‘License to Pill’
Illegal Entrepreneurs’ Tactics in the Online Trade of Medicines

Alexandra Hall and *Georgios A. Antonopoulos*[1]

Introduction

Product counterfeiting is a long-established criminal pursuit that has increased at an exponential rate in recent times, so much so that the trade in counterfeit goods is estimated to account for anything up to 7 per cent of world trade, equivalent to $500 billion (see Yar, 2005; 2008). This includes a burgeoning global trade in ‘fake’ medicines. With the advent of the Internet and e-commerce – increasingly seen as the cornerstone of the new global social and economic order (Castells, 2001) – this market has expanded significantly. It is estimated that the ‘fake’ medicine trade alone has increased by 90 per cent since 2005, with an approximate turnover of $200 billion (IRACM, 2013: 16). However, despite resultant criminal profits, as well as social and physical harms, the illegal online trade of medicines has received little scholarly attention, and research and preventative action remain largely ineffective.

The aim of the present chapter is to provide an original empirical account of the tactics and methods illegal entrepreneurs employ in order to market medicines online while avoiding being detected by law enforcements agencies and health regulatory authorities. The chapter is based primarily − although not exclusively − on our research in the UK, which is part of the FAKECARE project: a European Commission–funded project that aims to develop expertise that can help appropriate agencies to tackle the online trade of ‘fake’ medicines by, among other things, providing an in-depth knowledge of the supply and demand dimensions of this criminal market.

Following the introduction, the chapter is organised into five sections. The first section briefly outlines the broader context of the trade in illicit medicines. The

[1] Alexandra Hall is researcher at the Teesside Centre for Realist Criminology, Teesside University, UK. Georgios A. Antonopoulos is professor of criminology at the Teesside Centre for Realist Criminology, Teesside University, UK. The authors would like to thank the reviewers for their comments and suggestions.

second section focuses on the infrastructure required in order to trade in medicines online. In the third section, we offer a description of the methodology adopted to explore the phenomenon. In the fourth section we focus on the findings: firstly we concentrate on the online tactics illicit entrepreneurs use to market their merchandise; and secondly we offer an account of the ways in which entrepreneurs trading in medicines online attempt to avoid detection by law enforcement and regulatory agencies. The chapter finishes with a discussion and analysis of our overall findings.

The broader context of the illicit medicine trade

The nature and specifics of the chapter's objectives demands some preliminary contextualisation of the illegal trade in medicines. The 'fake' medicine trade can be categorised according to three distinct 'business' models that work across different sites, scales and networks:

1. 'Entities' trading exclusively offline in the 'real' world;
2. 'Entities' that were originally involved in the trade offline, but have now moved online to distribute their merchandise;
3. 'Entities' that focus their skills exclusively in the virtual world.

One specific example of the latter is Glavmed, which has been described as "one of the most significant cases of cybercrime in the pharmaceutical sector" (IRACM, 2013: 70); a case we will return to in our analysis below. In this chapter we will focus primarily on the second and third models, whereby business is conducted either in part, or solely, online. Having said that, it is important to challenge the false dichotomy existing between online and offline processes involved in the formulation, manufacture and distribution of 'fake' medicines. Indeed, the online trade includes crucial offline dimensions. Here, we support the work of Guarnieri and Przyswa, who draw on the work of Sassen (2007), to argue that online and offline domains are not hybridised, but are interconnected with distinct characteristics (Guarnieri and Przyswa, 2013: 219).

Furthermore, there is an on-going debate surrounding the definition of 'fake' medicines. For reasons of economy in the chapter we use the term 'fake' to connote:

- *Counterfeit medicines*:

Here we adopt the World Health Organisation's (WHO) definition: "*A counterfeit medicine is one which is deliberately and fraudulently mislabelled with respect to identity and/or source. Counterfeiting can apply to both branded and generic products and counterfeit products may include products with the correct ingredi-*

ents or with the wrong ingredients, without active ingredients, with insufficient active ingredients or with fake packaging" (WHO, 2012).

- *Falsified medicines*:

Part of the debate regarding the definition of 'fake' medicines relates to the separation of counterfeits from the market in substandard and unlicensed generic drugs. For this reason the European Commission prefers to distinguish between *counterfeit* and *falsified* medicines. Whereas counterfeits are those infringing intellectual property (IP) rights, falsified medicines are any fakes attempting to pass themselves off as an authentic medicine. The term *falsification*, therefore, moves beyond merely legal-economic terms relating to copyright infringement and embeds public health and the 'sticky subject' of generics in the definition (see IRACM, 2013: 14).

- *Legally produced yet illegally supplied medicines*:

One of the problems facing those involved in preventing the global trade in counterfeit medicines is the varied IP rights and licensing laws operating over different jurisdictional boundaries. This includes variations across European states, where trademark infringement in one country may differ in another. On occasion, traders dealing in generics or various branded products produced abroad yet sold in the UK seek to by-pass existing IP laws and patents; these products may have been legally produced but are illegally supplied. For example, in the UK legitimate generics are licensed and, therefore, authorised as copies of a once patented and branded drug. However, when a patent expires an opening in the market for genuine and fake generics is created (see Chan, 2013): the most recent example in the UK being Viagra (sildenafil citrate) in 2013. Fakes in this instance can be counterfeits falsely claiming to be the branded product, or unlicensed products claiming to contain the identical active ingredients found in the formerly branded/patented product. One example is that of Kamagra, a sildenafil citrate based erectile dysfunction (ED) drug legally produced in India, which is not licensed in the UK. During our research we found a variety of online sites offering this product for sale as 'Generic Viagra' to UK customers. There is also a growing market of legally produced yet illegally supplied medicines entering the legitimate pharmaceutical supply chain (Yar, 2012).

Infrastructure required for online trading (of medicines)

In order to identify the tactics used by illegal online traders in pharmaceuticals we must first consider the infrastructure required for online sales of medicines (although this is the infrastructure that is necessary for any type of e-commerce). An

obvious primary component of the infrastructure is an *internet service provider*. An internet service provider is an organisation that provides services for accessing, using, or participating in the Internet. Internet service providers may be organised as commercial, community-owned, non-profit, or otherwise privately owned entities (e.g. Virgin Media, BT and Sky in the UK, Freenet AG and T-Online in Germany, Claranet and NLnet in the Netherlands, etc.).

Secondly, a *registrar* is an important node in the system. The Internet Corporation for Assigned Names and Numbers (ICANN) accredits commercial entities called 'registrars' that are authorised to sell domain names to the public. A very popular example is *GoDaddy.com*. Registrars are compelled to follow the law in their everyday business and are obliged to shut down illegal online pharmacies by suspending and 'locking' the domain name, therefore, ensuring that it is not transferred to another member of the public. A registrar that is found to be accepting fees from known illegal online pharmacies is considered to be a participant in the criminal activity. However, registrars respond to notifications from law enforcement authorities in various ways. Some cooperate, whereas others do not and are deemed non-compliant registrars.

Thirdly, a *payment processor* is required. A payment processor is a company (often a third party) appointed by a merchant to handle credit card transactions for merchants' acquiring banks. Payment processors enable the merchants to receive debit or credit card payments online by providing a connection to an acquiring bank. These processors perform a number of functions, which include evaluating whether transactions are valid and approved, and providing anti-fraud measures to assure that a purchase transaction is initiated by the source it claims to be. An established payment processor is, for instance, Mastercard.

Fourthly, *payment gateways* are a vital part of the process. They send credit card transactions to the payment processors, who are appointed to handle transactions with the acquiring bank. Significantly, payment gateways encrypt merchant and customer information during e-commerce transactions and offer secure pages. Registrars, payment processors and payment gateways are integral nodes of the infrastructure needed to trade in 'fake' medicines online, so much so that law enforcement consider them as the 'choke points' of the process (Burke, 2014); points that, if adequately controlled, can result in the closure of illegal online pharmacies.

Finally, an important part of the infrastructure is a *postal delivery service,* which guarantees that the merchandise traded online reaches customers in the 'real' world. This is one aspect of the infrastructure that largely involves legitimate companies (the large courier firm FedEx was recently indicted in the USA on charges of conspiracy to deliver illicit pharmaceuticals; see Walker 2014).

Methods and data

As part of our broader exploration of the supply and demand of 'fake' medicines online, a number of methods and sources were used to provide an account of the tactics illegal traders in pharmaceutical products employ in order to, firstly, market their merchandise online and, secondly, avoid the efforts of law enforcement agencies to prevent the trade. The methodology included a virtual ethnography. Traditionally, ethnographies were established as a means by which anthropologists and sociologists could explore cultural groups by using the technique of 'participant observation'. Observing and engaging with a specific group over an extended period of time allowed 'thick description' (Geertz, 1973), which both described and contextualised human behaviour and everyday experiences, actions and environments. In the present-day context, however, where everyday life for many includes a significant proportion of time spent in virtual communities, ethnography and social research more generally has been compelled to account for the multi-sited, mobile and transnational nature of modern social, cultural, political and economic life. Traditionally, local ethnographic research sites have therefore been expanded to analyse global, 'glocal', transnational and virtual sites (see Wittel, 2000). Whether in forums, blogs or social networking sites, social processes and patterns of communication take place in a new 'sphere' established by the Internet (Fielding *et al.*, 2008: 161). This requires from the ethnographer a methodology able to offer insights into the virtual worlds we regularly inhabit. What is typically labelled 'virtual ethnography' or 'netnography' has steadily increased in usage to offer researchers finely detailed insights into virtual communities (see for example Davey *et al.*, 2012; Fox *et al.,* 2005; Hine, 2000; Ward, 1999).

Primary data was collected via the virtual ethnography in both non-reactive and reactive ways (see Fielding *et al*, 2008). Initially, research began with a period of non-participant observation (sometimes referred to as 'lurking'), whereby observations were made in public forums and social networking sites without direct interaction with users. This was an invaluable primary stage of data collection that gave us the opportunity to familiarise ourselves with such a mass of information and specific interactions. Screenshots of images and text from forums, online pharmacies, social networking sites and classified advertising were collected. Moreover, social media and forum profiles, and email accounts were established in order to interact with users and take part in discussions with online consumers and suppliers of medicines. Just as Webber and Yip found in their analysis of 'carding' and the online trade in fake credit cards, internet forums are a largely untapped resource of empirical criminological research (Webber and Yip, 2013: 193).

In terms of selecting forums to enter, a literature review and online searches via Google were undertaken to identify forums that related to specific topics with links

(unintended or otherwise) to pharmaceutical consumption. Namely: health forums, bodybuilding, sleep, weight loss, pro-anorexia, mental health, sexual health, men's and women's health, general forums with keyword searches, drug forums and their prescription drug sections, and pregnancy and motherhood. Active participation followed and conversations were generated in these forums, as well as social networking sites – including Facebook and Twitter - and email discussion. It would be impossible to research the entirety of the web. Therefore, decisions were made to enter networks and online communities that appeared or claimed to primarily cover UK contexts over certain periods of time. This was decided after general searches, observations and discussions as to the most appropriate forums that individual users would utilise to discuss their experiences of buying and consuming specific prescription drugs. Thus such online networks and communities would be more likely to reveal information relating to the locations and identities of the pharmaceutical products' suppliers.

With regards to the supply side of the online trade in illicit medicines, this method was used to collect data from various online sellers and sites, which was then analysed, pooled and categorised in order to look for common patterns. This included posing as customers and interacting with sellers online in order to collect a number of specific details from a range of online sites. The virtual ethnography allowed us to collect rich data from online sites used for supply and to begin to analyse the networks that have proliferated throughout the various stages of the trade that caters for consumer demand in the UK.

However, there are limits to the utility of a virtual ethnography as an isolated method in this context. For instance, the researcher can only pool information that is openly available online. Moreover, illicit medicines are also physically traded, therefore, the distribution of the physical goods also requires investigation. For these reasons we also collected data from a range of other sources in order to triangulate the findings and offer richer and more comprehensive empirical evidence. Data from judicial and investigative cases, interviews with relevant stakeholders and enforcement officers, and secondary media and academic sources were gathered and analysed. Specifically, we collected data from the UK Medicines and Healthcare products Regulatory Agency (MHRA), National Crime Agency (NCA), Interpol and LegitScript[2]. This involved semi-structured interviews and general discussions with experts in these organisations in the UK and Europe. For example, we interviewed analysts at Interpol's Medical Product Counterfeiting and Pharmaceutical Crime Sub-Directorate, a head analyst at the UK's National Cyber Crime Unit responsible for 'shutting down' illegal online pharmacies, and the head of enforcement for the MHRA. Experts also provided us with some quantitative data. The NCA provided data regarding known illegal online pharmacies, which includ-

[2] LegitScript is a verification and monitoring service for online pharmacies.

ed information on domain names, registrars and registrants. The MHRA provided us with statistics relating to seizures of counterfeit medicines during raids from 2009-2014. We also gained access to ten investigative and judicial case files relating to online pharmaceutical crime at the MHRA. The above data have been used, alongside our ethnographic research, to build an accurate picture of the online trade in 'fake' medicines and, in the context of this chapter's objectives, to begin to analyse the tactics used by cyber-criminal entrepreneurs involved in the trade.

In addition, we attended the two-day workshop of the 'Pangea' Single Points of Contact (SPoCs) at INTERPOL's headquarters in Lyon in March 2014, where representatives of law enforcement agencies (police and customs), health regulatory agencies (including the MHRA) and representatives of the private sector (for example Mastercard, Microsoft and LegitScript) were present to discuss various aspects of the 'Pangea' operation. This is an annual international operation that began in 2008, which takes place for one week and is specifically aimed at tackling the online trade in illicit medicines. 'Pangea' is coordinated by INTERPOL, the World Customs Organisation, the Permanent Forum of International Pharmaceutical Crime (PFIPC), the Heads of Medicines Agencies Working Group of Enforcement Officers (HMA WGEO), the pharmaceutical industry and the electronic payments industry. During the two-day workshop we obtained data from presentations and informal interviews with individuals from the aforementioned agencies and organisations, as well as from unpublished manuals and reports used by the authorities in various countries.

Finally, we collected data via traditional ethnographic methods. The offline ethnography was conducted in a gym in the Northeast of England in which the use and trade of anabolic steroids is widespread. At this point it should be mentioned that this particular locale has one of the highest rates of steroid use in the UK (see Kean, 2012). Within the context of this ethnographic research, we had the opportunity to acquire knowledge regarding a variety of illegal activities and, most importantly for this chapter, the use and (online) trade of anabolic steroids. To a considerably lesser extent, data were also collected in relation to other performance-enhancing substances. Interviews were conducted as free-flowing conversations with participants on a series of occasions between January 2014 and July 2014. Most of the interviews were quite informal and brief, in which a few questions were asked yet usable data was received (see Schwalbe and Wolkomir, 2003). This data was simply recorded in notebooks because the use of a tape-recorder was, on most occasions, impractical.

Findings

a. Marketing tactics

Online Pharmacies

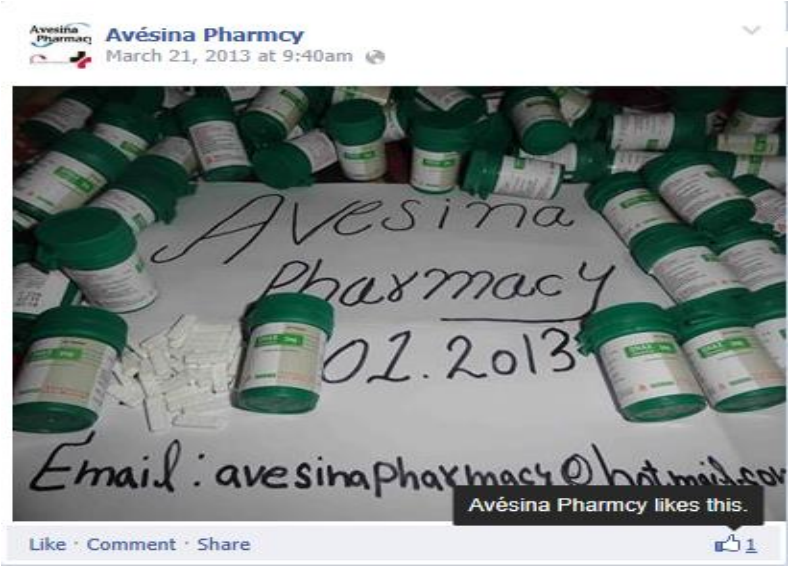
The primary site for medicine supply online is *Online Pharmacies* (OPs). OPs are pharmacies that operate over the Internet and post their products to consumers via a shipping company or the postal service. There are various types of online pharmacies and, with the global and detached nature in which they operate, the distinction between legitimate and illegitimate operations can often become blurred. Outside legitimate online pharmacies a range of illegitimate pharmacies are in operation. Legitimate online pharmacies include well-known pharmacy chains' online subsidiaries and independent pharmacies' online sites set up to simplify the ordering process and compete with larger companies. However, there are huge numbers of illegitimate OPs in operation. In order to identify illicit providers a number of common indicators can illustrate whether online sites are acting illegally. Most offer what should be prescription only (PO) medicines without a prescription, whereas others offer forged online prescription services which simply ask the customer to 'virtually discuss' their supposed health concerns with someone posing as an online doctor. Other obvious ways to tell if an OP is acting illegitimately is the concealment of their physical address and the webpage's connection to a non-compliant registrar. To project the appropriate image and enhance credibility illegal entrepreneurs pay particular attention to the design of the website, providing scientific information on the issue, accompanied by photographs of health professionals. In addition, these websites are embellished with extremely detailed *Frequently Asked Questions* (FQA) sections as another indication of reliability. In 2008 the UK introduced the green cross logo in order to offer legitimacy and to help UK consumers identify authentic online pharmacies. However, some rogue pharmacies have attempted to plagiarise the logo on their sites.

Use of Social Media Sites

The virtual ethnographic research revealed numerous examples of social media sites, particularly Facebook, acting as online sites for supply of illicit medicines. Connections between seller and buyer were forged via friends' lists and Facebook groups affiliated to prescription drugs, or linked to subcultures wherein prescription drug use is prevalent and normalised. 'Friends' tended to post stock available directly on their wall or on the page of a group, often with photographic evidence of the product alongside their personal or business name, their contact details and the date (see figure 1). Virtual 'word of mouth' plays an important role in terms of

establishing, assuring and circulating the legitimacy of a seller and quality of the service on offer, especially as users are concerned about becoming victims of 'scams' and subsequently being defrauded. Some actors used a variety of social networking sites to advertise their products. For example, we also found evidence of opioids and erectile dysfunction drugs for sale via sellers posting on sites such as Instagram and Twitter.

Figure 1.
Stock posted to the page of a Facebook group, March 2013.



Source: authors' research

Participatory web cultures and social media sites allow for a process of 'prosumption' (Toffler, 1980) in 'fake' pharmaceutical trading, where often there is no clear demarcation between the producer, trader and consumer involved in marketing and advertising processes. This, we are quite convinced, is further evidence of a cultural shift in consumption − and business relations − more generally and suggests that the online market in 'fake' pharmaceuticals is an important example of this shift. Moreover, entrepreneurs use a variety of online sites/avenues (email, Facebook, OPs) interchangeably to market their products, usually bought in bulk from distributors. For example, initial links made between buyers and sellers on social media sites can direct buyers to OPs and/or lead to more detailed email conversations about the products. This also explains why particular sellers offer free samples or added extras in order to market specific products they have in stock and need to sell. Other actors using social media are small scale amateur sellers, sometimes also users/consumers of prescription drugs, a procedure that seems to mimic the 'real' street-level dealers involved in illicit drug distribution.

Online Wholesalers and Classified Advertising

We found two specific online marketplaces based in Asia selling large quantities of pharmaceutical chemicals, materials, equipment or finished medicinal products to distributors and consumers. These products are attempting to bypass IP laws and are therefore deemed as 'fake'. These sites offer B2B and direct B2C platforms for trade in 'fake' medicines. *Alibaba* is one of the largest e-commerce markets in the world, so big that in 2012 the site processed the selling of more goods than Amazon and eBay combined (The Economist, 2013). However, it is also rife with counterfeit products. We found large quantities of powdered APIs (Active Pharmaceutical Ingredients) under their generic names. For example, Zopiclone, a non-benzodiazepine, a patented product with Sanofi Aventis for sale in the UK, being sold in powdered form in 25 kilo quantities direct from a chemical company based in mainland China. Moreover, the equipment needed to press pills at home was also for sale on the site.

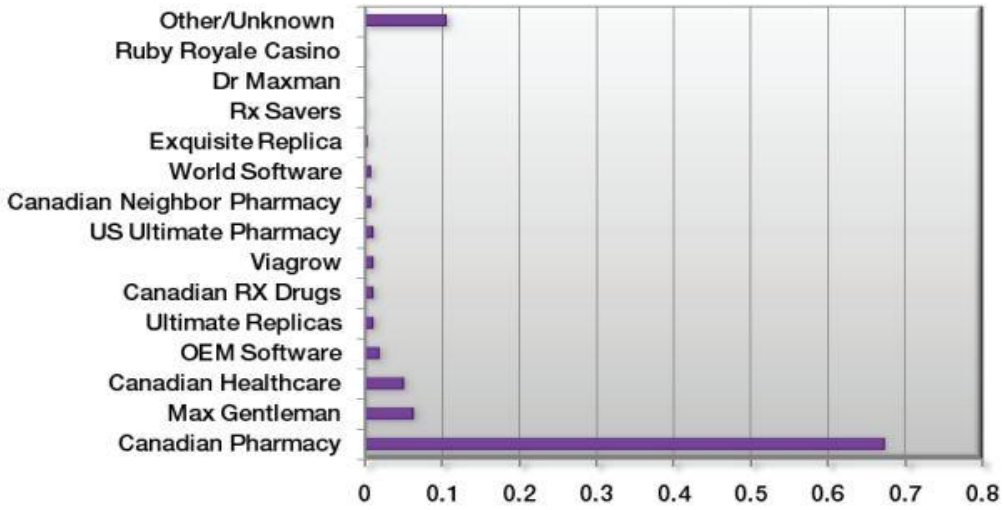
TradeIndia, an online Indian based B2B portal, was another large online marketplace illegitimately offering direct sales of pharmaceutical products under patent in the UK. We found direct evidence of a seller on Facebook who was supplied by a TradeIndia seller. In this case the ingredients/chemicals and pressing and packaging were being supplied to small clandestine operations based in the UK. Furthermore, we found classified advertising via such sites as *Craigslist* being used to sell smaller quantities of 'fake' medicines. We found Oxycontin, Ritalin and Percocet among others for sale, mainly in the 'Health and Beauty' section. Further still, a variety of sites posing as UK-based online pharmaceutical wholesalers offered 'special products', which suggests that goods and services lying at the margins of legitimacy are being advertised. This may feed the 'new breed of retail drug dealer' sourcing their stock – in this case prescription drugs - online (see Aldridge and Décary-Hétu, 2014).

'Pandora's (in)box': E-mail and spam

Another way illegal pharmacies promote their business and merchandise online is through the use of spam e-mails. One of the most prolific counterfeit medicine traders online known to the authorities is the Russian-based GlavMed. They run their online pharmacy operation alongside their large spam company SpamIt. According to M86 Security Labs, the sites advertised in Glavmed/Spamit emails − best known by their "Canadian Pharmacy" brand name− were by far the most prevalent affiliate brands promoted by spam as of June 2010 (Krebs on Security, 2011) (see figure 2). In addition, after researching 218 drug related queries over nine months in 2010-2011, cybersecurity researchers at Carnegie Mellon Universi-

ty found that illegal pharmacies use spam e-mails to manipulate web search results and promote their business (Medical Daily, 2011).

Figure 2.
Affiliate brands promoted by spam, June 2010



Source: Kerbs on Security (2011)

The practice of using spam e-mails has been used − primarily by illegal entrepreneurs with the highest IT 'literacy' − in conjunction with another practice: web manipulation. Web manipulation has been viewed as much more efficient a method than spam e-mails. As the lead researcher of the project at Carnegie Mellon University noted, ". . . unauthorised online pharmacies have been using e-mail spam to tap the wallets of unwary online consumers but that method did not blanket enough customers so now [the illegal entrepreneurs] are infecting websites to redirect unwary consumers to hundreds of illegal online pharmacies" (Science Daily, 2011). Specifically, they found that one-third of their collected search results during the study − 7000 infected websites − triggered an active redirect to a few hundred illegal online pharmacies sites. Affiliate and sub-affiliate networks often play a crucial role in this process, which we will return to below in our discussion of detection avoidance tactics.

Forums

There is an abundance of marketing research suggesting that consumers are heavily influenced by internet-based forums before they make purchasing decisions (Dellarocas, 2006). Therefore, entrepreneurs exploit discussions in these forums in the knowledge that potential customers tend to be more interested in a product if it is

perceived as 'authentically' endorsed, rather than a product purposefully promoted by marketer-generated sources (Bickart and Schindler, 2001). In a similar vein, online forums have been identified as critical and strategic discussion platforms allowing for what Woerndl *et al.* (2008) call 'viral marketing': transmitting messages and information about products quickly to a much wider audience. This can be manipulated by criminals involved in the trade who pose as consumers, or more directly via the use of affiliates (see discussion below). It also confirms a point we made earlier that production and consumption are involved in a process of co-creation in the context of participatory web cultures and pharmaceutical trading. Virtual specialised forums are not only spaces in which illegal entrepreneurs identify (and persuade) potential customers to purchase medicines for medical conditions that concern them, but also in which customers often collectively discuss their pharmaceutical consumption online without such persuasion. Moreover, forums have also emerged in the form of what Soudijn and Zegers (2012) call 'convergence setting' for criminals; locations in which potential collaborators may meet one another. Hence, internet-based forums – in an increasingly normalised process of time/space compression – provide large numbers of consumers in dispersed locations *and* offer the formation of transient relationships between (cyber)criminal entrepreneurs.

The Deep Web

There has been a lot of discussion in the UK media regarding the SilkRoad, an unregulated US-based online marketplace recently seized by the FBI. This is only one example of operations on the so-called 'deep web', which enforcement agencies suspect might proliferate over time. Designed for online anonymity, Tor, or The Onion Router, offers layered encryption to buyers and sellers. It is a network designed to pass IP addresses and carry out web transactions through numerous relays, using random and anonymised URLs in order to conceal users' locations and internet activities. Once Tor is accessed a buyer and seller trade in digital currencies, such as Bitcoin, and use data encryption and decryption tools, for example PGP encryption (Pretty Good Privacy), to encrypt and decrypt messages. This has provided distributors of drugs a relatively anonymous and unregulated online marketplace. Our research has found numerous sellers of prescription-only medicines, steroids and other illicit drugs on the deep web across various sites. Clearly, a variety of online sites and avenues are implicated in the online trade in 'fake' medicines. However, along with the online sites of supply, a variety of other channels and networks have emerged and developed, through which the trade is put into practice, reiterating the importance of a discussion of both the virtual and physical elements of the trade and their interconnections, which we will turn to now.

Marketing of online business on physical locations

Entrepreneurs also promote their online businesses offline, during pharmaceutical conventions and other relevant events and venues. For example, during our offline ethnography we came across an illegal entrepreneur, 'Pete', a nutritionist by training, who attended the gym in Northeast England. With his cousin, who is based in India, 'Pete' owns an illegal pharmacy that sells steroids and a variety of other pharmaceutical products to UK and European-based customers. 'Pete' also promotes the use and purchase of anabolic steroids in the gym, among individuals who are attempting to 'bulk up', and especially among those who have been having difficulty in doing so. He also promotes his illegal business during local and national bodybuilding, power-lifting and mixed martial arts events. His professional background as a nutritionist not only allows him to offer detailed advice on nutritional matters, but also partly legitimises his illegal business in the gym. 'Pete' is regularly 'taxed' on his profit by the owner of the gym in return for the opportunity to market his business on the premises.

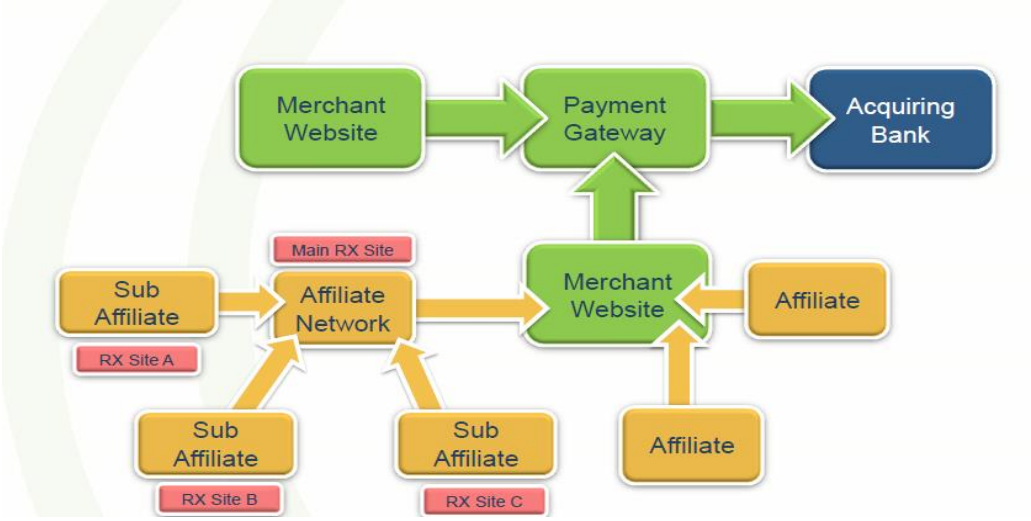
Asking for personal details from customers

Finally, entrepreneurs selling 'fake' medicines online market their merchandise by asking for a phone number when collecting billing information from customers making initial orders. The collected numbers are then used to contact customers for *repeat* business. In order to secure a customer's number, the entrepreneurs make the provision of a telephone number compulsory if an online transaction is to be completed. Although an initial connection is made online, future sales can then be made over the telephone without any online interaction.

b. Detection avoidance tactics

As mentioned earlier, apart from tactics used to promote their business and merchandise, illegal entrepreneurs use a number of techniques to avoid law enforcement and health regulatory agencies' efforts to close them down and bring them before the courts. Firstly, the tactics involve the use of affiliate and sub-affiliate networks to 'muddy the waters' (see figure 3).

Figure 3.
Payment gateways in the online trade of counterfeit medicines



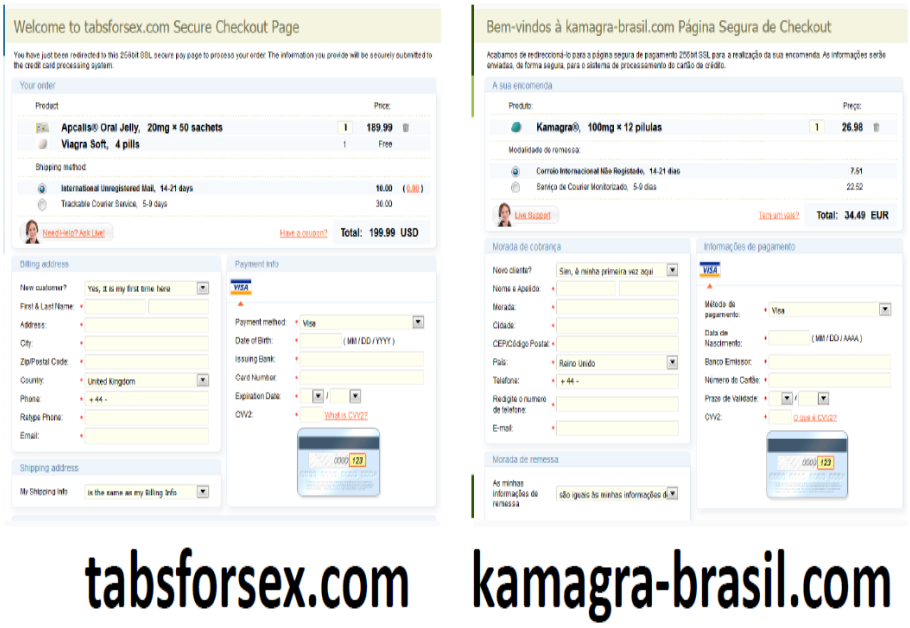
Source: Groves (2014)

An afflilate network is constructed in two ways: 1. By entrepreneurs who are responsible for a number of websites illegally trading in medicines; often the websites have a very similar if not identical template (see figure 4); 2. By the use of 'affiliates', whereby larger 'organisations' operating OPs pay commercial entities commission to surf the web and 'set up clone pages mimicking the website of the "spider" and/or merely post a URL link' on their site to the pharmacy. In other words, individuals or affiliate programs run by individuals post links to OPs on various online sites and are paid for each 'customer who has 'clicked through' the affiliate's link' (DeKeiffer, 2005: 9). Therefore, alongside muddying the waters, these networks provide a crucial marketing function.

Firstly, it is very interesting to note the case of 'Glavmed' mentioned earlier. This particular criminal enterprise owned and operated 2026 domain names (although all of these names used similar website templates), provided by 36 different registrars, leading to only 12 payment gateways or pages. Similarly, the Pangea IV operation identified 1412 illegal online pharmacies, 928 of which led to payment pages. Of those, 649 websites (or approximately 70%) were connected to only 4 payment pages (see Anaman, 2014). These examples emphasise the presence of large-scale, concentrated, schemes involved in the online trade of 'fake' medicines.

Figure 4

Illegal online pharmacies belonging to an affiliate network



Source: figure provided by the UK Medicines and Healthcare products Regulatory Agency (MHRA)

Secondly, illegal entrepreneurs buy their domains from 'rogue registrars', such as *TodayNIC; BizCN; WebNIC.cc.; Joker.com; IPMirror, etc.* These non-compliant registrars tend to ignore law enforcement and regulatory agencies' requests to block and shut down specific sites deemed to be associated with the illegal sale of medicines.

Thirdly, illegal entrepreneurs engage in something similar to counterintelligence. They attempt to identify unusual patterns of 'behaviour' on the part of law enforcement and health regulatory agents posing as customers. Specifically, they check the details of visitors to their affiliate sites, including the frequency of visits and the debit/credit card used for purchases. If a visitor is found to be making a number of visits to a number of their affiliate sites, as well as using the same card for payment, this is an indication of a law enforcement officer or health regulatory agent monitoring the website and/or conducting test purchases. If the illegal entrepreneurs identify such 'unusual' behaviour from the 'fingerprint' (IP address), the 'potential client' is blocked or re-directed to another website (for example, back to Google or to a site unrelated to the pharmaceutical industry).

Fourthly, illegal entrepreneurs actively attempt to avoid the WHOIS check that is performed by law enforcement authorities and regulatory agencies in order to identify illegal online pharmacies. WHOIS checks the following: 1. the company acting as the 'registrar'; 2. the registrant of the domain name (basically the compa-

ny or individual who has bought the domain name); 3. the registration date; 4. IP address; 5. the company address. Law enforcement and health regulatory agents use WHOIS services provided by websites such as *www.domaintools.com*. According to the Permanent Forum on International Pharmaceutical Crime (PFIPC) (2014), it can be extremely difficult to track the ultimate source of a website, as many of the major illegal pharmacies use 'fast flux' in order to hide their physical location:

> "The simplest type of 'fast flux', referred to as 'single-flux', is characterised by multiple individual nodes within the network registering and de-registering their addresses for a single DNS (Domain Name System) name. This creates a constantly changing list of destination addresses for that single DNS name – perhaps as often as every three minutes. The list can be hundreds or thousands of entries long" (PFIPC, 2014: 14).

Fifthly, criminal entrepreneurs re-route payments through intermediaries and thus obfuscate the relationships existing between illegal activities and payments (see Burke, 2014). Law enforcement and health regulatory agencies consider 'following the money' as a reliable way of identifying illegal entrepreneurs involved in the illicit pharmaceutical trade. Indeed, 'following the money' is regarded as a way of counterbalancing the limitations of other aspects of the criminal investigation and a way of targeting the most important actors involved in a pharmaceutical crime network. However, illegal entrepreneurs largely avoid asking for bank payments because, on occasion, according to MHRA agents, the name of the beneficiary can be obtained from the transaction's paper trail. Instead, entrepreneurs prefer money transfer services (such as Western Union) because they are extremely easy to conduct, and – for smaller transactions – no identification is required. In addition, illegal entrepreneurs forge multiple banking relationships in numerous ways. They have been known to ask family members, friends and/or acquaintances to borrow their accounts for a number of transactions, or have rented the accounts of others for a short time.

Finally, illegal entrepreneurs generally avoid providing any personal information and details on delivery items accompanying the merchandise they send (such as delivery notes, invoices, leaflets etc.). Some unsuccessful or not so diligent illicit entrepreneurs use telephone numbers, which is quite a crucial piece of information for the investigative authorities. During our research, authorities showed us one delivery note sent with a batch of counterfeit Viagra that included the following message: *"Thank you for your purchase. For more information call XXXX 393348"*. As a result, the investigative team at the MHRA managed to trace a major, but not very intelligent, actor in an illegal online pharmacy operation distributing their merchandise in the UK.

Conclusion and discussion

The 'fake' medicine trade is a growing and under-researched global phenomenon encompassing instances of counterfeit, substandard, unlicensed and illegally supplied pharmaceutical products. Based on data gathered as part of a broader ongoing study investigating the online trade in 'fake' medicines, this chapter has outlined a range of tactics adopted by illegal entrepreneurs involved in the trade. Specifically, the chapter focused on two distinct, although not entirely separate, aspects of our findings relating to the tactics and methods used. On the one hand, it offered an insight into how 'fake' medicines are marketed online. On the other hand, it highlighted how the entrepreneurs involved in the trade avoid detection by the authorities. As the chapter has shown, in terms of marketing techniques, online suppliers of 'fake' medicines use a range of sites − often simultaneously − to target their market and circulate the value of their products to consumers. These include online pharmacies, social media sites, online wholesalers, classified advertising, email and spam, online forums, and cryptomarkets found on the deep web; as well as on physical locations and via telephone marketing.

We have also found that affiliate and sub-affiliate networks can play a crucial role in marketing 'fake' medicines online (by providing greater market reach) *and* in attempts to avoid detection (by obscuring individual market operations). Furthermore, cyber-criminal entrepreneurs supplying 'fake' medicines use a range of other common detection avoidance practices. As discussed, they choose non-compliant registrars to access domain names, monitor the behaviour of visitors to their sites, circumvent the WHOIS protocol, re-route payments, and avoid paper trails.

Although this chapter is empirical in its scope, our investigation into the online tactics illegal entrepreneurs employ in order to trade in 'fake' medicines online allows us to make a number of observations. For the most part these observations relate to the ongoing debate surrounding whether modern ICTs have facilitated old or produced new forms of criminal activity. This specific illegal market can, therefore, be characterised by a tension between *logic consequence* (the view that professional or 'organised' criminals become involved in cyber-crime at any given opportunity) and *pragmatism* (the view that questions the need and/or ability of 'organised' criminals to exploit the virtual world) (McCusker, 2006; see also Levi, 2001; Savona and Mignone, 2004; Holt and Copes, 2010).

First of all, while computer crime has been identified as the 'new' threat or the 'new' frontier for law enforcement, policy makers, the media and an increasingly large number of academics, in reality the online trade in illicit medicines is largely based upon a set of established criminal acts: intellectual property crime (in the case of counterfeit medicines infringing IP laws) and fraud. McQuade (2011)

would define these criminal activities as *adaptive* in the sense that they constitute technological variations of ordinary crimes. Similarly, as Naylor (2000: 3) very characteristically puts it:

> "It is important to distinguish new crime from new methods. To take one common case, frequently "computer crime" is singled out as a prime new area of concern. But it really boils down to a series of traditional criminal acts . . . that happen today to be assisted by the use of computers. The crimes remain the same. The only difference is the technique used to commit them, and the ability to do them from much further away than was commonly the case" (see also Grabosky, 2001).

However, what our research on the illegal e-trade of medicines highlights is that although the Internet might enable the "distancing of offenders from their illegal goods and services" (Levi and Naylor, 2000: 10; see also Filipkowski, 2004), it can also increase the authorities' ability to detect the offences and offenders (see, for example, Coscia and Rios, 2012; Moore, 2007).

Moreover, this particular market emphasises that the illicit traders involved in marketing and supplying medicines online "resemble many professional criminals in their 'adaptive pragmatic organisation'" (Shover *et al*., 2003: 501). These professional criminals continue to evolve while responding to 'shifting terrains' (Hobbs, 2001), including new and frequently mutating technologies (see Levi, 2002; Bequai, 2001) and strategies in law enforcement and security (von Lampe, 2005). These "[e]conomic and social changes inevitably transform the worlds in which these professional criminals entertain options and organise for pursuit of criminal income" (Shover *et al*., 2003; see also Hobbs, 1995; 1997; 2013; Hall, 2012). Indeed, the rise of the Internet is one factor working in conjunction with the non-digital dimension in a dynamic way, along with a variety of social, cultural, political and economic processes, to enable production and consumption of 'fake' medicines. The relationship existing between these economic and social changes, legal economies and illegal markets, online and offline 'worlds', is flexible and complex, and is manifested in the surrounding entrepreneurial landscapes and their elements (van Duyne, 2005; Antonopoulos and Papanicolaou, 2014). In Bauman's (1992) words, "[the] entrepreneurial ethic that underpins both legal and illegal performances thrives upon new technical, social, psychological and existential skills" (Bauman, 1992), which in turn are bordered by new configurations of cultural and technological capital" (Shover *et al*., 2003: 502; see also Treadwell, 2011).

Our findings, however, highlight another key issue that merits attention, given the hype that accompanies internet-related crime. Ongoing legal and criminological research on cyber-crime is primarily concerned with *diffusion* and the ever increasing criminal opportunities offered by the Internet (Hayward, 2012: 139). One would assume, therefore, that the Internet would allow many more criminal entre-

preneurs to become involved in the process of illegally selling medicines online. Yet our study shows that various perpetrator roles may be found. It shows that the business is highly concentrated among a smaller number of individuals and groups operating on a wider scale, some of whom have a fair amount of IT knowledge and skill, or a team to which IT services can be contracted out. However, this finding may be problematic because it is the product of investigations by the authorities focusing on specific known illegal pharmacies. Therefore, it may neglect small-scale actors who are involved in the illegal online trade of medicines (such as those we found during our ethnographic research). Overall, we have found that the actors involved in the online trade of 'fake' medicines and their operations exist on varied yet simultaneous scales; some are larger criminal organisations with pockets of concentrated power and reach (*e.g.* Glavmed) while others are small-scale nationally or locally based groups or individuals. This indicates that the market's social composition does not change as a result of digitisation, and similar subjective desires and demands emerge.

Finally, despite the 'transnationality' of this illegal market – in as much as it encompasses a multiplicity of interactions and linkages of individuals and institutions across the borders of nation states – it also has *national* and *local* manifestations. Our research has shown that the illegal online sale of medicines is illustrative of the "counter-geographies of globalisation" (Sassen, 1998): the dynamic and fluid networks that are – to a considerable extent – part of the informal economy, but also use sectors of the *legal* economy's 'infrastructure' and support across various spatial scales. These networks are intertwined with the foremost dynamics constitutive of globalisation, such as the 'formation of global markets' and the establishment and intensification of 'transnational and trans-local networks', but these are coupled with a diversity of everyday grounded and localised economies (both legal and illicit) and occupational cultures in which the overall process of globalisation is embedded (Sassen, 1998; see also Hobbs, 1998).

References

Aldridge, J., and D. Décary-Hétu, "Not an 'Ebay for drugs": The cryptomarket "Silk Road" as a paradigm shifting criminal innovation". *Social Science Research Network,* 2014, available online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436643

Anaman, P., 'Mapping out organised crime networks, patterns and trends'. Presentation at INTERPOL, Lyon, France, March 14, 2014

Antonopoulos, G.A. and G. Papanicolaou, *Unlicensed capitalism, Greek style: Illegal markets and 'organised crime' in Greece.* Nijmegen: Wolf Legal Publishers, 2014

Bauman, Z., *Intimations of postmodernity*. London: Routledge, 1992

Bequai, A., 'Organised crime goes cyber', *Computers & Security*, 2001*, vol. 20*, 475-478

Bickart, B. and R.M. Schindler, 'Internet forums as influential sources of consumer information'. *Journal of Interactive Marketing,* 2001, *vol.15(3),* 31-40

Burke, D., 'Pangea choke points: Website takedowns and following the money'. Presentation at INTEPOL, Lyon, France, March 13, 2014

Castells, M., *The internet galaxy: Reflections on the internet, business and society.* Oxford: Oxford University Press, 2001

Chan, S. P., 'Viagra maker Pfizer faces competition from generic rivals as patent expires', *The Telegraph,* December 3, 2013 available online at: http://www.telegraph.co.uk/finance/newsbysector/pharmaceuticalsandchemicals/10095251/Viagra-maker-Pfizer-faces-competition-from-generic-rivals-as-patent-expires.html

Coscia, M. and V. Rios, *Where do criminals operate? Using Google to track mexican drug trafficking organisations.* Harvard University, 2012, available online at: http://www.gov.harvard.edu/files/CosciaRios_GoogleForCriminals.pdf

Davey, Z., F. Schifano, O. Corazza and P. Deluca, 'e-Psychonauts: Conducting research in online drug forum communities'. *Journal of Mental Health*, 2012, *vol.21*, 386–394

deKieffer, D.E., 'The internet and the globalization of counterfeit drugs'. *Journal of Pharmacy Practice*, 2006, *vol.19*, 171–177

Dellarocas, C., 'Strategic manipulation of internet opinion forums: Implications for consumers and firms'. *Management science,* 2006, *vol.52(10)*, 1577-1593

Fielding, N., R.M. Lee and G. Blank (eds.), *Online research methods*. London: Sage, 2008

Filipkowski, W., 'Internet as an illegal market place'. Paper presented at the 6th Cross-border crime colloquium, Berlin, Germany, October, 2004

Fox, N.J., K.J. Ward and A. O'Rourke, 'The 'expert patient': Empowerment or medical dominance? The case of weight loss and the internet'. *Social science and medicine*, 2005, *vol.60(6)*, 1299-1309

Geertz, C., *The interpretation of cultures.* New York: Basic Books, 1973

Grabosky, P., 'Crime in cyberspace'. In P. Williams and D. Vlassis (eds.), *Combating transnational crime: Concepts, activities and responses.* (pp.195-208) London: Routledge, 2001

Groves, K., 'Payment systems and illegal online pharmacies'. Presentation at INTERPOL, Lyon, France, March 13, 2014

Guarnieri, F. and E. Przyswa, 'Counterfeiting and cybercrime: Stakes and challenges'. *The Information Society*, 2013, *vol.29(4)*, 219-266

Hall, S., *Theorising crime and deviance.* London: Sage, 2012

Hayward, K., 'Using cultural geography to think critically about space and crime'. In S. Hall and S. Winlow (eds.) *New directions in criminological theory.* (pp.123-144). London: Routledge, 2012

Hine, C., *Virtual ethnography*. London: Sage, 2000

Hobbs, D., *Bad business.* Oxford: OUP, 1995

Hobbs, D., 'Professional crime: Change, continuity and the enduring myth of the underworld'. *Sociology,* 1997, *vol.31*, 57-72

Hobbs, D., 'Going down the glocal: The local context of organised crime'. *Howard Journal of Criminal Justice,* 1998, *vol.37(4)*, 407-422

Hobbs, D., 'The firm: Organisational logic and criminal culture in a shifting terrain', *British journal of criminology,* 2001, *vol.41*, 549-560

Hobbs, D., *Lush life*. Oxford: OUP, 2013

Holt, T.J. and Copes, H., 'Transferring subcultural knowledge online', *Deviant behaviour,* 2010, *vol.31*, 625-654

IRACM, *Counterfeit medicines and criminal organisations*. Paris: IRACM, 2013

Kean, J., *Anabolic steroids*. Unpublished MSc criminology dissertation, Middlesbrough: Teesside University, 2012

KPMG, *An overview of risk and disclosure in the global pharmaceutical and life sciences industry.* London: KPMG, 2012

Krebs on Security, 'SpamIt, Glavmed pharmacy networks exposed'. *KrebsOnSecurity,* February, 2011, available online at: https://krebsonsecurity.com/2011/02/spamit-glavmed-pharmacy-networks-exposed/

Levi, M., 'Between the risk and the reality falls the shadow: Evidence and urban legends in computer fraud'. In D. Wall (ed.), *Crime and the internet.* (pp.44-58) Abingdon: Routledge, 2001

Levi, M., 'Breaking the economic power of organised crime groups'. Paper presented at the CIROC (Centre for information and research on organised crime) seminar, Amsterdam, The Netherlands, October 16, 2002

Levi, M. and R.T. Naylor, 'Organised crime, the organisation of crime, and the organisation of business'. DTI crime foresight panel essay, 2000, available online at: http://www.cf.ac.uk/socsi/resources/levi-orgcrime.pdf

McCusker, R., 'Transnational organised cyber-crime: Distinguishing threat from reality'. *Crime, Law & Social Change,* 2006, *vol.46*, 257-273

McQuade, S., 'Technology-enabled crime, policing and security'. *The Journal of Technology Studies,* 2011, *vol.32(1),* 1-9

Medical Daily, 'Illegal online pharmacies exploiting the web'. *Medical Daily,* August 17, 2011

Moore, R., 'The role of computer forensics in criminal investigations'. In Y. Jewkes (ed.), *Crime online.* (pp.81-94) Cullompton: Willan, 2007

Naylor, R.T., *Economic and organised crime: Challenges for criminal justice.* Ottawa: Research and statistics division, 2000

Permanent Forum on International Pharmaceutical Crime (PFIPC), *Investigators' guide for the conduct of internet investigations concerning illegal internet pharmacies*. Unpublished investigators' guide, 2014

Sassen, S., *A sociology of globalisation*. New York: W.W. Norton, 2007

Sassen, S., *Globalisation and its discontents: Essays on the new mobility of people and money.* New York: The New Press, 1998

Savona, E.U. and M. Mignone, 'The fox and the hunter: How ICT changes the crime race'. *European Journal on Criminal Policy and Research,* 2004, *vol.10*, 3-26

Schwalbe, M.L. and M. Wolkomir, 'Interviewing men'. In J.A. Holstein and J.F. Gubrium J.F. *Inside interviewing: New lenses, new concerns*. (pp.55-71) Sage: Thousand Oaks, Ca., 2003

Science Daily, 'Tracking illegal online pharmacies: Evidence of web manipulation'. *Science Daily*, August 12, 2011

Shover, N., G.S. Coffey and D. Hobbs, 'Crime on the line: Telemarketing and the changing nature of professional crime'. *British Journal of Criminology,* 2003, *vol.43*, 489-505

Soudijn, M.R.J. and B.C.H. Zegers, 'Cyber-crime and virtual offender convergence'. *Trends in Organised Crime,* 2012, *vol.15(2/3),* 111-129

The Economist, 'Alibaba: The world's greatest bazaar', *The Economist,* November 3, 2013 available online at: http://www.economist.com/news/briefing/21573980-alibaba-trailblazing-chinese-internet-giant-will-soon-go-public-worlds-greatest-bazaar

Toffler, A., *The third wave*. New York: William Morrow & Co., 1980

Treadwell, J., 'From the car boot to booting it up? eBay, online counterfeit crime, and the transformation of the criminal marketplace'. *Criminology & Criminal Justice,* 2011, *vol.12(2),* 175-191

van Duyne, P.C., 'Crime and commercial activity: An introduction to two half-brothers'. In P.C. van Duyne, K. von Lampe, M. van Dijck and J.L. Newell (eds.), *The organised crime economy: Managing crime markets in Europe.* (pp.1-18) Nijmegen: Wolf Legal Publishers, 2005

von Lampe, K., 'Making the second step before the first: Assessing organised crime - The case of Germany'. *Crime, Law and Social Change,* 2005, *vol.42(4&5),* 227-259

Walker, T., 'FedEx facing drug-trafficking charges over illicit pharmaceuticals'. *The Independent*, July 20, 2014, available online at:

http://www.independent.co.uk/news/business/news/fedex-facing-drugtrafficking-charges-over-illicit-pharmaceuticals-9616936.html

Ward, K.J., 'The cyber-ethnographic (re)construction of two feminist online communities'. *Sociological Research Online*, 1999, *vol.4(1)*

Wertheimer, A.I. and P.G. Wang, (eds.), *Counterfeit medicines volume I: Policy, economics and countermeasures*. Hertfordshire: ILM, 2012

Webber, C. and M. Yip, 'Drifting on and off-line: Humanising the cybercriminal'. In Winlow, S. and R. Atkinson (eds.) *New directions in crime and deviancy.* (pp.191-205) London: Routledge, 2013

Wittel, A., 'Ethnography on the move: From field to net to internet', *Qualitative Social Research,* 2000, *vol.1(1)*, available online at: http://www.qualitative-research.net/index.php/fqs/article/view/1131/2517

Woerndl, M., S. Papagiannidis, M. Bourlakis and F. Li, 'Internet-induced marketing techniques: Critical factors in viral marketing campaigns'. *International Journal of Business Science and Applied Management,* 2008, *vol.3(1),* 33-45

World Health Organisation (WHO), *Substandard/spurious/falsely labelled/falsified/counterfeit medical products: Report of the working group of member states*. Geneva: WHO, 2012

Yar, M., 'A deadly faith in fakes: Trademark theft and the global trade in counterfeit automotive components', *The Internet Journal of Criminology*, 2005, available online at: http://www.internetjournalofcriminology.com/Yar%20-%20A%20Deadly%20Faith%20in%20Fakes.pdf

Yar, M., *Cybercrime and society*. London: Sage, 2006

Yar, M., 'The *other* global drugs crisis: Assessing the scope, impacts and drivers of the trade in dangerous counterfeit pharmaceuticals'. *International Journal of Social Inquiry,* 2008, *vol.1(1),* 151-166

Yar, M., 'Sociological and criminological theories in the information era'. In W. Stol and R. Leukfeldt (eds.), *Cyber-safety.* Utrecht: Eleven international publishing, 2012