Internet Traces to Better Understand Online Illicit Markets

Quentin Rossy, École des sciences criminelles, Université de Lausanne & David Décary-Hétu, École de criminologie, Université de Montréal

Abstract

This chapter discusses how forensic science and criminology can combine to apprehend online illicit markets. In line with Felson’s ecological theory and the work of Soudijn and Zegers, we first postulate that online illicit markets rely on ‘virtual convergence settings’ where offenders interact and leave traces. We therefore offer a classification of these settings in regard to three stages enabled by the Internet: promotion, selling and review processes. Dedicated websites and online communities are defined as two distinct types of virtual convergence settings that require specific investigation and monitoring processes to acquire relevant traces. We then define Internet traces as a subtype of digital traces and show how they may be used to reconstruct the illicit activities of online offenders. First we discuss the importance of trust in illicit markets and how it may lead to a new form of traceability of offenders based on the way they manage their only identities. We then address the question of the reconstruction of networks of offenders and networks of markets based on the detection of forensic links inferred from Internet traces. The specific case of human trafficking as an illicit market where the ‘products’ sold are not goods, but human beings’ services is then taken as an example. We conclude with a discussion about the integration of Internet and physical traces to reconstruct global illicit trafficking processes that encompass the online part of illicit markets.

From Behaviour Crime Systems to Virtual Convergence Settings

Aristotle is believed to be the first to have said that “man is by nature a social animal” (Vinciarelli et al. 2012). The social nature of all things related to humanity has unsurprisingly also been identified and studied in much of the past research on crime. Sutherland (1947), for example, through his differential association theory, argued that crime is a behaviour that is learned through contact with others. Repeated and intimate contact with offending others may turn certain individuals into offenders through exposure to unfavourable definitions of laws and social norms. Other researchers have since followed in Sutherland's footsteps (Bandura 1971; Akers et al. 1979) and offered a revised social learning theory that focuses on learning behaviours from others through contact with them but also through observation and reinforcements and punishments.

A perhaps even more important contribution of Sutherland to criminology comes from his behaviour crime systems theory, which focuses on the macro interactions of offenders (Tremblay 2010). Sutherland (1947) argues that offenders should be categorized, for research purposes, in very small but homogeneous sociological units called behaviour crime systems. These systems are built around a very specific type of offence such as confidence fraud or theft. The legal definitions of offences are of no use to Sutherland as they are broad and encompass many types of offenders. Indeed, kidnappers can target their victims for political gains, money or even revenge in the case of intra-family kidnappings. These different motivations can be found in kidnappers of different types who have very little in common. Sutherland (1947) surmises that to understand crime, it is necessary to drill down to the core of each type of offence and study the offenders who are involved in it as a unit. These offenders likely share with each other a group way of life, motivations, tools and techniques. They also likely share a sense of belonging with their peers as well as many rationalizations. Of the utmost importance to participants in behaviour crime systems are their "convergence settings" (Felson 2003) where they can meet and debate the best offending practices for maximizing benefits and minimizing risks. Traditionally, these convergence settings were often local bars and resorts attended by offenders and their social relations.

Behaviour crime system theory, although understudied (Tremblay 2010), makes a significant contribution to the field of criminology and crime sciences in general by highlighting the presence and the need for convergence settings. In our modern connected world, these convergence settings have moved on past local bars and resorts and are now hosted on the Internet (Soudijn and Zegers 2012). These now virtual settings were at first meeting spaces like newsgroups and bulletin board systems (BBS) where offenders could meet and share information and electronic tools (Meyer 1989). Their functionalities were very limited, allowing only for the sending of public and private messages and the sharing of computer files. As computer-mediated communications evolved, so did the convergence settings, which moved from newsgroups and BBS to the open World Wide Web. Convergence settings have evolved toward synchronous communication channels hosted in online chat rooms that have the benefit of not storing any messages for later review. All participants have to be online at the time of broadcast to capture messages (Décary-Hétu et al. 2014). They've also evolved toward asynchronous communication channels hosted on online forums where participants can build personal profiles and interact with others both publicly and privately (Holt 2007). Both synchronous and asynchronous communications also integrate the ability to share files.

The size and scope of virtual convergence settings are believed to vary greatly from a single-digit number of participants for private and exclusive settings to hundreds of thousands of participants for the largest, public settings. Participants will take on many roles and normally follow the Internet 1 percent rule (van Mierlo 2014). This rule states that about 90 percent of participants will only view content while about 9 percent will very occasionally edit or create content and about 1 percent will be responsible for the bulk of content creation.

Online Illicit Markets as Virtual Convergence Settings

In addition to helping offenders share their best practices, tools and techniques, virtual convergence settings have over the past decades slid toward becoming online commodity markets (Holt and Lampke 2010; Motoyama et al. 2011; Décary-Hétu and Leppänen 2016). These online illicit markets allow offenders to buy and sell illicit goods and services rather than sharing them for free. Buyers and sellers can put up listings for what they are looking to buy, rent or sell along with a description and a price. These listings can be browsed and out-of-band channels can be used to negotiate a price. Online illicit markets were at first specialized in virtual goods and services, mostly financial fraud, intellectual property fraud and computer fraud (Kruithof et al. 2016). These had the benefit of being virtual, meaning that offenders did not have to commit at any point in time to a connection with the physical world. More recently, online illicit markets have grown to encompass the sale of physical goods, which are shipped through the mail (Christin 2013). Offenders have become quite skilled at hiding their products in innocuous packages that can evade inspections by law enforcement and mail services (Rhumorbarbe et al. 2016; Aldridge and Askew 2017).

Online illicit markets can be classified in two groups: dedicated websites and online communities. The former includes online shops created and hosted by sellers. Most of the dedicated websites, which are mainly oriented to the sale of counterfeit goods and pharmacy, are organized in ‘affiliate programs’, where affiliate websites advertise and redirect the client to a main shopping website that provides products (Levchenko et al. 2011; Kanich et al. 2011). Online communities are shared settings where sellers may integrate their shops or their listings within a predefined marketplace that may be known to support legal trade (e.g., ebay) or to be focused on the trade of illicit goods and services (e.g., cryptomarkets on Tor). The annual sales facilitated by cryptomarkets, a small subset of all online illicit markets, are believed to be in the range of hundreds of millions of US dollars per year (Soska and Christin 2015; Kruithof et al. 2016). Online communities that host the sale of illicit goods and services also include crowdfunding services, which have been used to promote the development of goods that will never be produced (Fredman 2015). Promoters may also present their product as innovative and new but in reality their product may simply be already available counterfeit goods that are produced and sold after the crowdfunding campaign. Peer-to-peer applications are another setting used by sellers of illicit goods and services. OpenBazaar[1] for instance is a peer-to-peer bitcoin marketplace where illicit trade seems to have emerged.[2] Illicit markets are also moving to mobile applications such as ‘Wish’ where counterfeit goods are plentiful, and to anonymous messaging applications like ‘Whisper’. As far as we know, no dedicated illicit shop application is available on mobile devices, apart from the misuse of applications dedicated to the selling of medical marijuana (e.g., Nestdrop).

To help buyers evaluate the trustworthiness of sellers, review sites have been launched so that buyers can share experiences and rate sellers. These sites take on the form of dedicated websites such as blogs or of online communities (e.g., boards and forums). Instant messages on a direct peer-to-peer app such as Skype or asynchronous messaging applications such as Whatsapp or emails may also be used. The sustained analysis of review convergence settings may feed qualitative research (Van Hout and Hearne 2017) and the reconstruction of social networks of actors involved in online illicit markets (Décary-Hétu and Laferrière 2015). Review sites can also feed intelligence-led screening strategies to detect new online illicit markets (Pineau et al. 2016).

In synergy with the trends affecting licit businesses, illicit markets have been transformed by their online setting, which impacts the promotion strategies, the sales process, the sharing of feedback and the communications between buyers and sellers (Holt et al. 2016). To reach potential customers, sellers tend to use one of two techniques. They may first try to impose themselves into their potential customers' online space. This can be achieved through the use of massive or targeted email campaigns (Levchenko et al. 2011) or by taking advantage of online advertisement (ads) services (Li et al. 2012). An alternative is to wait until potential customers actively search for illicit products and end up on the sellers' page. Global search engines (e.g., Google, Bing, Yandex, Baidu) are obviously excellent tools for sellers looking to get noticed and these search engines can be manipulated through search-redirection attacks. Also known as 'cloaking', this attack changes search results or the action that is taken once a link is clicked in a search engine (Leontiadis et al. 2011). Private and localized search engines integrated in online communities may also be used by sellers to get noticed. This has led to the emergence of a fraudulent accounts market where accounts are sold to promote scams, phishing and other illicit markets (Thomas et al. 2013). Other online communities, such as classified advertisements websites, are also important promotion convergence settings for illicit markets (see the example of trafficking in human beings [THB] described below).

In some cases, the same virtual convergence setting can host multiple sections that serve to promote, sell and review sellers (see Table 1). Facebook pages can be used as a promotion means to redirect customers to a dedicated sale website, as a direct online storefront that advertises products for sale, and as a review site through dedicated groups. Cryptomarkets may contain a forum to facilitate discussions and integrate a review system to rate sellers. Moreover, if emails are more often than not used to redirect the target to a website, they may also lead to a direct communication and a sale.

<Insert Table 1 here>

Internet Traces to Apprehend Online Illicit Markets

Online illicit markets have attracted a lot of attention from researchers since they provide a vast and fertile ground from which to collect data on offenders (see Décary-Hétu, 'Online Crime Monitoring' in this volume). This data is collected through online monitoring that acquires digital (i.e., computer) traces that are available on the Internet. As defined by Margot (see chapter Margot, 'Traceology, the fundamental bedrock of forensic science' in this volume), a trace is the fundamental and most direct remnant of a criminal activity. In this context, a criminal activity has to be understood in its broadest sense to include litigious and security issues that cause harms. Jaquet-Chiffelle (personal communication) further defines a trace as a subsequently observable modification (e.g. a adjunction, a transformation or a suppression) resulting from an (crime) event. Digital traces can be considered a subtype of traces that may be collected on all kinds of electronic systems, including computers but also devices like mobile phones (Casey 2011, 7).

The digital forensic field encompass all forms of digital traces related to criminal activities. It focuses much of its efforts on digital traces that can be directly collected by physically accessing a device. Digital traces can also, however, be accessed from virtual environments that are remote to the forensic scientist (i.e., the Internet and most frequently in the web). These digital traces are called Internet traces to express their specificity. Internet traces are the remnants of a criminal activity that leads to a modification, subsequently observable through the Internet. Internet traces pose a challenge to forensic scientists because they only allow the observation and copying of digital traces, never their collection. Indeed, only a private access to the file system allows the extraction (or copy) of the specimen physically present on the remote computer. Collecting traces requires a physical access to its source (a computer system) that can be thousands of kilometres away. Aside from hindering the possibility to collect the traces, Internet as an indirection between the forensic scientist and the digital trace creates transformations that may be assimilated to an observation effect. Indeed, forensic scientists may use different software to collect Internet traces and these various software may render Internet content in different ways or, even worse, may not render some of the content at all. In some cases, the website programmer herself may choose to change the content depending on the tool used to access it[3] or the visitor's location.[4] Combined, these challenges demonstrate the need to fully understand the implications of using Internet traces for research purposes.

The next section introduces the discussion of the roles of Internet traces in reconstructing the illicit activities of online sellers. It starts with the importance of trust in illicit markets and how this may lead to a new form of traceability of offenders based on the way they manage their unique identities. It then addresses the question of the reconstruction of networks of offenders and networks of markets based on the detection of forensic links (see Ribaux and Caneppele, 'Forensic Intelligence' in this volume) inferred from Internet traces. Finally, the current state of research on how the Internet has impacted trafficking in human beings is presented as a special case of illicit markets where the 'products' sold are not goods, but human beings' services.

Trust in Online Markets: Impact on the Traceability of Seller Identities

Online illicit markets pose a series of logistical and security challenges to their participants. The first challenge relates to trust and the detection of participants who act opportunistically when entering into contact with others (Wehinger 2011). Given the anonymity that the Internet affords, it can be difficult for participants to evaluate the trustworthiness of others and to identity undercover agents posing as drug dealers or fraudsters exploiting the market to steal money or data from other participants. To address this challenge, offenders have built online personas around a vanity name (Décary-Hétu and Eudes 2015). These personas have a history that is stored online publicly so that others can go through it and evaluate its experience and past realizations. Building a trustworthy online persona is, however, not enough since trusted vendors face the very real risk of identity theft. Indeed, other vendors may take advantage of the reputation of an alias and use it on other online illicit markets. More structured tools have also been created to manage reputation including automated feedback systems, which log feedback following transactions between participants. Participants can use these systems to shame others who have acted opportunistically and drive participants to sellers who have delivered on their word in the past. Participants also rely on higher authorities, namely market administrators who are tasked with the social regulation of the markets (Holt and Lampke 2010). These administrators vet new participants, test the products and services they have for sale and hold payments in escrow until a transaction is completed. While administrators may strive to limit opportunistic behaviour among their market participants, many markets appear to be “lemon markets” where so many sellers are acting opportunistically that it becomes difficult for reliable sellers to sell their goods and services at a decent price. These sellers are forced to sell at a lower price, matching that of disreputable sellers. This creates tension in online illicit markets, which are prone to conflicts.

Another challenge for market participants revolves around their need for anonymity. Participants need to communicate with each other in a secure fashion and have adopted encryption protocols like PGP to protect against eavesdropping (Soska and Christin 2015; Broséus et al. 2016b) and as an authentication means to avoid identity theft. Connections between the markets and their participants are also increasingly encrypted and the use of the Tor network facilitates the use of encryption to obfuscate both the participants’ location and the location of the servers hosting the illicit markets. The payment methods for goods and services sold in online illicit markets were for a long time either money transfers using private companies like Western Union, or virtual currencies like Liberty Reserve. More recently, the creation of cryptocurrencies, which are based on cryptography (e.g., the Bitcoin) rather than trust, has removed the need for third parties to manage the currency.

Reconstructing the Market Structure Using Internet Traces

Offenders leave many Internet traces online, either through their promotion and sales activity or through their efforts to remain anonymous. This has created new opportunities to observe traces of offenders that can be used to link virtual identities together, identify and gather intelligence on new and unknown offenders, find the physical location of offenders and estimate the size and scope of their activities. The acquisition of Internet traces in order to reconstruct the market structure and, in particular, networks of offenders, differs between dedicated websites and online communities. In online communities, offenders take advantage of settings created by third parties that might be criminal or not. They post information and leave traces in web pages’ content but do not handle the creation and management of the website, whereas the creation of a dedicated website requires instrumental pre-condition and preparation during which offenders may leave other kinds of traces (e.g., when registering a domain name or hosting the website). These traces are dependent on the infrastructure and the protocols used on the Internet. We thus refer to them as protocol traces.

To detect links between virtual identities in online communities, communications (public and private messages) and transactions data (feedback) have been used as the fundamental pieces of information for analysis. Past research on communications has shown that online illicit markets are often decentralized settings where few key players can be identified (Décary-Hétu et al. 2012). The networks are far from dense and are structured around cliques. They bring together large numbers of loosely connected actors.

In addition to linking offenders together, Internet traces can be used to link dedicated websites that facilitate the sale of illicit goods and services. Relationships between websites can be detected using unique identifiers located in the source code of websites. Google Analytics identifiers, for example, have been used to connect online illicit markets to each other (Pazos et al. 2013) and to deanonymize up to a certain point the actors who run these markets.[5] The analytics software requires that the website owner insert his unique identifier in his code and if that trace is found on multiple websites, these websites are likely controlled or at least managed by the same group of actors. Secure socket shell (SSH) certificates are also highly valuable to infer links among websites, and in some cases, they may deanonymize hidden services hosted on servers containing websites available through the 'surface web'.[6] These certificates are bound to a single identity and can therefore be used to link websites together.

Internet traces can also be used to identify links based on technical traces created by the many protocols used to communicate through the Internet (i.e., protocol traces). Online illicit markets are hosted on web servers and must use the domain name system (DNS) to translate their domain name (e.g., evilmarket.com) to an IP address that computers can understand. This requires that market administrators register their domain names with legitimate companies called registrars. This registration process leaves digital traces in publicly available databases known as WHOIS records databases. Contact information of the registrant (i.e., a name, a physical address or an email) can be mined on these databases. Although this data can be spoofed or anonymized, it may help in the detection of relationships between domain names acquired by same offenders.

Because DNS records store the IP address of each domain name, it is also possible to look for websites hosted on the same IP address as online illicit markets and to create ties between all the websites hosted on the same IP address. Researchers or investigators have, however, to be cautious when interpreting such links since several computers may share the same IP address at the same time because their hosting service may use carrier-grade network address translation (CGN) to overcome the limits of the IPv4.[7] Software like Maltego[8] have been devised to automate as much as possible the analysis of the infrastructure used by offenders to lift their anonymity by collecting connection logs and contact information.

The collection of HTTP traffic headers can be used to detect the type of server being run, the version of the operating system it runs and other discriminant traces like cookies. At the application level, each choice made by the designer of a website leaves traces. Of particular interest is the integration of other services such as anonymization services (e.g., Cloudflare) and content delivery networks where offenders have to register an account and potentially divulge information about themselves. This can help build a technological profile (i.e., a 'web app fingerprint'[9]) of offenders' infrastructure that can support the detection of their activities. Finally, a completely unexplored field of study is the exploitation of clock-skews to infer links between web servers. Each clock of a computer has deficiencies that may lead to temporal shifts due to imperfections in the cheap quartz they use. If these clock-skews are not enough discriminant to lead to an individualization, they may, nevertheless, complete the profile of a website infrastructure to infer or revise links (Polcák and Franková 2015). These traces are of particular interest, since they are, as far as we know, the only Internet traces (i.e., timestamps of several protocols) resulting from a purely physical process.[10]

Whether they operate on dedicated websites or in online communities, offenders also routinely leak information about themselves through their social interactions and allow for the gathering of intelligence about them. Mining the content of their websites and their public posts has proven extremely valuable. Past research has identified email addresses and other personal information of offenders that have helped lift the veil of anonymity surrounding them. The case of the Silk Road administrator, the first cryptomarket launched in 2011, is particularly interesting. Its administrator appears to have posted on a forum a message asking for help to design his cryptomarket using his personal email address (Paul 2015). This supposedly led to his identification and subsequent arrest. In addition to an email address, phone numbers, Skype aliases, PGP keys and Bitcoin Wallet IDs are all Internet traces that can be used to link together the activity of multiple online personas (see, for instance, Broséus et al. 2016b).

The content of messages has also been mined for stylometry analysis to connect different online personas together. These studies have shown that many offenders used multiple nicknames but that their writing styles could leak information about their true identity. A forensic analysis of the passwords used by offenders has similarly found connections between sets of offenders who used the same password to identify themselves in online illicit markets (Décary-Hétu and Eudes 2015). On dedicated websites, a content comparison may also help to infer links between markets. Two approaches may be used. First, textual or multimedia content can be extracted and compared with hashes, for example. Second, traffic analysis can be used to define a profile of a web page content that can be compared to other webpages (Hintz 2002). This process may for instance support the comparison of the index page of websites. It may also support the detection of changes. Indeed, modifications are of high value to monitor online markets. On the one hand, they allow the detection of new activities and trends. On the other hand, a concomitant change can be the sign of the activity of a same offender. These kinds of coordinated modifications may be directly visible in the content of the web page (e.g., an offer or contact information modification) or more subtly, as in a technological choice modification. The same inference is done by comparing newsletters that offenders make available on selling websites. Indeed, a relationship can be detected when the same news is simultaneously received from two apparently distinct websites.

Evaluating the validity and the strength of a relationship inferred on the basis of Internet traces is challenging. Indeed, this forensic process relies on the evaluation of the probability of a common source (e.g., a same person, a same object) or a common cause (i.e., the criminal activity). This analogical reasoning is uncertain by nature and requires controlled conditions (i.e., situations where the common source or cause is known to be true) to estimate a probabilistic value to the link. Nevertheless, as noted by Morelato and colleagues (2014, 184), ‘the analyses conducted in an intelligence perspective are different from those conducted in the probative (traditional) process since what is sought is the proximity between two objects rather than the discrimination between objects'. Thus, if all Internet traces described above may be used to infer a common cause or activity, they may also be compared with each other to evaluate their validity or strengthen the hypotheses. Another approach is to combine Internet and physical traces (see below).

Identifying offenders' physical location is a key challenge with online illicit markets. Indeed, the market structure may greatly vary across countries (Broséus et al. 2016a; Broséus et al. 2017). Many Internet traces are linked to physical locations and their combination may lead to the localization of offenders: (1) IP addresses checked against geoip databases such as Maxmind; (2) area code extracted from phone numbers (although international call forwarding may be detected); (3) ccTLD and WHOIS information obtained from a URL; (4) a geotag in the metadata of an image; (5) the time zone of a timestamp; (6) finally, text content and language can also be an indicator.

The estimation of illicit order volumes is also challenging but some research has suggested inference techniques based on test purchases and online store order numbering, or based on opportunistic server log data access (Kanich et al. 2011; McCoy et al. 2012). A small subset of research has also sought to follow the money, a key endeavour of offline money laundering and drug dealing investigations. Sellers posting their Western Union client number or their Liberty Reserve identification number could indeed be tracked across markets or identified if they tried to create a new seller account after being banned for abusing other offenders. Cryptocurrencies now afford opportunities for even better tracking of offenders since most cryptocurrency transactions are posted publicly on the Internet in public ledgers which can be data mined and analysed. These ledgers have been used to evaluate the size and scope of cryptomarkets and to characterize ransomware campaigns, the type of malware attack that encrypts files on computers and then asks for a ransom to provide the decryption key. Specialized software like BitCluster offers a free and open-source tool to monitor the flows of cryptocurrencies like bitcoin (Lavoie and Décary-Hétu 2016).

Trafficking in Human Beings: The Case of Sexual Exploitation

Information technologies have facilitated the rise of new forms of human trafficking. In this section, we focus on sexual exploitation, which can be defined as obtaining services of a sexual nature through the use of force, threat, deception or coercion.[11] Sexual exploitation is the most frequently identified form of human trafficking. Past research indicates that the Internet can serve as an enabler of sexual exploitation and thus warrants further attention (Walby et al. 2016). Indeed, many virtual convergence settings are used by the actors in this market to either recruit victims or sell sexual services. In addition, the Internet is also being used to communicate with clients, to gather information on available services, and even to provide reviews of escort services by the clients (Kunze 2010; Sarkar 2015).

To recruit victims, online advertisements are (a) placed on classified advertisements sites, (b) placed on dedicated thematic websites of au pairs, international marriage or dating agencies, (c) shared through direct contacts in chat rooms or social networking services, or (d) sent by unsolicited emails (Europol 2014; Tidwell 2016; Sykiotou 2007; Watson et al. 2015). Victims may be attracted by job opportunities such as waitressing, childcare, dancing or modelling (Logan et al. 2009; McAlister 2014; Dixon 2013; Nazemi 2011; Sykiotou 2007). The extent to which the Internet is used and how effective it is in recruiting victims remains unclear. Indeed, in many cases of sex trafficking in Europe, the Internet does not seem to be used to recruit victims but rather as a facilitator to advertisements for the selling of services (Sykiotou 2007).

The Internet is an excellent medium to match sexually exploited individuals with clients using online illicit markets. Much of the traditional street prostitution trade appears to have moved online in favour of Internet-enabled indoor and hidden forms of prostitution (Farley et al. 2013). The Internet appears to have had the greatest impact on communications between sellers and buyers. Traffickers are using many types of websites to advertise including classified advertisement websites, social networking websites, chat rooms and dedicated escort websites. More recently, mobile applications are also used to assist customers to locate nearby sex services (Finn and Stalans 2016). More often than not, traffickers use legitimate services to promote their activities by hiding them as massage or ‘dating’ services (Heil and Nichols 2014). The detection of sex trafficking activities managed by organized crime groups (OCG) through the analysis of publicly available advertisements is thus the main challenge. Indeed, dedicated methodologies have to be settled to distinguish OCGs' advertisements from posters who are selling their own independent services (Konrad et al. 2017; Farley et al. 2013; Heil and Nichols 2014). Several approaches have been proposed and tested on American online services such as Craigslist and Backpage, to name two. The methodologies are based on the detection of (a) occurrences of terms of interest compiled through interviews with law-enforcement investigators, (b) language patterns such as the use of the third person or plural pronouns, (c) keywords related to a child (e.g., 'candy', 'fresh', 'new to the game', 'doll', 'daddy's girl'), (d) countries of interest, (e) multiple victims advertised, (f) age and weight as a sign of a child, (g) references to escort websites or spa massage therapy, (h) images, and finally (i) contact information (Kennedy 2012; Wang et al. 2012; Silva et al. 2014; Heil and Nichols 2014; Nichols and Heil 2015; Dubrawski et al. 2015; Nagpal et al. 2016; Alvari et al. 2016; Finn and Stalans 2016).

The detection of specific Internet traces allows the reconstruction of networks of advertisements, which may be linked to OCGs. Contact information (e.g., phone numbers, emails, URLs, social media handles) is of particular interest in inferring the activity of a same group of offenders. Language homologies, similarities in content, as well as locations and displacement patterns can also help to bridge gaps between groups (Latonero et al. 2012; Dubrawski et al. 2015; Nagpal et al. 2016; Alvari et al. 2016; Konrad et al. 2017). Spatial analysis of advertisements may also serve the detection of sex tours that may be the sign of exploitation (Hughes 2014). However, only a few online advertisements are currently accurately classified as linked to trafficking (Dubrawski et al. 2015; Alvari et al. 2016).

Peppet (2012) argues that the Internet has provided a new means for both clients and prostitutes to sort through and review each other and thus to reduce harms and the spread of diseases. Independent prostitutes may reach a huge number of customers and screen them on the web (e.g., by emails, online blacklists and identity verification services) to reduce risks of violence and disease. However, this may be true only if they are not coerced (Cunningham and Kendall 2013). Interactive review sites and escort websites allow clients to talk about and rate prostitutes online (Peppet 2012). This may inherently degrade women, creates an added stressor for prostitutes and a new way of exerting pressure for traffickers (Cunningham and Kendall 2013).

Since offenders leave Internet traces that can support law enforcement investigations, the development of accurate methodologies to detect the activities of OCGs during the online advertising process (for both recruitment and selling of services) is promoted as a key leverage that can lead to proactive actions (Europol 2016). Benefits include the ability to detect suspicious activities and 'hot spots' to start undercover operations and criminal investigations (Mitchell and Boyd 2014). Overall, the key issues are (a) the identification and protection of victims, (b) the development of a shared methodology to gather and interpret Internet traces, (c) the development of methodologies and technologies for detecting traffickers, and (d) the use of the Internet to disseminate and raise public awareness about THB and the danger of online recruitments (Walby et al. 2016).

Toward the Integration of Internet and Physical Traces to Reconstruct Illicit Trafficking

A rarely explored trend in research on online illicit markets is the collection and analysis of physical traces. The online activities of illicit markets' offenders are indeed only a part of the whole illicit trafficking process (see Figure 1). Even if each stage of the process may happen in the physical world, we focus our discussion on the relationships between situations where promotion, selling and review steps happen online and physical goods such as illicit drugs or counterfeiting goods are trafficked. Indeed, when digital goods are the object of the traffic, all the stages may happen online. The promotion, selling and review stage have already been discussed earlier in this chapter. The term 'acquisition' is chosen, because 'manufacturing' only applies to physical goods, although illicit trafficking may concern stolen goods as well as the trafficking of human beings. In the former case, 'acquisition' means 'theft' and it corresponds to the 'recruitment phase' in the latter.

<Insert Figure 1 here>

The integration of Internet traces with physical traces can take many forms. It may first help to better understand the structure of a market (i.e., the number of actors and their relationships) at each stage of the trafficking process, whether it takes place online and/or in the physical world.

Ultimately it aims to compare the findings at each stage to reconstruct the whole structure. Such a combination of information may lead to the evaluation of the volume of sales, their temporal trends, the number of actors, their location and their relationships all along the process. Moreover, comparisons lead to evaluation of the validity, significance and pertinence of each source of information and may help to interpret the findings.

The physical and/or chemical analyses of products bought in online markets or seized by law enforcement agencies are the first pathway to achieve integration. These products can be bought by law enforcement and interested groups like industry lobby groups seeking to help protect their members and researchers. For the last group, this may raise ethical considerations since purchasing illicit goods is illegal (McCoy et al. 2012). Further ethical considerations are raised since making purchases finances organized crime, which could lead to the victimization of certain individuals. Such cases are, therefore, few and far between. An innovative approach to skirt the ethical conundrums is to ask offenders themselves to provide researchers with samples. This is what Dr X has achieved with his drug-testing lab in Spain (Caudevilla 2016). Offenders pay 50 euros to get a drug sample analyzed and the report Dr X and his team generate can even help improve the public health of drug users as they can make sure that the drugs they are using are not dangerous.

In some case, researchers have managed to purchase illicit drugs such as cocaine, cannabis and GBH (Pazos et al. 2013; Rhumorbarbe et al. 2016). These purchases led to analyses of the chemical composition of the products and to the evaluation of the purity of their active ingredients as well as the detection of forensic links between purchases. The chemical composition (i.e., purity, cutting agents) of cocaine purchased online was similar to specimens confiscated in the streets, but a lower purity than claimed was observed (Rhumorbarbe et al. 2016). Packaging and concealment techniques described by sellers (in their online listings) appear to be accurate in regard to received products. Thus a more systematic analysis of online description may lead to interesting new knowledge (Aldridge and Askew 2017). From the few studies that have performed online purchases, global outcomes may be outlined: (1) the forensic analysis of products bought online allows the evaluation of the relevance and, in some cases, the accuracy of digital data collected on the website (Rhumorbarbe et al. 2016); (2) the analysis of transportation traces such as delivery notes, tracking information and packaging may confirm the country of origin; (3) links detected between websites may be compared to physical and/or chemical links detected by the forensic analysis of products to better understand the market structure at each step (Pazos et al. 2013; Broséus et al. 2016a); (4) financial traces may be analysed and order numbering used to evaluate sales' volumes (Levchenko et al. 2011; McCoy et al. 2012).

Another promising integration between Internet and physical traces is the comparison of online selling and review settings with the analysis of wastewater. On the one hand, identifying the most discussed substances in online forums (see, for instance, Pineau et al. 2016) or sold online (see, for instance, McCoy et al. 2012) may help target the strategy of wastewater analysis. On the other hand, the comparison of online and physical indicators may lead to a more accurate evaluation of the prevalence and detection of new trends of consumption (for a more detailed discussion, see Esseiva et al., 'Evaluating the Consumption of Illicit Drugs via Wastewater Analysis' in this volume).

Conclusion

This chapter has reflected on the use of Internet traces either on their own or in combination with physical traces. Through this discussion, we highlighted the numerous challenges that offenders face when buying and selling illicit goods and services online as well as the challenges researchers are likely to face when collecting Internet traces.

In order to maximize the research potential of Internet traces, collaboration between forensic scientists, criminologists and even computer scientists will be essential. The acquisition of this particular type of digital trace requires the use of adequate methodologies and technical tools. Criminologists and most forensic scientists are not trained in the use of these tools and will need each other and/or the help of computer scientists to determine appropriate approaches and integrate them into their data collection processes. Given the specificity of Internet traces, it is essential that researchers who take advantage of them are aware of their limits in order not to overstate their meaning. And as explained earlier, the software used to collect web pages may transform their content and not collect parts of the page in many cases. Researchers or investigators must therefore be very careful when they analyze Internet traces. The forensic scientists who have the necessary skills to collect Internet traces and physical traces may not be familiar enough with the context of online illicit markets and the networks of offenders who populate them. They may therefore be able to gather traces but have more difficulty giving them some context and understanding how they fit in the overall markets. Such lack of knowledge may even prevent them from detecting or using relevant traces. Herein lies a dual relationship between forensic science and criminology.

The study of online illicit markets is therefore an excellent example of how combining physical and Internet traces can help both disciplines to better understand offenders. This collaboration will become ever more important as more and more offenders shift their activities to the Internet either in the 'surface web' or the 'dark web'. Their activities will likely become stealthier over this transition and a precise understanding of who the actors are and how they network with each other will be needed. It appears that the rate of criminal innovation is constantly increasing and the collaboration between forensic scientists and criminologists will be one important strategy in keeping up with offenders who work in teams that benefit from the specialization of their members.

References

Akers, R.L., M.D. Krohn, L. Lanza-Kaduce and M. Radosevich. 1979. 'Social Learning and Deviant Behavior: A Specific Test of a General Theory'. *American Sociological Review* 44(4): 636–655.

Aldridge, J., and R. Askew. 2017. 'Delivery Dilemmas: How Drug Cryptomarket Users Identify and Seek to Reduce Their Risk of Detection by Law Enforcement'. *International Journal of Drug Policy* 41: 101–109.

Alvari, H., P. Shakarian and J.K. Snyder. 2016. 'A Non-Parametric Learning Approach to Identify Online Human Trafficking'. IEEE Conference on Intelligence and Security Informatics: Cyber Security and Big Data (ISI): 133–138.

Bandura, A. 1971. *Social Learning Theory*. New York: General Learning Press.

Broséus J., S. Baechler, N. Gentile, and P. Esseiva. 2016a. ‘Chemical Profiling: A Tool to Decipher the Structure and Organisation of Illicit Drugs Markets: An 8-Year Study in Western Switzerland’. *Forensic Science International* 266(September): 18–28.

Broséus J., D. Rhumorbarbe, C. Mireault, V. Ouellette, F. Crispino and D. Décary-Hétu. 2016b. ‘Studying Illicit drug Trafficking on Darknet Markets: Structure and Organisation from a Canadian Perspective’. *Forensic Science International* 264: 7–14.

Broséus, J., D. Rhumorbarbe, M. Morelato, L. Staehli and Q. Rossy. 2017. 'A Geographical Analysis of Trafficking on a Popular Darknet Market'. *Forensic Science International*, submitted.

Casey, E. 2011. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Waltham, MA: Academic Press.

Caudevilla, F., M. Ventura, I. Fornís, M.J. Barratt, C. Vidal, P. Quintana, A. Muñoz and N. Calzada. 2016. ‘Results of an International Drug Testing Service for Cryptomarket Users.’ *International Journal of Drug Policy* 35: 38–41.

Christin, N. 2013. ‘Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace.’ Proceedings of the 22nd International Conference on World Wide Web, Rio de Janeiro.

Cunningham, S., and T. Kendall. 2013. ‘Prostitution 3.0: A Comment’. *Iowa Law Review Bulletin* 98: 131–141.

Décary-Hétu, D., B. Dupont and F. Fortin. 2014. ‘Policing the Hackers by Hacking Them: Studying Online Deviants in IRC Chat Rooms’. In A.J. Masys, ed., *Networks and Network Analysis for Defence and Security*, 63–82. New York: Springer.

Décary-Hétu, D., and M. Eudes. 2015. ‘Partenariats criminels au sein d’un forum de carding: alliés, rivaux ou escrocs? Étude de l’utilisation d’identités virtuelles multiples’. *Revue internationale de criminologie et de police technique scientifique* 68(3): 299–314.

Décary-Hétu, D., and D. Laferrière. 2015. ‘Discrediting Vendors in Online Criminal Markets’. In A. Malm and G. Bichler, eds., *Disrupting Criminal Networks: Network Analysis in Crime Prevention*, 129–152. Boulder: Lynne Rienner.

Décary-Hétu, D., and A. Leppänen. 2016. ‘Criminals and Signals: An Assessment of Criminal Performance in the Carding Underworld’. *Security Journal* 29(3): 442–460.

Décary-Hétu, D., C. Morselli and S. Leman-Langlois. 2012. ‘Welcome to the Scene: A Study of Social Organization and Recognition among Warez Hackers’. *Journal of Research in Crime and Delinquency* 49(3): 359–382.

Dixon, H. 2013. ‘Human Trafficking and the Internet (and Other Technologies, Too)’. *Judges Journal* 52(1): 36–39.

Dubrawski, A., K, Miller and M. Barnes. 2015. ‘Leveraging Publicly Available Data to Discern Patterns of Human-Trafficking Activity’. *Journal of Human Trafficking* 1(1): 65–85.

Europol. 2016. *Situation Report: Trafficking in Human Beings in the EU*. The Hague: Europol.

Europol. 2014. *Trafficking in Human Beings and the Internet*. The Hague: Europol, Intelligence Notification 15/2014.

Farley, M., K. Franzblau and M. Kennedy. 2013. ‘Online Prostitution and Trafficking’. *Albany Law Review* 77(3): 1039–1094.

Felson, M. 2003. ‘The Process of Co-Offending’. In M.J. Smith and D.B. Cornish, eds., *Theory for Practice in Situational Crime Prevention* 16, 149–168. Devon: Willan Publishing.

Finn, M.A., and L.J. Stalans. 2016. ‘How Targeted Enforcement Shapes Marketing Decisions of Pimps: Evidence of Displacement and Innovation’. *Victims & Offenders* 11(4): 578–599.

Fredman, C. 2015. ‘Fund Me or Fraud Me? Crowdfunding Scams Are on the Rise’. Online http://www.consumerreports.org/cro/money/crowdfunding-scam.

Heil, E., and A. Nichols. 2014. ‘Hot Spot Trafficking: A Theoretical Discussion of the Potential Problems Associated with Targeted Policing and the Eradication of Sex Trafficking in the United States’. *Contemporary Justice Review* 17(4): 421–433.

Hintz, A. 2002. ‘Fingerprinting Websites Using Traffic Analysis’. In *International Workshop on Privacy Enhancing Technologies*, 171–178. New York: Springer Berlin Heidelberg.

Holt, T.J. 2007. ‘Subcultural Evolution? Examining the Influence of On- and Off-Line Experiences on Deviant Subcultures’. *Deviant Behavior* 28(2): 171–198.

Holt, T.J., and E. Lampke. 2010. ‘Exploring Stolen Data Markets Online: Products and Market Forces’. *Criminal Justice Studies* 23(1): 33–50.

Holt, T.J., O. Smirnova, and Y.T. Chua. 2016. ‘Data Thieves in Action: Examining the International Market for Stolen Personal Information.’ New York: Palgrave Macmillan.

Hughes, D.M. 2014. ‘Trafficking in Human Beings in the European Union : Gender, Sexual Exploitation, and Digital Communication Technologies’. *SAGE Open* 4(4): 1–8.

Kanich, C., N. Weaver, D. McCoy, T. Halvorson, C. Kreibich, K. Levchenko, V. Paxson, G.M. Voelker and S. Savage. 2011. ‘Show Me the Money: Characterizing Spam-Advertised Revenue’. Proceedings of the USENIX Security Symposium, San Francisco, 15–15.

Kennedy, E. 2012. ‘Predictive Patterns of Sex Trafficking Online’. Honours thesis, Carnegie Mellon University, Pittsburgh. http://repository.cmu.edu/hsshonors/155/.

Konrad, R., A.C. Trapp, T.M. Palmbach and J.S. Blom. 2017. ‘Overcoming Human Trafficking via Operations Research and Analytics: Opportunities for Methods, Models, and Applications’. *European Journal of Operational Research* 259(2): 733–745.

Kruithof, K., J. Aldridge, D. Décary-Hétu, M. Sim, E. Dujso and D. Hoorens. 2016. *Internet-Facilitated Drugs Trade: An Analysis of the Size, Scope and the Role of the Netherlands*. RAND Corporation, Santa Monica, CA, and Cambridge, UK. http://www.rand.org/pubs/research_reports/RR1607.html.

Kunze, E.I. 2010. ‘Sex Trafficking via the Internet: How International Agreements Address the Problem and Fail to Go Far Enough’. *Journal of High Technology Law* 10(2): 241–289.

Latonero, M., J. Musto, Z. Boyd, E. Boyle, A. Bissel, K. Gibson and J. Kim. 2012. *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*. Research Series on Technology and Human Trafficking. http://technologyandtrafficking.usc.edu/files/2012/11/Tech_Trafficking_2012_SUMMARY.pdf.

Lavoie, M., and D. Décary-Hétu. 2016. ‘De-Anonymizing Bitcoin One Transaction at a Time’. https://livestream.com/internetsociety2/hopeconf/videos/130587981.

Leontiadis, N., T. Moore and N. Christin. 2011. ‘Measuring and Analyzing Search-Redirection Attacks in the Illicit Online Prescription Drug Trade’. Proceedings of the USENIX Security Symposium, San Francisco, 1–17.

Levchenko, K., A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich … and S. Savage. 2011. ‘Click Trajectories: End-to-End Analysis of the Spam Value Chain’. 2011 IEEE Symposium on Security and Privacy, Oakland, CA (SP): 431–446.

Li, Z., K. Zhang, Y. Xie, F. Yu and X. Wang. 2012. ‘Knowing Your Enemy: Understanding and Detecting Malicious Web Advertising’. Proceedings of the 2012 ACM Conference on Computer and Communications Security 674–-686.

Logan, T.K., R. Walker and G. Hunt. 2009. ‘Understanding Human Trafficking in the United States’. *Trauma, Violence & Abuse* 10(1): 3–30.

McAlister, R. 2014. ‘Webscraping as an Investigation Tool to Identify Potential Human Trafficking Operations in Romania’. Proceedings of the ACM Web Science Conference (WebSci ’15), 2. New York: ACM.

McCoy, D., A. Pitsillidis, G. Jordan, N. Weaver, C. Kreibich, B. Krebs, M. Voelker, S. Savage and K. Levchenko. 2012. ‘Pharmaleaks: Understanding the Business of Online Pharmaceutical Affiliate Programs’. Proceedings of the 21st USENIX Conference on Security Symposium, Bellevue, WA.

Meyer, G.R. 1989. ‘The Social Organization of the Computer Underground’. MSc thesis, Northern Illinois University.

Mitchell, K.J. and D. Boyd. 2014. ‘Understanding the Role of Technology in the Commercial Sexual Exploitation of Children: The Perspective of Law Enforcement’. Crimes Against Children Research Center University of New Hampshire: Durham, NH. http://scholars.unh.edu/ccrc/37/

Morelato, M., S. Baechler, O. Ribaux, A. Beavis, M. Tahtouh, P. Kirkbride, C. Roux and P. Margot. 2014. ‘Forensic Intelligence Framework. Part I: Induction of a Transversal Model by Comparing Illicit Drugs and False Identity Documents Monitoring’. *Forensic Science International* 236(March): 181–190

Motoyama, M., D. McCoy, K. Levchenko, S. Savage and G.M. Voelker. 2011. ‘An Analysis of Underground Forums’. Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement, Berlin, Germany, 71–80.

Nagpal, C., K. Miller, B. Boecking and A. Dubrawski. 2016. ‘An Entity Resolution Approach to Isolate Instances of Human Trafficking Online’. arXiv preprint arXiv:1509.06659.

Nazemi, N. 2011. ‘Role of Internet in Human Trafficking’. *Indian Journal of Social Development* 11(2): 517–540.

Nichols, A.J., and E.C. Heil. 2015. ‘Challenges to Identifying and Prosecuting Sex Trafficking Cases in the Midwest United States’. *Feminist Criminology* 10(1): 7–35.

Paul, K. 2015. “How Silk Road’s Founder Could Have Avoided Getting Busted.” Online: https://motherboard.vice.com/en_us/article/the-five-hidden-service-commandments.

Pazos D., P. Giannasi, Q. Rossy and P. Esseiva. 2013. ‘Combining Internet Monitoring Processes, Packaging and Isotopic Analyses to Determine the Market Structure: Example of Gamma Butyrolactone’. *Forensic Science International* 230(1–3): 29–36.

Peppet, S.R. 2012. ‘Prostitution 3.0’. *Iowa Law Review* 98: 1989–2060.

Pineau, T., A. Schopfer, L. Grossrieder, J. Broséus, P. Esseiva and Q. Rossy. 2016. ‘The Study of Doping Market: How to Produce Intelligence from Internet Forums’. *Forensic Science International* 268(November): 103–115.

Polcák, L., and B. Franková. 2015. ‘Clock-Skew-Based Computer Identification: Traps and Pitfalls’. *Journal of Universal Computer Science* 21(9): 1210–1233.

Rhumorbarbe D., L. Staehli, J. Broséus, Q. Rossy and P. Esseiva. 2016. ‘Buying Drugs on a Darknet Market: A Better Deal? Studying the Online Illicit Drug Market through the Analysis of Digital, Physical and Chemical Data’. *Forensic Science International* 267(October): 173–182.

Sarkar, S. 2015. ‘Use of Technology in Human Trafficking Networks and Sexual Exploitation: A Cross-Sectional Multi-Country Study’. *Transnational Social Review* 5(1): 55–68.

Silva, D.R., A. Philpot, A. Sundararajan, N.M. Bryan and E. Hovy. 2014. ‘Data Integration from Open Internet Sources and Network Detection to Combat Underage Sex Trafficking’. Proceedings of the 15th Annual International Conference on Digital Government Research—dg.o ’14, Aguascalientes, Mexico, 86–90.

Soska, K., and N. Christin. 2015. ‘Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem’. Proceedings of the 24th USENIX Security Symposium, Washington, DC 33–48.

Soudijn, M.R., and B.C.T. Zegers. 2012. ‘Cybercrime and Virtual Offender Convergence Settings’. *Trends in Organized Crime* 15(2–3): 111–129.

Sutherland, E.H. 1947. *Principles of Criminology*. 4th ed. Chicago: J.B. Lippincott Co.

Sykiotou, A.P. 2007. *Trafficking in Human Beings: Internet Recruitment*. Directorate General of Human Rights and Legal Affairs, Council of Europe, Strasbourg. https://ec.europa.eu/anti-trafficking/publications/trafficking-human-beings-internet-recruitment-misuse-internet-recruitment-victims_en.

Thomas, K., D. McCoy, C. Grier, A. Kolcz and V. Paxson. 2013. ‘Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse’. Proceedings of the 22nd USENIX Security Symposium 13: 195–210.

Tidwell, R. 2016. ‘Caught in the Web: The Importance of Ethical Computing Illustrated via an Exploration of the Online Recruitment of Women and Girls into Sex Trafficking’. Honors Senior thesis, Western Oregon University. http://digitalcommons.wou.edu/honors_theses/111/.

Tremblay, P. 2010. *Le délinquant idéal. Performance, discipline, solidarité*. Montréal: Liber.

Van Hout, M.C, and E. Hearne. 2017. ‘New Psychoactive Substances (NPS) on Cryptomarket Fora: An Exploratory Study of Characteristics of Forum Activity between NPS Buyers and Vendors’. *International Journal of Drug Policy* 40: 102–110

van Mierlo, T. 2014. ‘The 1% Rule in Four Digital Health Social Networks: An Observational Study’. *Journal of Medical Internet Research* 16(2): e33.

Vinciarelli, A., M. Pantic, D. Heylen, C. Pelachaud, I. Poggi, F. D’Errico and M. Schroeder. 2012. ‘Bridging the Gap between Social Animal and Unsocial Machine: A Survey of Social Signal Processing’. IEEE Transactions on Affective Computing 3(1): 69–87.

Walby, S., J. Towers, B.J. Francis, K. Shire, L. Kelly, B. Apitzsch, ... and S. Kirby. 2016. *Study on Comprehensive Policy Review of Anti-Trafficking Projects Funded by the European Commission*. HOME/2014/ISFP/PR/THBX/0052. http://eprints.lancs.ac.uk/82220/.

Wang, H., C. Cai, A. Philpot, M. Latonero, E.H. Hovy and D. Metzler. 2012. ‘Data Integration from Open Internet Sources to Combat Sex Trafficking of Minors’. Proceedings of the 13th Annual International Conference on Digital Government Research: 246–252.

Watson, H., A. Donovan and J. Muraszkiewicz. 2015. ‘Role of Technology in Human Trafficking’. http://trace-project.eu.

Wehinger, F. 2011. ‘The Dark Net: Self-Regulation Dynamics of Illegal Online Markets for Identities and Related Services’. European Intelligence and Security Informatics Conference (EISIC), Athens, 209–213.

[1] https://openbazaar.org/.

[2] http://www.financemagnates.com/cryptocurrency/education-centre/went-shopping-drugs-fake-ids-guns-using-bitcoin-openbazaar/.

[3] For instance try to access: … with Chrome and Firefox.

[4] See geopeeker.com and insert a well-known url such as http://www.ubs.com or more interesting: http://www.timescopy.cn/.

[5] Several online databases are available to search links with Google Analytics identifiers: http://sameid.net, http://spyonweb.com, https://www.shodan.io or http://nerdydata.com.

[6] For instance, see the online databases of https://www.shodan.io or https://censys.io.

[7] This situation may occur in the specific case of a dynamic addressing of the IP address.

[8] https://www.paterva.com.

[9] See, for instance, http://wappalyzer.com.

[10] Although we can speculate that the accelerometer and the gyroscope of a mobile device may also produce or impact digital traces, they might unlikely be Internet traces.

[11] http://www.ohchr.org/EN/ProfessionalInterest/Pages/ProtocolTraffickingInPersons.aspx.