoin contre environ 8 370 euros en juin 2020). Les efforts des autorités pour briser la confiance des criminels dans le système de Darkweb en passant par les cryptomonnaies et les saisies de sommes importantes, pourrait alors avoir un impact éthique important pour les usagers y voyant un investissement

[74] « Trafic de drogue intégré au PIB : ce que ça va changer pour la France », Capital, février 2018, https://www.capital.fr/economie-politique/trafic-de-drogue-integre-au-pib-ce-que-ca-va-changer-pour-la-france-1269283

[75] Sulleyman A, « Bitcoin price is so high because criminals are using it for illegal trades, research suggests », The Independant, janvier 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-fall-criminals-blockchain-anonymous-cryptocurrency-zcash-monero-dash-a8174716.html

[76] Popper N, « Bitcoin Has Lost Steam. But Criminals Still Love It. », The New York Times, janvier 2020, https://www.nytimes.com/2020/01/28/technology/bitcoin-black-market.html

d'avenir. La chute de la valeur du Bitcoin aurait des conséquences économiques certaines. Il pourrait être risqué de procéder à ses saisies massives de bitcoin de la part des autorités, qui peuvent avoir un impact sur le cours.

III.2 Innovations dans les mesures de contrôle des trafics illégaux

III.2.1 Mesures préventives et contrôle des marchandises susceptibles d'être échangées sur le dark web

La valeur du trafic d'armes sur le Darkweb pourrait donner l'impression qu'il est moins dangereux que les estimations des experts sur le sujet. Pourtant, bien que la majorité des transactions reviennent à la vente de drogue, de données bancaires ou d'images pédopornographiques, le trafic d'armes tue déjà lors d'attentats et contribue à l'insécurité dans les pays développés et bientôt dans les pays en développement, si le Darkweb s'exporte dans de nouvelles régions.

III.2.1.1 *Contrôle des nouvelles technologies (imprimantes 3D) et de la vente d'armes non létales sujettes au reconditionnement*

La diffusion d'armes intraçables issues des technologies d'impression 3D, légales aux États-Unis ont fait leur chemin jusqu'en Europe[77]. Face à l'augmentation de ces armes « invisibles », de nombreuses réglementations commencent à émerger, même aux États-Unis. Avec la crise du Coronavirus, la vente d'armes a explosé, ce qui a mené plusieurs sénateurs à introduire une loi visant à l'interdiction des armes « fantômes », qui empirent la situation internationale du trafic d'armes.[78] Il s'agira donc d'obtenir une licence de fabricant et d'intégrer un numéro de série sur les pièces. L'acte relatif aux armes à feu intraçables propose aussi l'interdiction d'armes pouvant passer les postes de sécurité des douanes sans être détectées. Il faut noter que seuls 15 sénateurs américains supportent ce projet de loi, pouvant alors délocaliser les activités de production dans d'autres États. Cette mesure pourrait avoir un impact sur la diffusion et la création de telles armes, facilement exportable sur le trafic d'armes européen. Les armes à feu fabricables en kit bénéficieront également de contrôle grâce au traçage de pièces détachées,

[77] « VIDÉO : Des armes en kit ou fabriquées avec des imprimantes 3D : un phénomène inquiétant aux États-Unis », LCI, février 2020, https://www.lci.fr/international/video-des-armes-en-kit-ou-fabriquees-avec-des-imprimantes-3d-un-phenomene-inquietant-aux-etats-unis-2144715.html

[78] *The Untraceable Firearms Act of 2020,* Richard Blumenthal United States Senator for Connecticut, 2020, http://www.blumenthal.senate.gov/imo/media/doc/Untraceable%20Firearms%20Act%20of%202020%20-%20OnePager%20-%20200513.pdf

permis par le programme iARMS. Ce dernier permet de tracer automatiquement les armes saisies ou trouvées ainsi que de les analyser dans des laboratoires scientifiques pour en déterminer les vendeurs et les acheteurs.[79] Le Réseau d'Information balistique d'INTERPOL permet également d'échanger des données balistiques à l'international pour permettre de faire évoluer les enquêtes grâce à une coopération internationale pour mettre la main sur des réseaux de trafiquants[80].

Suite aux attentats de 2015, de nouvelles directives européennes ont permis de contrôler les processus de reconversion des armes non létales. Elles agissent notamment sur les entités pouvant procéder à ces neutralisations et tentent d'homogénéiser les procédures, qui se différenciaient entre la Slovaquie et l'Allemagne par exemple. Cette directive a également revu les critères concernant la qualification d'une arme définitivement inutilisable ainsi que les marquages, qui devraient être appliqués de sorte à ce qu'ils soient impossibles à modifier ou effacer par les trafiquants. Elle demande aussi que chaque pays de l'Union Européenne possède un marquage différent afin d'aider les autorités à en identifier la provenance. L'utilisation d'armes retroconverties lors des attentats a également amené l'Union Européenne a repenser leur qualification, les définissant dorénavant comme des armes à feu de catégorie C, correspondant à leur catégorie d'origine avant d'être neutralisées. Cette modification implique une déclaration obligatoire de toutes les armes à feu neutralisées en rendant la vente d'armes neutralisées à capacité de tir automatique interdite. Cette directive ne fait pourtant pas mention d'une quelconque destruction d'armes issues de stocks gouvernementaux excédentaires. Les États gèrent seuls leur législation concernant la destruction de ces armes pouvant être reconverties (le cas des fusils militaires espagnols des années 1970 par exemple). L'OSCE (Organisation pour la Sécurité et la Coopération en Europe) encourage les États à privilégier une destruction plutôt qu'une neutralisation de ces armes excédentaires, étant donné que les trafiquants ont pu montrer leur capacité d'inversion du processus, recommandation réitérée par le Programme d'action des Nations Unies. Concernant les pistolets d'alarme pouvant être reconvertis, la Commission Européenne s'entretenait avec des industriels des armes d'alarme en 2017 concernant les spécifications techniques des armes pouvant être reconverties. En 2019, cette réunion aboutit à la « directive d'exécution 2019/69 de la commission établissant des

[79] « Illicit Arms Records and tracing Management System (iARMS) », Interpol, https://www.interpol.int/Crimes/Firearms-trafficking/Illicit-Arms-Records-and-tracing-Management-System-iARMS

[80] « IBIN : le Réseau d'Information balistique d'INTERPOL », Interpol, janvier 2017, https://www.interpol.int/Crimes/Firearms-trafficking/Illicit-Arms-Records-and-tracing-Management-System-iARMS

spécifications techniques relatives au marquage des armes d'alarme et de signalisation au titre de la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes »[81]. Cette directive revient sur certaines pièces d'armes d'alarme régulièrement sujettes à des conversions, visant par exemple à ne pas pouvoir modifier ou enlever les canons sans que cela endommage l'arme de manière irréversible et autres détails techniques modifiant la structure générale de ces armes depuis les usines de fabrication.

III.2.1.2 *Renforcement du contrôle terrestre sur les frontières et « territoires pivots »*

En 2019, Interpol, dans le cadre du programme iARMS publie un protocole à suivre en cas de saisie d'armes par les autorités. Ce protocole est le produit d'une révision d'Interpol sur la stratégie à employer pour mettre un terme à des réseaux entiers de vente d'armes dans le cadre du Programme sur les armes à feu. Il vise avant tout à promouvoir la mise en commun des informations collectées par les forces de police et les laboratoires scientifiques. La saisie d'armes à elle seule ne suffisant plus pour résoudre durablement le trafic, il est important de rassembler différents éléments d'identification extérieurs de l'arme, comme la marque, le calibre, le numéro de série et le modèle afin de reconstituer son itinéraire. Les laboratoires récoltent de l'ADN, des empreintes digitales qui permettront de remonter à la source des trafics. Si une arme saisie n'est pas enregistrée dans les fichiers iARMS, une enquête de traçage est lancée par le pays membre concerné, en faisant appel à la coopération d'autres États membres d'où pourrait provenir l'arme.[82]

À l'échelle nationale, le Ministère de l'Intérieur s'était prononcé sur les nouvelles mesures entreprises afin de lutter concrètement contre l'entrée d'armes illégales sur le territoire, grâce à des réformes des structures de contrôle, permettant de destabiliser des filières de trafic d'armes ainsi que de renforcer la traçablité des armes. D'un point de vue opérationnel, il s'agissait avant tout de renforcer les contrôles et la coordination de la police, la gendarmerie et les douanes dans les lieux d'accès au territoire, comme les aéroports et les zones portuaires.[83] D'autres innovations comme les cyberpatrouilles à l'échelle nationale ainsi que l'identification des principaux axes routiers permettront de mieux intercepter les différentes filières. Il s'agissait

[81] *Directivce d'exécution (UE) 2019/69 de la Commission du 16 janvier 2019 établissant des spécifications techniques relatives au marquage des armes d'alarme et de signalisation au titre de la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes,* Journal Officiel de l'Union Européenne, Eur-Lex, janvier 2019, https://eur-lex.europa.eu/homepage.html?locale=fr

[82] *Protocole à suivre en cas de découverte d'armes à feu : rassembler, partager et analyser toutes les informations sur la criminalité liée aux armes à feu afin de lutter contre le terrorisme, les auteurs de crimes violents et les trafiquants d'armes,* Interpol, 2019

[83] « Contrôle du trafic d'armes de guerre en France », Sénat, mars 2016, https://www.senat.fr/questions/base/2016/qSEQ160320877.html

également de faire des « coups d'achat » en reproduisant les stratégies employées pour le démantèlement de trafic de drogues pour tenter de les infiltrer.[84] En 2018, les efforts du Ministère de l'Intérieur et des Douanes ont permis de saisir 1 363 armes à feu, soit 42,3% de plus que l'année précédente et pas moins de 100 kg de munitions.[85]

III.2.2 Adaptation de la scène internationale aux nouveaux outils de commerce

Les innovations juridiques et les réinterprétations des priorités de la scène internationale en matière d'identification des menaces sur le web ont permis de faire évoluer les institutions en charge de la cybersécurité en les incluant davantage dans les questions de sécurité publique. Ainsi, l'intégration de hackers, cyberexperts, des cyberpatrouilleurs dans les forces de police mais aussi dans les différentes structures de sécurité publique ces dernières années ont permis de montrer des résultats encourageant pour le contrôle du marché noir en ligne. Bien plus qu'auparavant, la communauté d'utilisateurs internet peut également être sollicitée pour la sécurité publique.

III.2.2.1 *Progrès des autorités pour le contrôle du cyberespace et des cybercrimes : l'exemple de Hansa*

L'une des plus grandes preuves d'adaptation des autorités face à la nouvelle menace que représentait le Darkweb est sans aucun doute le démantèlement de la plateforme Hansa.

La police Néerlandaise en collaboration avec la police Allemande avaient réussi à prendre la place des administrateurs, grâce à une stratégie expliquée pour la première fois en détail pour une telle opération, qui ont alors pu enregistrer chaque mot de passe des utilisateurs, ayant accès aux adresses de chaque acheteur. Ils ont également fait en sorte que les metadonnées des photos partagées des produits en vente ne soient pas supprimées automatiquement du site, leur permettant même d'activer la géolocalisation sur les photos prises. Ce succès a été permis grâce à l'intégration de société de cybersécurité dans le processus d'enquête comme BitDefender, bien qu'aucune entreprise n'ait été officiellement annoncée par la National Hi-Tech Crime Unit (NHTCU). La société de sécurité avait réussi à trouver les serveurs de développement de Hansa et avait réussi à mettre la main sur une version béta (version du site qui permettait de tester

[84] « Comment l'intérieur entend lutter contre le trafic d'armes », l'Obs, novembre 2015, https://www.nouvelobs.com/societe/20151113.OBS9363/comment-l-interieur-entend-lutter-contre-le-trafic-d-armes.html

[85] *Résultats 2018,* Douanes & Droits Indirects, Ministère de l'Action et des Comptes Publics, 2019, https://www.douane.gouv.fr/sites/default/files/uploads/files/2019-04/douane-resultats-2018.pdf

certaines fonctionnalités avant de le mettre en ligne). Les autorités néerlandaises ont alors pu prendre contact avec l'hébergeur Web afin de demander l'accès au centre de données et d'installer un système de surveillance sur le réseau. La police néerlandaise a pu espionner tout le trafic entrant et sortant de cet hébergeur, ce qui a permis de découvrir le serveur de développement du site ainsi que d'autres serveurs localisés en Allemagne. Enregistrer l'historique des transactions Hansa et des conversations hébergées sur le site n'a pas été très compliqué par la suite. L'identification exacte des administrateurs a pu être faite grâce aux toutes premières conversations de la plateforme entre les deux administrateurs, où ils renseignaient leur nom complet et même l'adresse d'un des deux. Les deux Allemands étaient déjà suspectés pour la diffusion de livres électroniques piratés par les autorités allemandes, ce qui permettait aux suspects d'être arrêtés pour ce motifs et laissait le champ libre pour la police néerlandaise de prendre la place des administrateurs. Bien que le stratagème de la police ait fuité et enclenché le silence radio sur la plateforme et le transfert de l'activité sur un autre serveur Tor, ils ont quand même décidé d'éplucher l'historique des transactions et de chercher des informations quant aux identités des utilisateurs. Ils ont choisi de laisser la plateforme fonctionner pour localiser les nouveaux serveurs afin de les détourner. Une transaction en 2017 effectuée en Bitcoin à partir d'une adresse déjà renseignée dans la messagerie a permis de retracer la transaction grâce au logiciel Chainalysis. Parallèlement, le FBI avait pu mettre la main sur les serveurs de l'autre géant AlphaBay, qui a provoqué un afflux d'utilisateurs sur Hansa (5000 nouveaux utilisateurs), qui était alors sous contrôle de la police néerlandaise. La police allemande se saisit des disques durs non cryptés des deux suspects, et aide la police néerlandaise a rediriger les serveurs du sites vers un serveur contrôlé intégralement par la police des Pays-Bas. Ce coup-ci, personne ne soupçonnait le site d'être sous contrôle des autorités. A partir de là, ils ont pu réecrire le code du site pour enregistrer toutes les photos, tous les mots de passe, toutes les discussions entre acheteurs et vendeurs, permettant de créer un carnet d'adresse conséquent, en plus des données de localisation fournies par les photos, ce qui a renseigné la localisation de 50 vendeurs majeurs. Le dernier « coup de maître » de la NHTCU a été de créer un fichier permettant d'avoir accès au Bitcoin dus après 90 jours, même si le site fermait ou tombait en panne. Lorsque le vendeur suivait le lien en question, son adresse IP était révélée à la police. Ils ont pu identifier 64 vendeurs supplémentaires de la sorte. Tenus de renseigner chaque transaction à Europol, la police néerlandaise a rapidement été submergée par les 1000 transactions moyennes quotidiennes. En 27 jours, elle a enregistré 27 000 transactions et a décidé de procéder aux arrestations en communiquant les adresses aux services de police des États concernés (au moins 10 000) par le biais d'Europol. 12 millions de dollars de Bitcoin

ont été saisis malgré la protection établie par les anciens administrateurs de Hansa concernant les transactions multi-signatures grâce au sabotage du site par la police[86]. Les vendeurs repérés sur Hansa ont été dissuadés de se relocaliser sur une autre plateforme, à l'inverse des vendeurs AlphaBay qui s'étaient rendus sur d'autres sites. Les autorités responsables de la fermeture de Hansa ont réussi le pari de briser la confiance de ses utilisateurs pour les dissuader d'y avoir recours. Une telle opération est amenée à être reconduite, le Darkweb étant constamment animé par le commerce illicite, très lucratif.

III.2.2.2 *Sensibilisation et contribution de la population*

En 2001, les Nations Unies publient le *Rapport de la Conférence des Nations Unies sur le Commerce Illégal d'Armes de Petit Calibre et d'Armes Légères dans Toutes Ses Formes*[87], l'Organisation mentionne explicitement l'importance de la société civile dans les efforts généraux de lutte contre le trafic d'armes, que ce soient les organisations non-gouvernementales et les industries. Pour ce faire, elle appelle les États membres à renforcer la sensibilisation de leurs populations aux dangers de tels trafics tout en établissant une confiance de la part des civils dans les programmes d'éradication de ces trafics. Enfin les Nations Unies appellent les insitutions de santé, les institutions financières internationales et les centres de recherche à se pencher sur les conséquences du trafic d'armes illicites sur les sociétés et leur économie, afin de permettre une meilleure compréhension générale des enjeux d'un tel trafic sur la sécurité des civils. Au niveau des organisations non-gouvernementales, l'International Action Network on Small Arms (IANSA) prend part à des conférences des Nations Unis en tant que membre consultatif au sein du Conseil Economique et Social (ECOSOC), composée en majorité de civils. D'autres organisations comme Armement Research Services, composée de professionnels des industries de l'armement, de complexes scientifiques et d'autres secteurs stratégiques pour la lutte contre le trafic d'armes s'engage dans le conseil pour des structures gouvernementales et non-gouvernementales et propose des publications mensuelles accessibles à tous afin de faciliter l'accès à l'information dans le domaine de l'armement. A plus petite échelle, le programme iARMS invite les particuliers à tracer leur arme. De plus, en 2019 le gouvernement Français a introduit le Système d'Information sur les Armes, permettant de contrôler les armes légales en France (SIA). D'autres associations permettent d'informer la

[86] Greenberg A, « Operation Bayonet : Inside the Sting That Hijacked an Entire Dark Web Drug Market », Wired, août 2018, https://www.wired.com/story/hansa-dutch-police-sting-operation/

[87] *Report of the United Nations Conference on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects,* United Nations, juillet 2001, https://www.un.org/events/smallarms2006/pdf/N0150720.pdf

population sur les procédures à suivre en cas de détention illégale d'armes, de détention d'arme non déclarée issu d'un héritage ou découverte d'une arme perdue supposée être neutralisée ou rendue à un armurier compétent. On retrouvera par exemple l'association de l'Union Française des Amateurs d'Armes (UFA). Dans d'autres cas, comme au Danemark ou aux Pays-Bas, le gouvernement incite sa population à rendre des armes neutralisées ou non déclarées contre une petite commission.

Lorsque les utilisateurs ne souhaitent pas se rendre sur le Darkweb, ils ont toujours la possibilité d'agir sur les réseaux sociaux, qui peuvent accueillir des annonces de vente d'ALPC. Les algorithmes de détection de contenus malveillants sont aussi ajustés et développés pour accompagner les contributions humaines.

III.2.2.3 *Quelques risques à prévoir*

Malgré les progrès de la scène internationale et des institutions internationales dans la détection et le contrôle d'armes en vente sur le web, certains éléments devraient être mis en lumière concernant un retour en popularité du Darkweb pour le commerce d'armes. La crise du COVID-19 aux États-Unis a eu une incidence historique sur les ventes d'armes aux États-Unis se traduisant par un pic des ventes dès mars 2020, certains vendeurs voyant parfois leurs ventes augmenter de 1000%[88]. Or, les ventes massives d'armes par le passé ont souvent été traduites par une offre plus importante d'armes sur les réseaux ou le Darkweb, que ce soient les mains-mises sur des stocks gouvernementaux, ou des braquages de vendeurs d'armes, ces éléments venaient souvent impacter l'offre sur le Darkweb, la propagation d'armes sur le territoire a généralement un effet de cercle vicieux provoqué par un sentiment d'insécurité menant à l'armement d'autres citoyens. C'était le cas en 2016, à la suite des attentats en France, où des Français souhaitaient également s'armer à cause des menaces terroristes[89].

Les mesures de traçabilité engagées par l'Union Européenne et ses partenaires est engageante mais ne permettra pas de rappeler les quelques millions d'armes circulant dans les Balkans. Si la production et la reconversion d'armes illégales va certainement être empêchée, de nombreux sites de vente légaux proposent toujours des carcasses et des culasses permettant de convertir des armes telles que NaturaBuy, Ebay et même Leboncoin. L'épisode de Hansa était réussie, mais comme le précisaient les messages sur différents forums, « les choses vont se stabiliser,

[88] Gruet M, « Le coronavirus provoque une ruée sur les armes en Californie », Le Parisien, mars 2020, https://www.leparisien.fr/international/le-coronavirus-provoque-une-ruee-sur-les-armes-en-californie-25-03-2020-8287503.php

[89] « Enquête sur ces Français qui veulent s'armer », L'Obs, octobre 2016, https://www.nouvelobs.com/societe/20161031.OBS0569/enquete-sur-ces-francais-qui-veulent-s-armer.html

elles le font toujours »[90], ce qui montre une véritable détermination de continuer d'utiliser les marchés noirs, en redoublant de stratégies que les autorités devront être en mesure de prévoir et de contrecarrer. Le problème des armes imprimées en 3D et en kits posent aussi un véritable problème aux frontières et sur le web puisqu'elles sont facilement dissimulables sur internet et le Darkweb et lors des passages aux frontières. Bien que la communauté internationale depuis 2017 ait engagé des procédures de traçabilité, comme le SIA, iARMS, il se pourrait qu'autant de mesures attisent la méfiance des trafiquants qui pourraient se traduire par des comportements tout à fait imprévus. Déjà, la crainte d'une baisse de confiance des trafiquants pour le Bitcoin et leur migration vers des monnaies virtuelles moins répandues comme Monero, CashZ et Ethereum pourrait encore ralentir le travail des experts pour des futures opérations de démantèlement semblables à Hansa. Comme à chaque progrès des autorités dans la rupture d'anonymat, les cybercriminels peuvent avoir recours à des outils toujours plus perfectionnés, comme il était possible d'observer avec les services de messagerie cryptée comme Wire, Keybase ou Telegram, censées contourner le contrôle des autorités. Il faudrait également s'intéresser aux répercussions économiques si 43% des utilisateurs Bitcoin, procédant à des transactions illégales, se détournaient de la monnaie au profit d'une autre pour les 47% restants.

[90] Greenberg A, « Operation Bayonet : Inside the Sting That Hijacked an Entire Dark Web Drug Market », Wired, août 2018, https://www.wired.com/story/hansa-dutch-police-sting-operation/

CONCLUSION

Le Darkweb a réussi à se faire une place dans le marché noir international en alliant les avantages de la mondialisation des télécommunications et les innovations en termes de transactions cryptées. Un cadre idéal pour une biosphère criminelle qui semblait avoir besoin d'un renouveau et d'un nouveau souffle. Entre l'évolution des connexions à travers le monde, amenées à augmenter dans les années suivantes, et le virage progressif vers les cryptomonnaies, les criminels avaient simplement besoin de tendre le bras pour avoir accès à une clientèle internationale. Les nouvelles technologies de conception et les nouvelles compétences de conversion d'armes ont permis de donner un poids dangereux à un commerce quantitativement inférieur au trafic de drogues ou aux fraudes financières. En 2015, les attentats en Europe, causés par des armes achetées sur le Darkweb avaient confirmé l'essor d'un marché noir qui devenait létal. Ces attentats avaient cependant permis à l'Union Européenne, aux agences de police nationales et internationales et aux Nations Unies d'unir leurs forces pour lutter contre une menace, présente à la fois dans le cyberespace et au sein de la population. La réponse internationale a permis de montrer une communauté internationale soudée mais surtout réactive et à la page des stratégies des cybercriminels, qui a su concilier des efforts de contre-ingérence dans le cyberespace et des mesures opérationnelles concrètes de la part des gouvernements concernés.

Au cours des dernières années, les institutions internationales et les gouvernements européens ont accordé une importance toute particulière à la prolifération d'ALPC et d'armes de guerre dans leurs territoires grâce au web. Ils y ont vu à juste titre une menace à laquelle ils n'étaient pas encore préparés et qu'ils avaient peut-être même sous-estimé en Europe. Il faut pourtant souligner la rapidité avec laquelle l'Union Européenne, notamment la France, ont souhaité mener des décisions internationales pour le contrôle des armes et du Darkweb, afin d'éviter une nouvelle fusillade de Munich ou un nouveau *Charlie Hebdo*. De 2014 à 2016, le trafic d'armes sur le Darkweb était une véritable menace, qui avait véritablement fait des victimes mais qui avait également enclenché une vague de sentiment d'insécurité, qui pouvait mener à un armement clandestin de la population. Si la résolution du trafic d'armes en lui-même est en passe d'être pris en main de manière efficace, il pourrait y avoir des conséquences connexes, tout aussi négatives. Le démantèlement et la saisie de cryptomonnaies des trafiquants pourrait avoir des conséquences économiques, impliquant un mouvement de fonds vers des cryptomonnaies moins connues des autorités et impliquant une chute de la valeur du Bitcoin, ce qui se traduirait par d'importantes pertes pour les investisseurs honnêtes. Il faudrait aussi

être en mesure de garder un œil sur les compétences des utilisateurs du Darkweb, qui s'adaptent également aux techniques des forces de l'ordre pour la clôture des sites illicites, dont la création est encore impossible à enrayer.

Il convient également, à l'avenir, de comprendre la sociologie ainsi que les différents évènements internationaux qui peuvent enclencher un retour des trafics d'armes légères. Au même titre que le terrorisme ou les cyberattaques, le trafic d'armes doit avant tout être anticipé par les autorités pour permettre un contrôle optimal. Que ce soit la crise sanitaire internationale ayant poussé les Américains à s'armer en grande quantité ou encore des conflits remettant le trafic d'armes au goût du jour en Ukraine, il faudrait être en mesure d'identifier les origines des nouvelles offres sur ces marchés noirs. Les conflits libyen et syrien ont déjà montré l'importante responsabilité des États belligérants dans les futurs trafics, notamment lors de leurs retraits précipités, laissant des stocks d'armes et de munitions importants derrière eux.

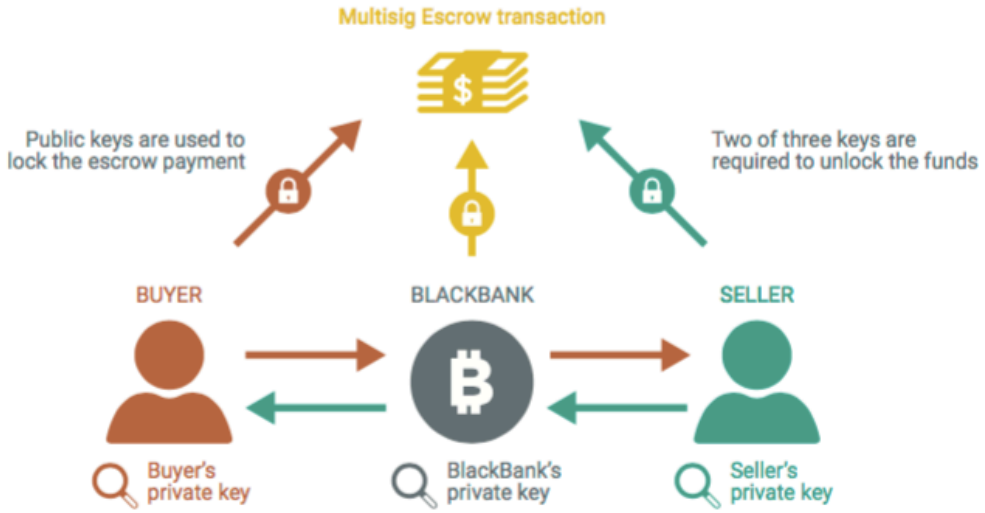
La qualification du trafic d'armes sur le Darkweb est encore sujet à débats auprès des experts, y voyant parfois une crise de confiance envers les représentants, pouvant alors gangréner la stabilité des États Européens, ou parfois un intérêt passager, que les autorités auront vite fait d'atténuer.

En d'autres termes, la communauté internationale a été capable d'identifier le cyber trafic d'armes comme une menace sérieuse suffisamment à temps pour l'empêcher d'être dépassée tout en permettant aux délinquants de se sentir légèrement moins invincibles sur le web.

ANNEXES

Annexe 1 : Fonctionnement des transactions Escrow simple et à signatures multiples

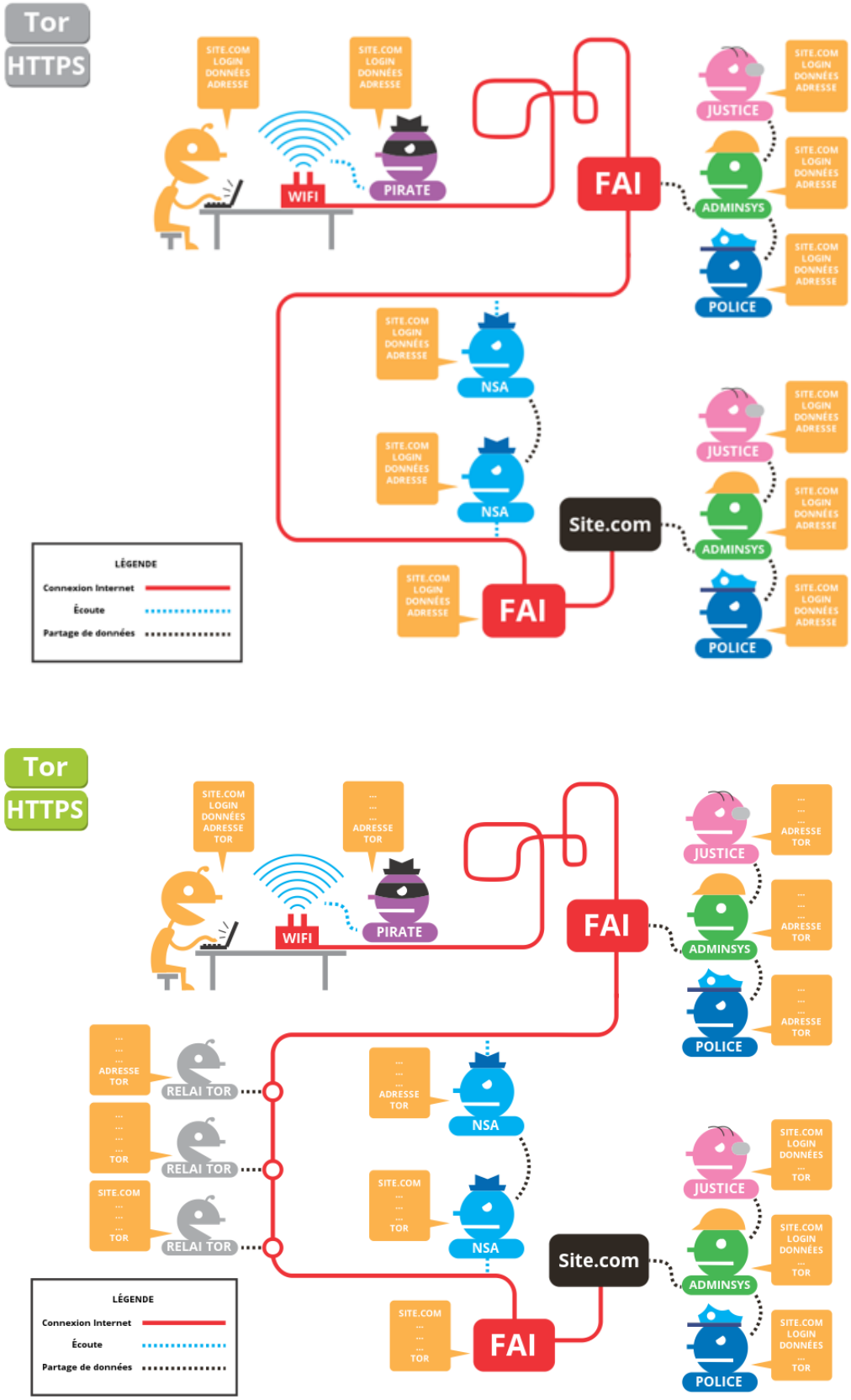
Source: adapted from Kujawa (2014)



Source: adapted from Deepdotweb (2014c)

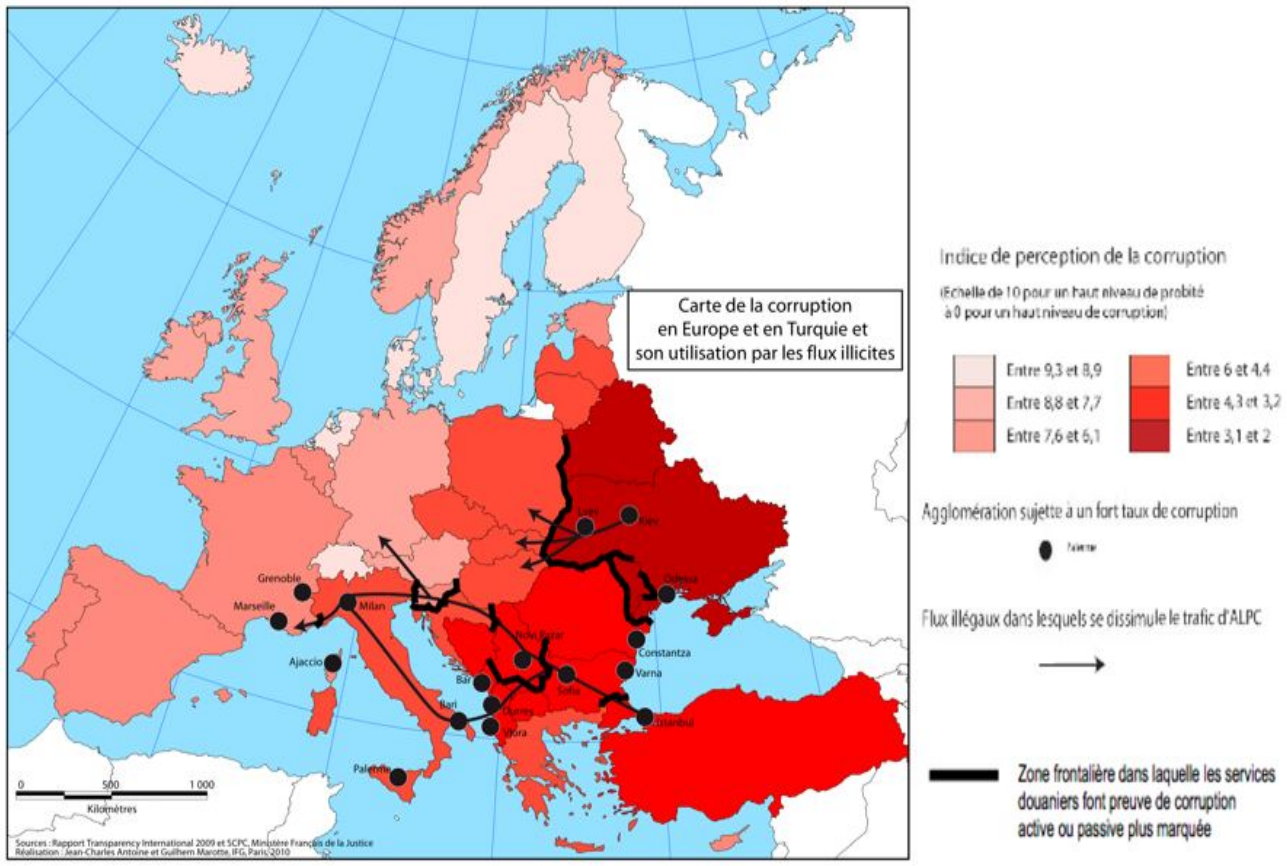
Source : Persi Paoli Giacomo, Adridge Judith, Ryan Nathan, Warnes Richard*, Behind the Curtain : the illicit trade of firearms, explosives and ammunition on the dark web,* RAND Europe, Cambridge, 2017, pp 20

Annexe 2 : Exemple de connexions sans et avec Tor



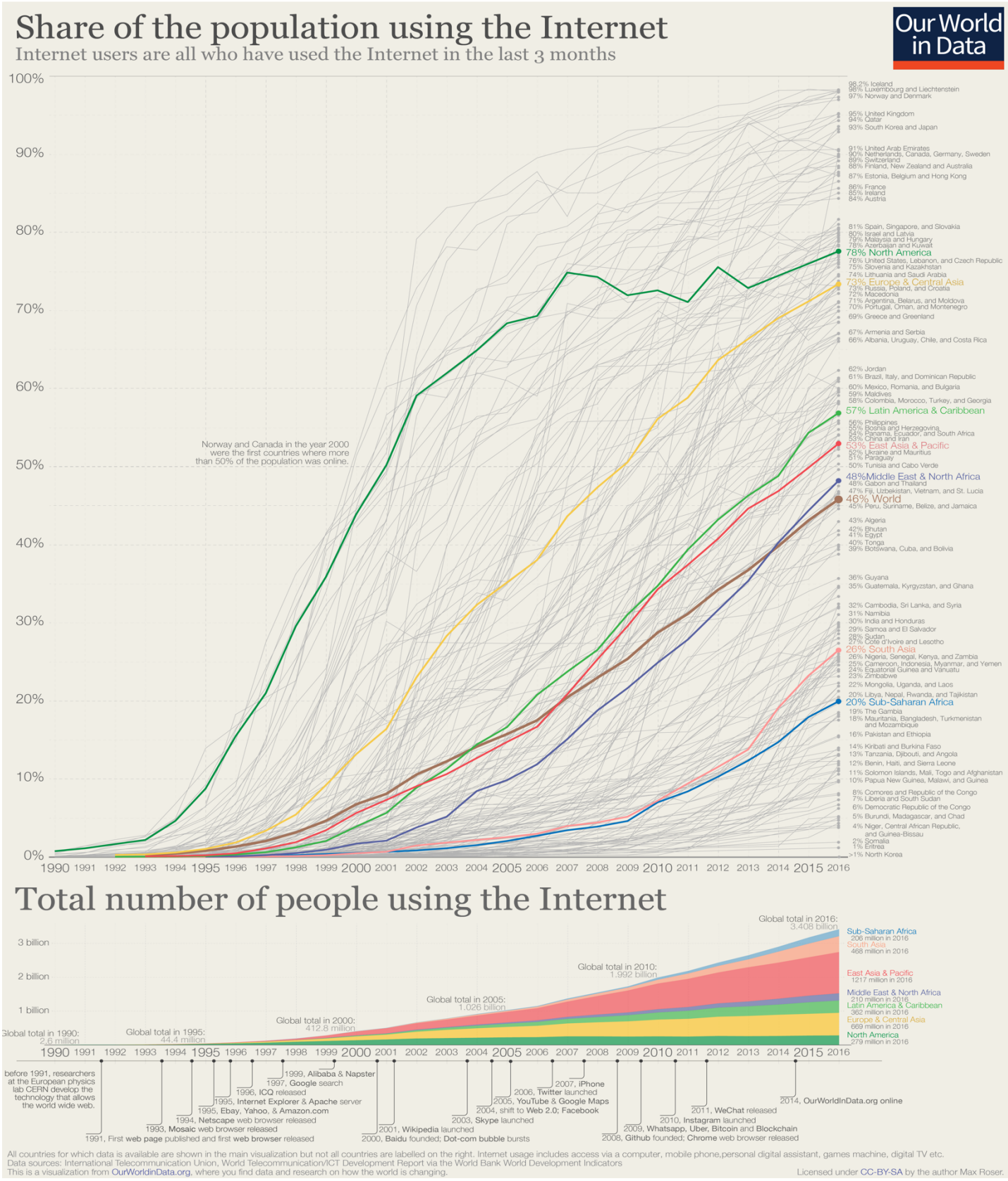
Source : « l'anonymat en ligne avec Tor », Framablog, mai 2016, https://framablog.org/2016/05/06/anonymat-en-ligne-nos-oignons/

Annexe 3 : Carte de la corruption en Europe et en Turquie et son utilisation par les flux illicites



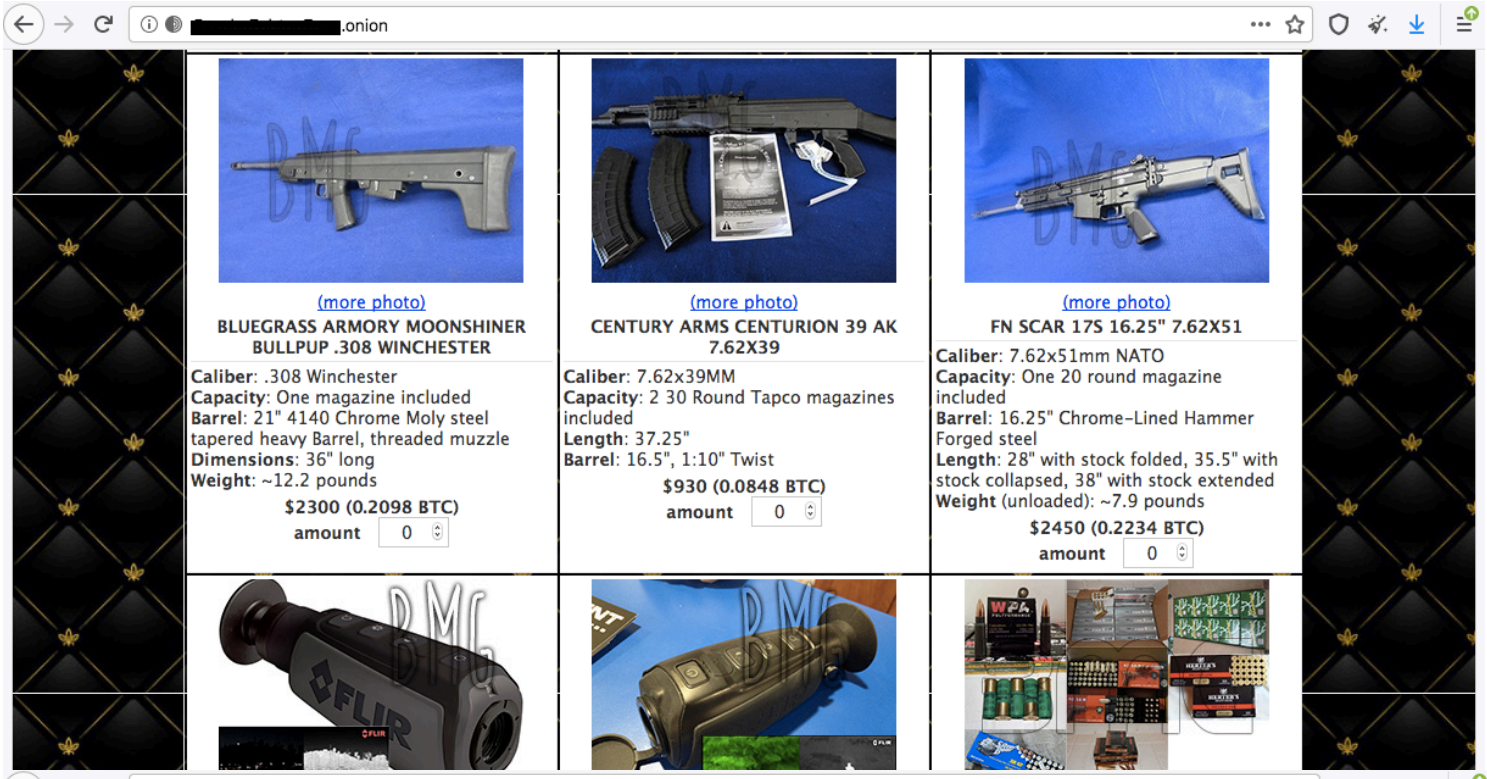
Source : Antoine Jean-Charles, « Frontières et trafic d'armes », Diploweb, mars 2015, https://www.diploweb.com/Frontieres-et-trafic-d-armes.html

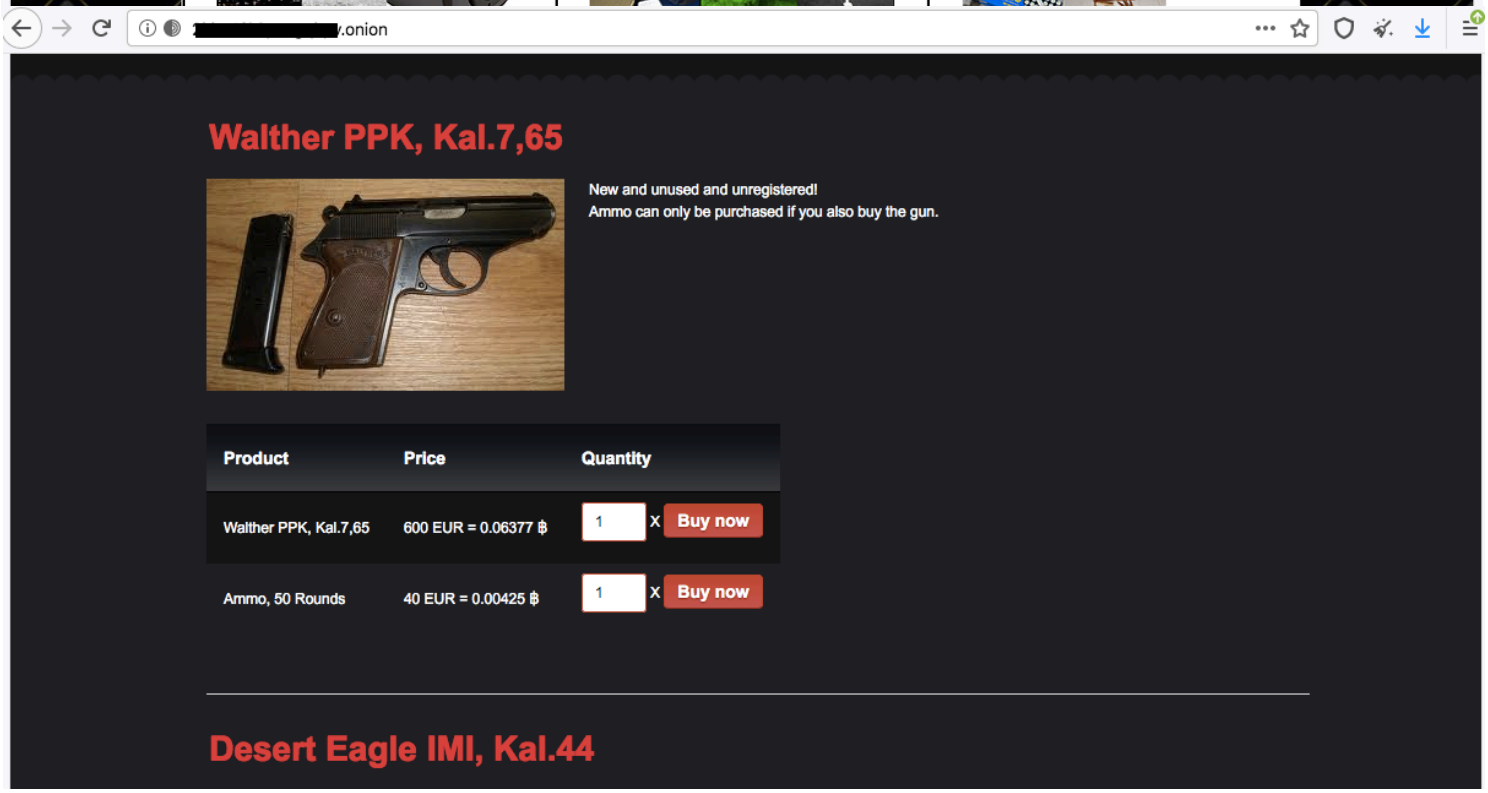
Annexe 4 : Part de la population utilisant Internet entre 1990 et 2016



Source : Rosner Max, Ritchie Hannah, Ortiz-Ospina Esteban, « internet », Our World in Data, 2020, https://ourworldindata.org/internet#citation

Annexe 5 : Exemple de deux sites de vente sur le Darkweb et des marchandises disponibles



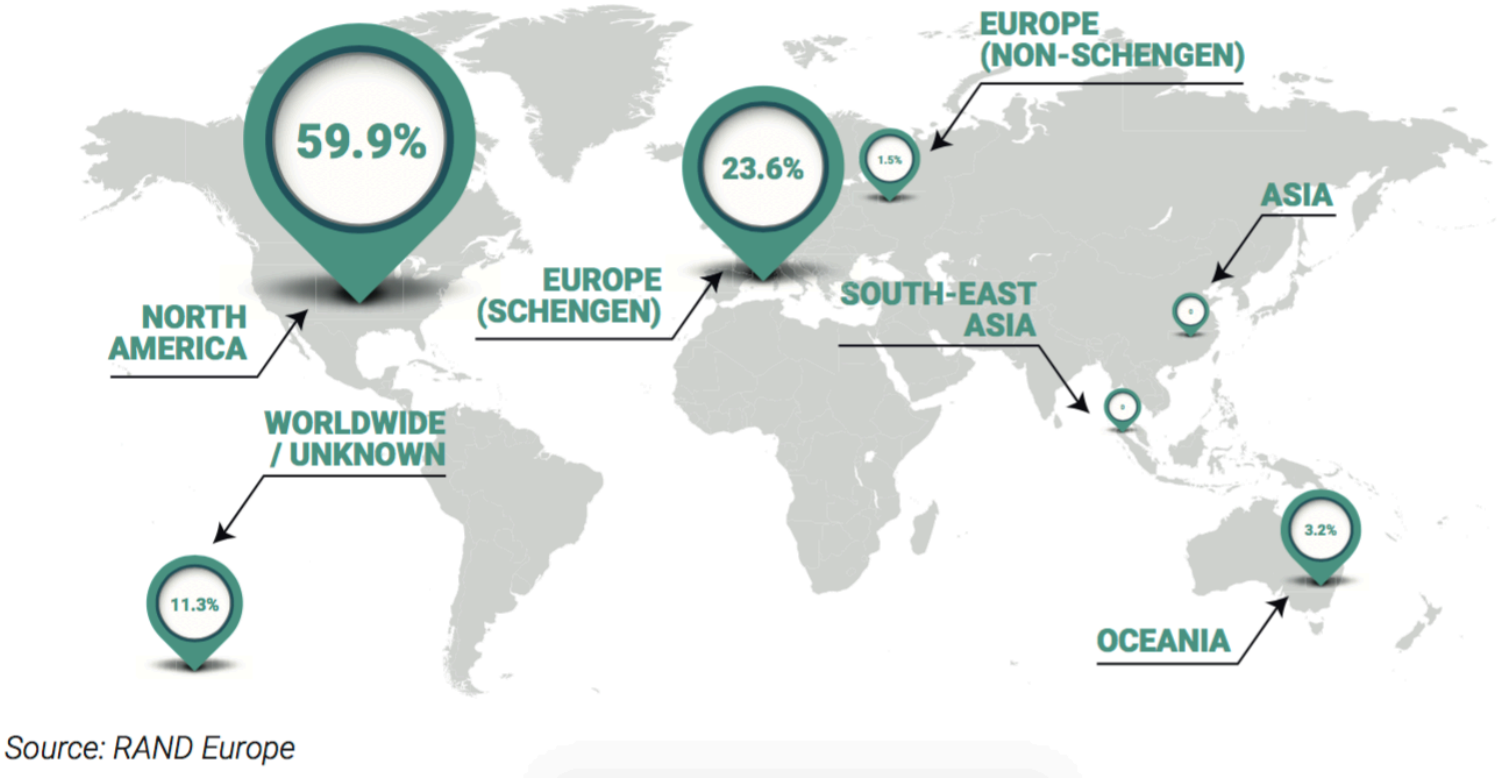


Source : Enquête de terrain sur le Darkweb, 17 juin 2020

Annexe 6 : Photo de la saisie par la gendarmerie section recherche d'Angers après le démantèlement d'un trafic entre la France et les États-Unis

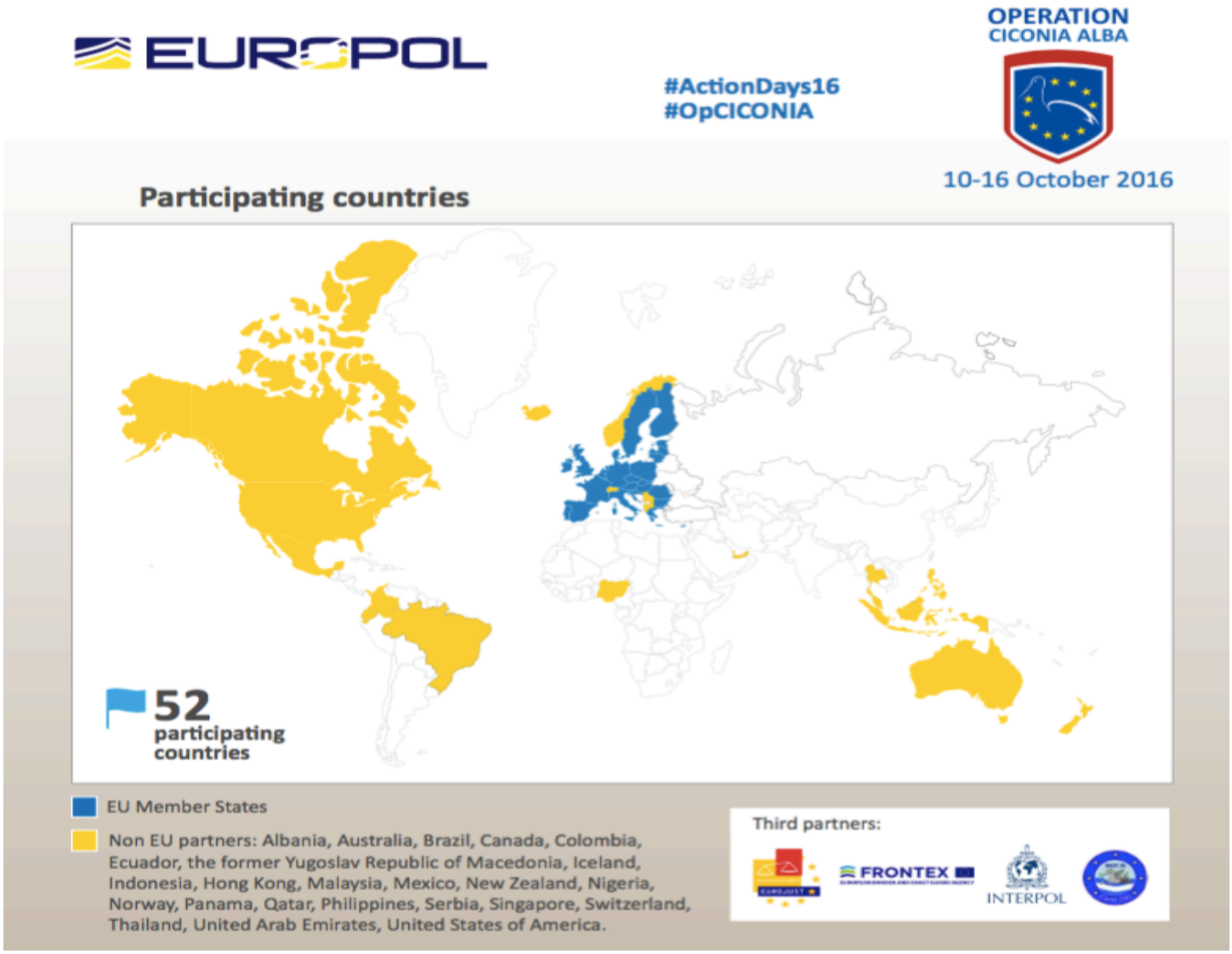
Source : Chevillard Thibault, « Angers : un trafic international d'armes à feu provenant des États-Unis démantelé », 20 minutes, mars 2019, https://www.20minutes.fr/faits_divers/2466627-20190306-angers-trafic-international-armes-feu-provenant-etats-unis-demantele

Annexe 7 : Répartition de vendeurs d'armes sur le Darkweb dans le monde par région



Source : Persi Paoli Giacomo, Adridge Judith, Ryan Nathan, Warnes Richard*, Behind the Curtain : the illicit trade of firearms, explosives and ammunition on the dark web,* RAND Europe, Cambridge, 2017, pp 58

Annexe 8 : Carte des participants à l'Opération Ciconia Alba lancée par Europol



Source : « EU Policy Cycle – EMPACT », Europol, https://www.europol.europa.eu/empact

BIBLIOGRAPHIE

CYBERESPACE : CRYPTOMONNAIES ET CRYPTOMARKETS

Ouvrages :

- Jenzen-Jones. N, McCollum. I, « Web Trafficking : Analysing the Online Trade of Small Arms and Light Weapons in Libya », Small Arms Survey, avril 2017

- Persi Paoli, G. « The Trade in Small Arms and Light Weapons on the Dark Web », UNODA Occasional Papers, Octobre 2018, n°32

- Rodriguez. Philippe, *La Révolution Blockchain : algorithmes ou institutions, à qui donnerez-vous votre confiance »,* Dunod, Mars 2017, pp 224

- Takkal Bataille Adli, Favier Jacques, *Bitcoin : la monnaie acéphale,* CNRS Éditions, Mai 2017, pp 280

Ressources internet :

- Aldridge Judith, Decary-Hetu David « Not an 'ebay for drugs' : the Cryptomarket 'Silk Road' as a paradigm Shifting Criminal Innovation », mai 2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436643

- Benotmane Linda, « Sur Instagram, on trouve aussi des Kalachnikov », Ouest-France, février 2017, https://www.ouest-france.fr/leditiondusoir/data/950/reader/reader.html#!preferred/1/package/950/pub/951/page/4

- Debelloir Marine, « Chainanalysis : les transactions illégales sur le dark Net à nouveau en hausse », Cryptoast, janvier 2020, https://cryptoast.fr/chainalysis-les-transactions-illegales-sur-le-dark-net-a-nouveau-en-hausse/

- Devecchio Alexandre, « Avec Laurent Gayard, plongée dans les profondeurs du Darknet », Le Figaro, janvier 2018, https://www.lefigaro.fr/vox/societe/2018/01/26/31003-20180126ARTFIG00288-avec-laurent-gayard-plongee-dans-les-profondeurs-du-darknet.php

- Manach Jean-Marc, « Le Darknet est trop compliqué pour les terroristes », Le Monde, avril 2016, https://www.lemonde.fr/blog/bugbrother/2016/04/01/le-darknet-est-trop-

complique-pour-les-terroristes/

- Paolini Esther, Lepoivre Ambre, « Snapchat, Whatsapp : les nouveaux codes du deal 2.0 », BFMTV, août 2019, https://www.bfmtv.com/police-justice/snapchat-whats-app-les-nouveaux-codes-du-deal-2-0_AV-201908020036.html

- Roser Max, Ritchie Hannah, Ortiz-Ospina Esteban, « internet », Our World in Data, 2020, https://ourworldindata.org/internet#citation
- « Digital 2020 : global digital overview », We Are Social et Hootsuite, janvier 2020, https://datareportal.com/reports/digital-2019-global-digital-overview

- « Les armes illégales viennent du cadre légal », RTL, émission du 24 avril 2019, https://www.youtube.com/watch?v=4niZrpcHrEs

- « Plus de 4 milliards de personnes n'ont pas accès à Internet », le Figaro, janvier 2016, https://www.lefigaro.fr/secteur/high-tech/2016/01/14/32001-20160114ARTFIG00078-plus-de-4-milliards-de-personnes-n-ont-pas-acces-a-internet.php

- « Tor et le routage en oignon », Openclassrooms, février 2020, https://openclassrooms.com/fr/courses/2939276-surfez-incognito-sur-internet-avec-le-reseau-tor/2955001-tor-et-le-routage-en-oignon#r-3281233

- « Trafic d'armes : internet, « boîte noire » difficile à pénétrer pour les autorités », l'Obs, novembre 2015, https://www.nouvelobs.com/societe/20151111.AFP6194/trafic-d-armes-internet-boite-noire-difficile-a-penetrer-pour-les-autorites.html

- « Vouloir fermer le Darknet est illusoire », Le Parisien, novembre 2016, https://www.leparisien.fr/societe/vouloir-fermer-le-darknet-est-illusoire-01-11-2016-6274134.php

GÉOPOLITIQUE DU TRAFIC D'ARMES

Ressources internet :

- Antoine Jean-Charles, « Frontières et trafic d'armes », Diploweb, mars 2015, https://www.diploweb.com/Frontieres-et-trafic-d-armes.html

- Antoine Jean-Charles, « Trafic d'armes et méthode géopolitique », Le Monde, mai 2012, https://www.lemonde.fr/idees/article/2012/05/23/trafic-d-armes-et-methode-geopolitique_1705562_3232.html

- Bonzon Ariane, Fontenille Marion, « Les turcs s'arment massivement », Slate, juin 2018, http://www.slate.fr/story/163328/turquie-folie-armes-apres-tentaive-coup-etat-

juillet-2016-partisans-akp-erdogan

- Bronskill Jim, « illicit gun sales made to canadians through dark web, Mounties warn », CBC, mars 2018, https://www.cbc.ca/news/politics/illicit-gun-sales-dark-web-1.4592937

- Chivers Christopher John, « How Many Guns Did the US Lose Track of in Iraq and Afghanistan ? Hundreds of Thousands. », The New York Times Magazine, août 2016, https://www.nytimes.com/2016/08/23/magazine/how-many-guns-did-the-us-lose-track-of-in-iraq-and-afghanistan-hundreds-of-thousands.html

- Duquet Nils, Goris Kevin, « Firearms acquisition by terrorists in Europe : research findings and policy recommendations of Project SAFTE », Flemish Peace Institute, avril 2018, https://www.flemishpeaceinstitute.eu/safte/files/vrede_syntheserapport_safte_lr.pdf

- Gardette Hervé, « Comment les armes se retrouvent-elles dans les mains des terroristes », émission Du Grain à Moudre du 25 mars 2016, France Culture, https://www.franceculture.fr/emissions/du-grain-moudre/comment-les-armes-se-retrouvent-elles-dans-les-mains-des-terroristes

- Keller Jared, « The Weapons America is Leaving Behind in Syria », The Soapbox, octobre 2019, https://newrepublic.com/article/155471/weapons-america-leaving-behind-syria

- Miguet Eric, « Marseille : trois personnes, dont une jeune femme de manière collatérale, blessés par balles dans la nuit », La Provence, juillet 2020, https://www.laprovence.com/actu/en-direct/6051921/.html

- Overton Iain, Jarvis-Norse Adam, Dathan Jennifer, Lombardi Mia, « US Department of Defence spend on guns in « War on Terror » revealed », Action on Armed Violence (AOAV), août 2016, https://aoav.org.uk/2016/us-department-of-defence-spend-on-guns-and-ammunition-in-the-war-on-terror-revealed/

- Persi Paoli Giacomo, Aldridge Judith , Ryan Nathan, Warnes Richard, « Behind the Curtain, the illicit trade of firearms, explosives and ammunition on the dark web », RAND Europe, 2017

- Shepp Jonah, « The American Gun Glut Is a Problem for the Entire Worid », New York Mag, février 2018, https://nymag.com/intelligencer/2018/02/the-american-gun-glut-is-a-problem-for-the-entire-world.html

- Truc Olivier, « Des navires occidentaux impliqués dans le trafic d'armes », Le Monde, février 2012, https://www.lemonde.fr/europe/article/2012/02/25/des-navires-

occidentaux-impliques-dans-le-trafic-d-armes_1648125_3214.html

- « Attentats de Paris : des armes utilisées ont été achetées en Allemagne », Le Point, novembre 2015, https://www.lepoint.fr/monde/attentats-de-paris-des-armes-utilisees-ont-ete-achetees-en-allemagne-27-11-2015-1985382_24.php

- « Le trafic d'armes en Seine-Saint-Denis : aspects géopolitiques et enjeux », Hérodote, n°162, mars 2016, https://www.cairn.info/revue-herodote-2016-3-page-73.htm, pp. 73-84

- « Marseille. Après une fusillade sur l'autoroute A7 et une sortie de route, un homme de 19 ans est mort », Ouest France, août 2020, https://www.ouest-france.fr/provence-alpes-cote-dazur/marseille-13000/marseille-apres-une-fusillade-sur-l-autoroute-a7-et-une-sortie-de-route-un-homme-de-19-ans-est-mort-6926707

- « Vendre et acheter des armes en Europe : où en est-on ? », France Inter, émission du 24 mars 2016, https://www.franceinter.fr/emissions/l-eco-du-matin/l-eco-du-matin-24-mars-2016

Rapports :

- Martyniuk Anton *Measuring Illicit Arms Flows*, Small Arms Survey, Genève, Avril 2017, pp. 8
- Rice Graeme, Jenzen-Jones Nic, *The Online Trade of Light Weapons in Libya, Security Assessment in north Africa*, Small Arms Survey, Genève, avril 2016, pp. 10

SOCIOLOGIE ET POLITIQUE DU TRAFIC D'ARMES SUR LE DARKWEB

Ouvrages :

- Bonelli Laurent, *La France a peur, une histoire sociale de l'insécurité*, La Découverte Poche, pp. 434
- Derville Grégory, *Le pouvoir des médias : mythes et réalités*, *2ème édition revue et augmentée*, PUG, 2005, pp. 205
- Overton Iain *Gun Baby Gun : voyage de tous les dangers au pays des armes à feu,* Belfond, janvier 2017, pp 502

Rapports :

Proposition de directive du Parlement Européen et du Conseil relative au contrôle de l'acquisition et de la détention d'armes (codification), 26 février 2020, Sénat, http://www.senat.fr/europe/textes_europeens/e14635.pdf

Valard Hubert, « Les armes et les munitions utilisées par les terroristes », *Bulletin de l'Académie Nationale de Médecine,* n°4-5, 705-712, mai 2016, https://www.europe1.fr/societe/important-vol-darmes-a-feu-sur-la-base-militaire-distres-2855050

Ressources Internet :

- Bucolo Elisabetta, « Racket, vols, corruption : comment les réseaux criminels profitent de la crise sanitaire », The Conversation, mai 2020, https://theconversation.com/racket-vols-corruption-comment-les-reseaux-criminels-profitent-de-la-crise-sanitaire-137841

- Dubuis Etienne, « Le trafic d'armes se développe sur Facebook », Le Temps, avril 2016, https://www.letemps.ch/monde/trafic-darmes-se-developpe-facebook

- Gruet Magali, « Le coronavirus provoque une ruée sur les armes en Californie », Le Parisien, mars 2020, https://www.leparisien.fr/international/le-coronavirus-provoque-une-ruee-sur-les-armes-en-californie-25-03-2020-8287503.php

- Lenoir Luc, « Armes illégales : un arsenal invisible au service de la délinquance », le Figaro, juin 2020, https://www.lefigaro.fr/armes-illegales-un-arsenal-invisible-au-service-de-la-delinquance-20200630

- Paolini Esther, « Ces Français qui revendiquent leur droit à disposer d'une arme à feu », le Figaro, novembre 2016, https://www.lefigaro.fr/actualite-france/2016/11/15/01016-20161115ARTFIG00108-ces-francais-qui-revendiquent-leur-droit-a-disposer-d-une-arme-a-feu.php

- Pinte Jean-Paul, « Les jeunes et le Dark Web », *Terminal*, décembre 2018, consulté le 24 juillet 2020, http://journals.openedition.org/terminal/3278 ; DOI : https://doi.org/10.4000/terminal.3278

- Rolland Sylvain, « Cybercriminalité : qui sont les escrocs du darknet français ? », La Tribune, septembre 2016, https://www.latribune.fr/technos-medias/cybercriminalite-qui-sont-les-escrocs-du-darknet-francais-599111.html

- « Après les attentats, les Français cherchent de plus en plus à s'armer », Europe 1, novembre 2016, https://www.europe1.fr/societe/apres-les-attentats-les-francais-cherchent-de-plus-en-plus-a-sarmer-2890766

- « Comment acheter une arme sur Facebook en 15 minutes », RTBF, février 2014, https://www.rtbf.be/info/medias/dossier/vu-sur-le-web/detail_comment-acheter-une-arme-sur-facebook-en-15-minutes?id=8211399

- « Enquête sur ces Français qui veulent s'armer », L'Obs, octobre 2016, https://www.nouvelobs.com/societe/20161031.OBS0569/enquete-sur-ces-francais-qui-veulent-s-armer.html

- « Important vol d'armes à feu sur la base militaire d'Istres », Europe 1, septembre 2016, https://www.europe1.fr/societe/important-vol-darmes-a-feu-sur-la-base-militaire-distres-2855050

- « La justice américaine met un coup d'arrêt temporaire à l'impression des armes en 3D », Le Monde, août 2018, https://www.lemonde.fr/ameriques/article/2018/08/01/la-justice-americaine-suspend-l-autorisation-d-imprimer-des-armes-en-3d_5338038_3222.html

- « Une vaste saisie d'armes illustre la frontière poreuse entre collectionneurs et crime organisé », Le Point, juin 2018, https://www.lepoint.fr/societe/une-vaste-saisie-d-armes-illustre-la-frontiere-poreuse-entre-collectionneurs-et-crime-organise-16-06-2018-2227747_23.php#

RECONVERSION / FABRICATION D'ARMES À FEU

Rapports :

- Florquin Nicolas, King Benjamin, *Quand le légal devient létal : les armes à feu converties en Europe,* Small Arms Survey, Genève, avril 2018, pp. 78

Ressources internet :

- Dearden Lizzie, « Use of 3D printed guns in German synagogue shooting must act as warning to security services, expert say », The Independant, octobre 2019, https://www.independent.co.uk/news/world/europe/3d-gun-print-germany-synagogue-shooting-stephan-balliet-neo-nazi-a9152746.html

- La J « Des pistolets d'alarme transformés en armes : la tendance inquiétante chez les petits délinquants », La Libre, août 2017, https://www.lalibre.be/belgique/des-pistolets-d-alarme-transformes-en-armes-la-tendance-inquietante-chez-les-petits-delinquants-599ab263cd706e263f83422f

- MacAskill Ewen, Hopkins Nick, « Bomb-making guides are online, but getting them to work is not easy », The Guardian, mai 2017, https://www.theguardian.com/uk-news/2017/may/23/bomb-making-guides-are-online-but-getting-them-to-work-is-not-easy

- Spencer Richard, « Al-Qaeda newspaper : Make a bomb in the kitchen of your mom », The Telegraph, juillet 2010,

https://www.telegraph.co.uk/news/worldnews/7865978/Al-Qaeda-newspaper-Make-a-bomb-in-the-kitchen-of-your-mom.html

- Yeazel Bryan, « Bomb Making Manuals on the Internet : Maneuvring a solution through First Amendment Jurisdprudene », Notre Dame Journal of Law, Ethics & Public Policy, février 2014, http://scholarship.law.nd.edu/ndjlepp/vol16/iss1/12

- « Armes légères », Nations Unies, https://www.un.org/disarmament/fr/convarms/armes-legeres/

- « Les munitions », Police Scientifique, https://www.police-scientifique.com/Armes-a-feu/les-munitions/
- « VIDÉO : Des armes en kit ou fabriquées avec des imprimantes 3D : un phénomène inquiétant aux États-Unis », LCI, février 2020, https://www.lci.fr/international/video-des-armes-en-kit-ou-fabriquees-avec-des-imprimantes-3d-un-phenomene-inquietant-aux-etats-unis-2144715.html

TRAVAIL DES AUTORITÉS ET DES INSTITUTIONS :

Rapports :

- Duquet Nils, *The 2018 EU SALW Strategy : Towards an Integrated and Comprehensive Approach*, Non Proliferation and Disarmement Consortium n°62, Paris, avril 2019, pp. 20 https://www.nonproliferation.eu/2018-eu-salw-strategy/

- *Directive (EU) 2017/853 of the European Parliament and of the Council of 17 May 2017 amending Council Directive 91477/EEC on control of the acquisition and possession of weapons*, Journal Officiel de l'Union Européenne, Bruxelles, mai 2017, pp. 18, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32017L0853&from=EN

- *Directivce d'exécution (UE) 2019/69 de la Commission du 16 janvier 2019 établissant des spécifications techniques relatives au marquage des armes d'alarme et de signalisation au titre de la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes,* Journal Officiel de l'Union Européenne, Eur-Lex, Bruxelles, janvier 2019, pp. 4, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019L0068

- *Drugs and the Darknet : perspectives for enforcement, research and policy*, Europol, European Monitoring Centre for Drugs and Drug Addiction, La Haye, 2017, pp.90
- *Fighting Illicit Firearms Trafficking Routes and Actors at European Level, Final Report of Project FIRE*, Transcrime, Milan, 2017, pp. 116, http://www.transcrime.it/wp-content/uploads/2017/03/FIREFinalReport.pdf

- *Extrait de la feuille de route présentée et adoptée par les chefs d'États de gouvernement lors du Sommet de Londres sur les Balkans Occidentaux du 9 au 10 juillet 2018*, pp.14 https://www.france-allemagne.fr/IMG/pdf/roadmap-final_version_july_2018.pdf

- *Journée contre la corruption : le Secrétaire Général appelle à s'unir pour mettre fin au détournement des ressources par les flux d'argent illicites, SG/SM/19901-OBV/1945,* Nations Unies, New York, décembre 2019, https://www.un.org/press/fr/2019/sgsm19101.doc.htm

- *Plan National de Lutte contre les Armes Illégalement Détenues*, Ministère de l'Intérieur, Paris, 2015, pp. 9, https://www.interieur.gouv.fr/content/download/90032/699995/file/dossier-presse-plan-armes.pdf

- *Prévention et lutte contre les trafics d'armes classiques : nouveaux défis et perspectives,* Compte-rendu et synthèse du séminaire organisé par l'IRIS et le GRIP pour le compte de la Direction générale des relations internationales et de la stratégie (DGRIS) du ministère des Armées, Paris, mai 2019, pp. 31, https://www.defense.gouv.fr/content/download/577395/9873550/file/201905-lutte_traffics_armes_EPS2018-18_CR_seminaire.pdf

- *Protocole à suivre en cas de découverte d'armes à feu : rassembler, partager et analyser toutes les informations sur la criminalité liée aux armes à feu afin de lutter contre le terrorisme, les auteurs de crimes violents et les trafiquants d'armes,* Interpol, Lyon, 2019

- *Protocole contre la fabrication et le trafic illicite d'armes à feu, de leurs pièces, éléments et munitions, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée,* Nations Unies, New York, 2001
- *Report of the United Nations Conference on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects,* United Nations, New York, juillet 2001, pp.29, https://www.un.org/events/smallarms2006/pdf/N0150720.pdf

- *Résultats 2018,* Douanes & Droits Indirects, Ministère de l'Action et des Comptes Publics, Montreuil, 2019, pp. 32, https://www.douane.gouv.fr/sites/default/files/uploads/files/2019-04/douane-resultats-2018.pdf

- *S/2017/1025 : Small Arms and Light Weapons : report of the Secretary-General,* United Nations Security Council, New York, décembre 2017, pp.25, https://undocs.org/S/2017/1025

- *Spread of 1 Billion Small Arms, Light Weapons Remains Major Threat Worldwide, High Representative for Disarmement Affairs Tells Security Council,* United Nations, février 2020, https://www.un.org/press/en/2020/sc14098.doc.htm

- *Traité sur le commerce des armes,* Nations Unies, New York, 24 décembre 2014, pp. 107

- *Traité sur le fonctionnement de l'Union Européenne,* Journal Officiel de l'Union Européenne, Bruxelles, pp. 153

- *UNODC Study sheds light on hidden crime of firearms trafficking*, UNODC, Vienne, juillet 2020, https://www.unodc.org/unodc/press/releases/2020/July/unodc-study-sheds-light-on-hidden-crime-of-firearms-trafficking.html

- *The Untraceable Firearms Act of 2020,* Richard Blumenthal United States Senator for Connecticut, 2020, http://www.blumenthal.senate.gov/imo/media/doc/Untraceable%20Firearms%20Act%20of%202020%20-%20OnePager%20-%20200513.pdf

Ressources internet :

- Biet Guillaume, « Un important trafic d'armes démantelé entre les États-Unis et la France », Europe 1, mars 2019, https://www.europe1.fr/societe/un-important-trafic-darmes-demantele-entre-les-etats-unis-et-la-france-3869177

- Brault Brigitte, « Démantèlement d'un trafic d'armes sur le réseau Whatsapp par la police de Fort-de-France et Antilles-Guyane », France TV Info, mai 2020, https://la1ere.francetvinfo.fr/martinique/demantelement-trafic-armes-reseau-whatsapp-police-fort-france-antilles-guyane-834158.html

- Chevillard Thibaut , « Angers : un trafic international d'armes à feu provenant des États-Unis démantelé », 20 minutes, mars 2019, https://www.20minutes.fr/faits_divers/2466627-20190306-angers-trafic-international-armes-feu-provenant-etats-unis-demantele

- Ducos Jean-Marc, « Un trafic d'armes « hors norme » démantelé en France : 1900 armes saisies », le Parisien, juin 2018, https://www.leparisien.fr/faits-divers/un-trafic-d-armes-hors-norme-demantele-en-france-1900-armes-saisies-15-06-2018-7775082.php

- Greenberg Andy, « Global Police Spring a Trap on Thousands of Dark Web Users », Wired, juillet 2017, https://www.wired.com/story/alphabay-hansa-takedown-dark-

web-trap/

- Greenberg Andy, « Operation Bayonet : Inside the Sting That Hijacked an Entire Dark Web Drug Market », Wired, août 2018, https://www.wired.com/story/hansa-dutch-police-sting-operation/

- Howell O'Neill Patrick, « A dark web tycoon pleads guilty. But how was he caught ? », MIT Technology Review, février 2020, https://www.technologyreview.com/2020/02/08/349016/a-dark-web-tycoon-pleads-guilty-but-how-was-he-caught/

- Planques Martin, « Comment le forum du « dark web » vient d'être démantelé en France », RTL, juin 2018, https://www.rtl.fr/actu/futur/comment-le-forum-du-dark-web-vient-d-etre-demantele-en-france-7793777376

- Povoledo Elisabetta, « Italian Police Arrests Over 300 in Raids on Organized Crime », The New York Times, décembre 2019, https://www.nytimes.com/2019/12/19/world/europe/ndrangheta-arrests-police-mafia.html

- Taylor Laura, « Police Dismantle One of The Largest Gun Trafficking Networks in Spain With Origins in Costa del Sol's Malaga », Euro Weekly News, juin 2020, https://www.euroweeklynews.com/2020/06/24/police-dismantle-one-of-the-largest-gun-trafficking-networks-in-spain-with-origins-in-costa-del-sols-malaga/

- « Comment l'intérieur entend lutter contre le trafic d'armes », l'Obs, novembre 2015, https://www.nouvelobs.com/societe/20151113.OBS9363/comment-l-interieur-entend-lutter-contre-le-trafic-d-armes.html

- « Contrôle du trafic d'armes de guerre en France », Sénat, mars 2016, https://www.senat.fr/questions/base/2016/qSEQ160320877.html

- « Cyber-patrolling week », Europol, https://www.europol.europa.eu/activities-services/europol-in-action/operations/cyber-patrolling-week

- «Dark Web : trois suspects mis en examen après le démantlèlement d'une plateforme illégale », Ouest France, juin 2019, https://www.ouest-france.fr/societe/justice/dark-web-trois-suspects-mis-en-examen-apres-le-demantelement-d-une-plateforme-illegale-6400560

- « EU Policy Cycle – EMPACT », Europol, https://www.europol.europa.eu/empact

- « German police shuts down one of world's biggest dark web site », The Guardian, mai 2019, https://www.theguardian.com/world/2019/may/03/german-police-close-

down-dark-web-marketplace

- « IBIN : le Réseau d'Information balistique d'INTERPOL », Interpol, janvier 2017, https://www.interpol.int/Crimes/Firearms-trafficking/Illicit-Arms-Records-and-tracing-Management-System-iARMS

- « Illicit Arms Records and tracing Management System (iARMS) », Interpol, https://www.interpol.int/Crimes/Firearms-trafficking/Illicit-Arms-Records-and-tracing-Management-System-iARMS

- « L'essentiel de la douane », Portail de la Direction Générale des douanes et droits indirects, Portail de l'Économie, des Finances, de l'Action et des Comptes Publics, https://www.douane.gouv.fr/la-douane/qui-sommes-nous/lessentiel-de-la-douane

- « Lutte contre les trafics illicites d'armes à feu dans les Balkans occidentaux – Déclaration à la presse de M.Jean-Yves Le Drian (Paris, 11.12.2018) », France Diplomatie, décembre 2018, https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/desarmement-et-non-proliferation/elimination-et-maitrise-des-armements-classiques/article/lutte-contre-les-trafics-illicites-d-armes-a-feu-dans-les-balkans-occidentaux

- « Massive Blow to Criminal Dark Web Activities after Globally Coordinated Operation », Europol, juillet 2017, https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

- « Massive arms trafficking ring dismantled by Italian and Austrian action, coordinated by Eurojust », Eurojust, mars 2019, http://www.eurojust.europa.eu/press/PressReleases/Pages/2019/2019-03-26.aspx

- « Worldwide operation Dragon sees 52 countries teaming up to thwart organised crime », Europol, juin 2017, https://www.europol.europa.eu/newsroom/news/worldwide-operation-dragon-sees-52-countries-teaming-to-thwart-organised-crime

CORRUPTION :

Ouvrages :

- Ferreira Carlos, Engelschalk Michael, Mayville William, *The Many Faces of Corruption : Tracking Vulnerabilities at the Sector Level,* « The Challenge of Combating Corruption in Customs Administrations », World Bank Group Publications*,* Washintgton, 2011, pp. 484

Rapports :

- Chêne Marine, *Corruption at borders*, CHR Michelsen Institute, Bergen, 2018, pp 29, https://www.u4.no/publications/corruption-at-borders.pdf

Ressources internet :

- « Vol d'armes sur une base militaire d'Istres. Quatre suspects écroués », Ouest France, septembre 2016, https://www.ouest-france.fr/societe/justice/vol-darmes-sur-une-base-militaire-distres-quatre-suspects-ecroues-4519296

ÉCONOMIE SOUTERRAINE ET LE DARKWEB :

Ressources internet :

- Popper Nathaniel, « Bitcoin Has Lost Steam. But Criminals Still Love It. », The New York Times, janvier 2020, https://www.nytimes.com/2020/01/28/technology/bitcoin-black-market.html

- Sulleyman Aatif, « Bitcoin price is so high because criminals are using it for illegal trades, research suggests », The Independant, janvier 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-fall-criminals-blockchain-anonymous-cryptocurrency-zcash-monero-dash-a8174716.html

- « Trafic de drogue intégré au PIB : ce que ça va changer pour la France », Capital, février 2018, https://www.capital.fr/economie-politique/trafic-de-drogue-integre-au-pib-ce-que-ca-va-changer-pour-la-france-1269283

RÉSUMÉ

Le trafic d'armes a longtemps été au centre des préoccupations des institutions internationales et nationales. Avec la vague d'attentats en Europe, l'impact du Darkweb dans la prolifération d'armes à feu dans le monde pourrait devenir inquiétante à mesure que l'accès à internet dans le monde se développe. Que ce soient les anciennes lacunes de la législation concernant les armes non létales, leur commercialisation sur les différents réseaux ou encore l'assiduité des contrôles aux frontières, il semblerait que les autorités internationales et régionales aient tout de même œuvré avec efficacité sur le plan législatif et opérationnel, en prévision d'un potentiel retard face aux cybercriminels. Aujourd'hui, la question de la dangerosité du trafic d'armes sur le Darkweb partage. Elle pourrait être considérée comme contrôlée, suite aux réussites des cyber experts à travers les programmes de coopération internationaux ou encore suite aux décisions internationales appliquées aux législations nationales. Néanmoins, il est toujours possible de voir le trafic d'armes sur le Darkweb comme une concrétisation de clivages socio-politiques bien plus ancrés, qui pourraient semer la confusion lorsqu'on tente d'analyser les causes ou les effets d'une fragilisation de la sécurité internationale.

Table des matières