JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 1(1), 2015, 81–92
doi: 10.1093/cybsec/tyv006
Advance Access Publication Date: 10 November 2015
Research Article

Research Article

Scripting the crime commission process in the illicit online prescription drug trade

Nektarios Leontiadis[1] and Alice Hutchings[2,*]

[1]CyLab, Carnegie Mellon University, Pittsburgh, PA 15213, USA and [2]Computer Laboratory, University of Cambridge, Cambridge CB3 0FD, UK

*Corresponding author. Computer Laboratory, 15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom. Tel: +44 (0)1223 763660; Fax: +44 (0)1223 334678; E-mail: alice.hutchings@cl.cam.ac.uk

Received 18 June 2015; revised 20 September 2015; accepted 28 September 2015

Abstract

This article considers the processes in the illicit online prescription drug trade, namely search-redirection attacks and the operation of unlicensed pharmacies using crime script analysis. Empirical data have been used to describe the salient elements of the online criminal infrastructures and associated monetization paths enabling criminal profitability. This analysis reveals the existence of structural chokepoints: components of online criminal operations being limited in number, and critical for the operations' profitability. Consequently, interventions targeting such components can reduce the opportunities and incentives to engage in online crime through an increase in criminal operational costs, and in the risk of apprehension.

Key words: online prescription drug trade; illicit online pharmacies; search-redirection attacks; crime script analysis; situational crime prevention.

Introduction

In this article, we examine two key processes of the illicit online prescription trade that allow this trade to be profitable [1], through crime script analysis (CSA) [2]. CSA involves outlining the consequential steps and actions undertaken in order to prepare for, undertake, and complete a certain offence or offence type. Scripts represent knowledge structures that allow for the organization of thoughts or understanding of events or social interactions, including crime [3]. We then use the derived crime script to identify appropriate situational crime prevention countermeasures that could be capable of disrupting the illicit online activity. The two processes we examine are: (i) one of the abusive advertising vectors widely employed in the trade for many years called search-redirection attack [1]; and (ii) the operation of illicit online pharmacies [web stores that focus primarily on the trade of drugs without necessarily abiding to the legal requirements (e.g. licensing, requirement for prescriptions) of operating such store in the countries of their customers].

While our rationale for examining the illicit online pharmacies through CSA is rather straightforward given their role in monetizing this illicit activity, the decision to focus on the specific advertising vector—the search-redirection attack—is based on its extent and impact [4]. This type of attack allows certain visitors to compromised websites (which are under the control of an adversary with or without the knowledge of the legitimate owner)—those who come to such websites after searching for certain keywords—to be redirected to online stores selling pharmaceutical drugs without a prescription. All other visitors, including the compromised websites' owners, see only the original sites. Consequently, such compromises have been proven to be long-lived [1], and add to the confusion related to the legitimacy of online pharmacies [5].

Our work is predominantly focused on the criminal activity associated with the illicit online prescription drug trade due to its societal impact. By enabling access to prescription drugs without a valid prescription and without proper health assessment by a medical doctor, consumers are essentially allowed to self-medicate. This practice is a dangerous one as it can lead to severe health issues [6]. However, the aspect of appropriate deterrents—which is a necessary aspect of a discussion on remediation—is equally interesting and important. Looking at the drug trafficking problem primarily from the US legal perspective—both online and offline—laws and statutes are rather adequate to persecute and punish offenders [7]. However, laws are limited in their ability to cover the international aspects of the online prescription drug trade, and the coordinated efforts to

police these markets are not temporally persistent and consistent [8]. Consequently, it is highly uncertain whether an offender will be punished for illicitly trading prescription drugs online. The inadequacy in enforcing existing laws on the Internet questions the certainty of punishment, invalidating a fundamental assumption of general deterrence. Indeed, according to Beccaria, the certainty of being punished when committing a crime is a necessary condition to prevent other from committing similar activities [9].

Our approach toward addressing this inadequacy in this work is straightforward. We use CSA to identify the structural chokepoints in the trade of illicit prescription drugs, outlining a holistic approach toward disrupting this illicit online market. The structural chokepoints are those parts of the script that are critical for the operation of the illicit enterprise. By applying intervention measures at structural chokepoints, we argue it is plausible to increase the effectiveness of the disruption method.

Impact of online pharmacies on public health

The operation of unlicensed pharmacies is not just a legal or regulatory issue, but also leads to social and public health problems. Independent testing has revealed that the drugs sold through these pharmacies often include the active ingredient, but often in incorrect and potentially dangerous dosages [10, 11]. Henney *et al*. [6] and Henney [12] show that, despite the convenience provided by online pharmacies (e.g. 24-h availability), they often do not follow due diligence in issuing prescriptions, or they forfeit this requirement altogether. Moreover, by providing access to unapproved drugs, unlicensed online pharmacies put the health of their customers at risk. Bessell *et al*. [13, 14] studied the pharmacological information of prescription and over-the-counter drugs advertised at internationally based online pharmacies. They found that the information was usually inappropriate, insufficient, or nonexistent, making the use of those products unsafe. A systematic review by Orizio *et al*. [15] similarly found a lack of or inappropriate information and labeling of drugs, particularly relating to side effects, that were sold through online pharmacies.

As the health risks associated with unlicensed online pharmacies are apparent, we would expect their market penetration to be minimal. However, the high costs of health care and health insurance in the USA makes them a high-risk alternative for low-income customers [16]. Unlicensed online pharmacies also attract customers of higher socioeconomic status, who can afford health care costs, but are instead interested in abusing prescription drugs for recreation [17]. In addition, unlicensed online pharmacies are not easily distinguishable from their legitimate counterparts. Ivanitskaya *et al*. [5] found that undergraduate students, even ones enrolled in health-related studies, could not easily identify illicit online pharmacies as such.

Legal and regulatory approaches to online pharmacies in the USA

Considering the US-focused context of our work, we briefly examine the regulatory framework in the USA pertaining to drugs. The Comprehensive Drug Abuse Prevention and Control Act of 1970, and especially Title II, the Controlled Substances Act, is the core piece of federal legislation regulating the drug market. Drugs are classified into "Schedules" according to potency for abuse and dangers of misuse. It regulates how drugs enter the market, how they are sold (after a physical examination, with a prescription, etc.), and imported. In 2008 the Ryan Haight Online Pharmacy Consumer Protection Act was passed, extending the Controlled Substances Act to regulate online pharmacies explicitly. Online pharmacies must have an associated physical "brick-and-mortar" pharmacy licensed in each state that it operates, and cannot sell, or claim to sell, prescription drugs without a prescription. Furthermore, issuing a prescription for the first time requires a physical in-person examination.

However, the problem of international pharmacies shipping their merchandise to the USA remains. This issue is compounded by the low prices of prescription drugs abroad [18], which create incentives for US-based customers to purchase their medication over the Internet. Other legislative efforts have tried to address different aspects of the problem of illicit online prescription drugs, albeit unsuccessfully (e.g. the Internet Prescription Drug Consumer Protection Act of 2000, Safe Online Drug Act of 2004, Pharmaceutical Market Access and Drug Safety Act of 2005, Internet Drug Sales Accountability Act of 2005, Safe Internet Pharmacy Act of 2007, and Safeguarding America's Pharmaceuticals Act of 2008). Internet and pharmaceutical industries have joined forces to self-regulate unlicensed pharmacies through accreditation, verification, and reputation programs [19–21]. Unlicensed pharmacies have been barred from purchasing Google AdWords since 2003 [22]. LegitScript [23], an online service that provides a list of law-abiding pharmacies, is reportedly used by Google and Microsoft to determine whether pharmacies are legitimate [24]. The National Association of Boards of Pharmacy provides accreditation, for a fee, to law-abiding online pharmacies, as well as an extensive list of "not recommended" online pharmacies, which fail to demonstrate that they abide to the law of their jurisdiction [25].

Other online verification programs do exist, which aim to assist consumers in making informed choices. Their stringency varies and range from requiring valid pharmacy licenses in the USA or Canada (e.g. pharmacychecker.com) to mere reputation forums (e.g. pharmacyreviewer.com). However, because of the large number of online pharmacies, many pharmacies are neither accredited or licensed, nor blacklisted. For instance, eupillz.com, an online pharmacy selling prescription drugs in 2013, did not appear at the time in any of the aforementioned databases.

Policing online pharmacies

In the USA, the Food and Drug Administration (FDA) oversees the safety of food, drugs, and cosmetics. The FDA has established cooperation with other federal agencies, namely the Department of Justice, the Drug Enforcement Administration, the Federal Bureau of Investigation, the US Customs and Border Protection (CBP), and the Postal Inspection Service [26]. The FDA recognized—as early as 2001—the significant complexities in investigating and enforcing policies relating to online pharmacies [12]. The FDA's efforts have focused on the shutdown of the illicit web stores, rather than on the identification of the structures that enable their operation. Examples of such operations are Cyber Chase [27] and Cyber X [28]. However, considering the extent of the problem and the significant duration of those law enforcement operations, the outcomes are usually underwhelming, highlighting the shortcomings of current enforcement mechanisms [8].

In the international arena, Interpol coordinates a series of operations to raise awareness and to identify the criminals engaging in the online prescription drug trade. Operation Pangea is an annual week-long operation with a large number of participating countries—a total of 111 participated in 2014—that enables coordinated action across many jurisdictions. Operations Mamba, Storm, and Cobra are in the same spirit as Pangea, but have regional focus (Eastern Africa, Southeast Asia, and Western Africa, respectively) and last longer (on average, one month; Storm I lasted five months)

[29]. Most importantly, the effects of these operations are short lived [8], and website takedown often ineffective as the online pharmacy can displace to other compromised hosts [30]. The efforts of enforcement need to be persistent for the effects to be long term.

Other efforts are subject to significant limitations due to a lack of international coordination. Operations targeting illicit sales of prescription drugs from international marketplaces depend on the capability to properly identify and examine packages at the port of entry. However, the immense number of packages arriving in the USA, and the limited capabilities for inspections by the US CBP, allow a potentially significant amount of illicit drugs to reach US-based customers [31, 32]. Even in cases with no jurisdictional issues to prosecute offenders residing abroad, the FDA depends on the foreign countries to take action against the wrongdoer [33].

Advertising illicit online pharmacies through search-redirection attacks

Online criminals interested in illicitly advertising products sold through web stores have been changing their methods through the years to achieve higher conversion rates. For example, due the small conversion rate of spam email (realized sales over emails sent), the miscreants started employing Twitter spam, which exploited people's trust to their online social network [34]. In addition, those advertising unlicensed pharmacies have also had to turn to innovative methods after being barred from legitimately advertising through search engines such as Google. "Search-redirection attacks," whereby web servers are compromised to manipulate web search results that promote the unauthorized sale of prescription drugs, are an example of such innovation. In this attack, traffic is dynamically redirected to different pharmacies based upon the particular search terms issued by the consumer. As the advertised site has at least a degree of relevance to the query issued, the conversion rate is much higher than for spam [1].

Figure 1 illustrates the attack. In this example, the top two results obtained for the query "cheap viagra" are compromised websites. The top result is the website of a news center affiliated with a university. The site was compromised to include a pharmacy storefront in a hidden directory. Clicking on any of the links in that storefront sends the prospective customer to pillsforyou24.com, a known rogue Internet pharmacy [23].

In search-redirection attacks, the website has been compromised, an act deemed as illegal in many countries. The compromised website redirects to content controlled by the offenders only when the search engine query matches what the attacker would like to display, in this example, advertisements for cheap Viagra. All other requests, including typing the web address directly into a browser, return the original content of the website. Therefore, website operators cannot readily discern that their website has been compromised. As a result of this "cloaking" mechanism, some of the victim sites remain infected for a long time [1].

Situational crime prevention and crime displacement

Clarke and Cornish's [35] perspective of "rational choices" in the criminal decision-making process provides a systematic approach for crime prevention. According to rational choice theory, offenders calculate the perceived costs and benefits of crime while seeking some type of advantage from their actions [36]. Choice structuring properties include the availability of tools, time, skills, and expertise, as well as the location of the target and the ease in which the crime can be committed undetected. Clarke and Cornish [35] observe criminal behavior as the "outcome of the offender's rational choices and decisions," and not as an effect of personal or societal dispositions. Therefore, crime prevention should focus on reducing criminal opportunity in the environments that are conducive toward crime.

Given this purposeful, procedural, and rational nature of crime, Clarke and Cornish [35] provide an analytic framework for crime

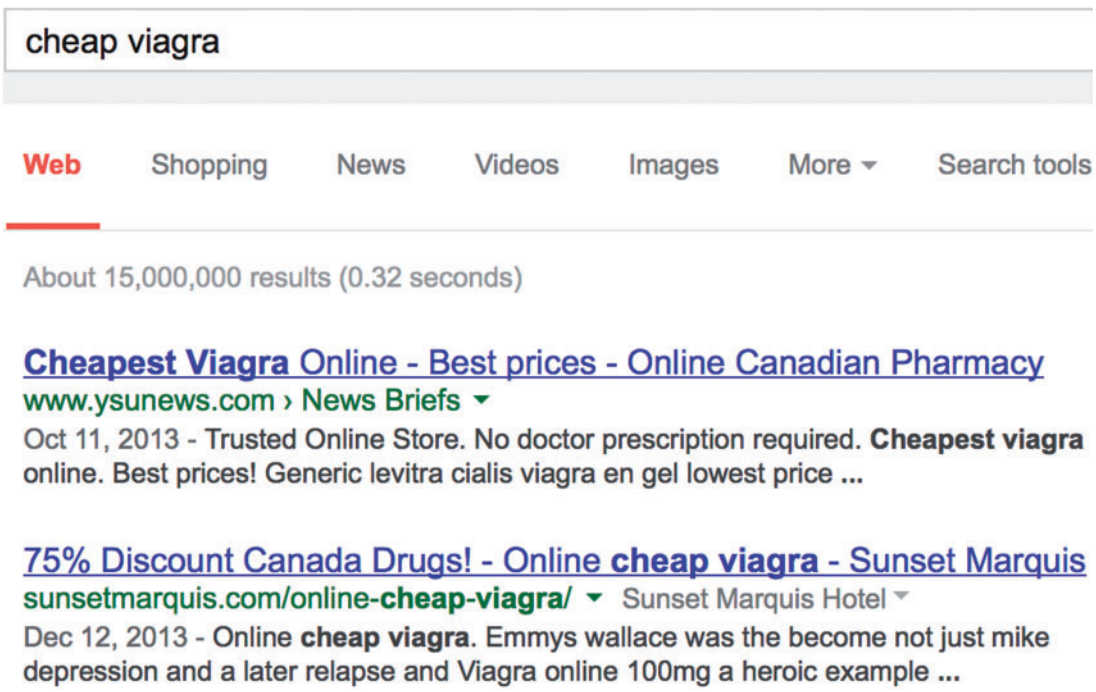

Figure 1. Example of a search-redirection attack. The first two results returned here are sites that have been compromised to advertise unlicensed pharmacies [4].

prevention, by placing the focus on the different stages of criminal events. The availability of opportunities plays a key role in criminal events, and by modifying the situation in which crime occurs, such as by installing physical barriers or improving lighting, crime may be prevented [37]. Situational crime prevention is not limited to physical locations, but is transferrable to crime that occurs online [38]. Situational crime prevention approaches are crime specific, requiring close attention to the associated situational factors. For example, there may be separate, but overlapping, models for website compromise, where the intent is to manipulate search engine results, as opposed to website defacement.

A common concern in relation to crime reduction techniques through situational prevention measures is what happens to the net amount of criminal activity deflected through such measures—i.e. the "displacement effects" [36, 39]. Indeed, there are various types of crime displacement that may occur after an intervention. For example, criminals can alter (i) the location, (ii) the temporal characteristics, (iii) the individual targets, and (iv) their techniques in committing their crime, or even (v) switch to a completely different criminal activity altogether [39, 40]. Indeed, the use of search-redirection attacks to advertise unlicensed pharmacies is an example of how techniques in committing a crime have changed in response to policy implementation. In this case, Google prevented offenders from advertising unlicensed pharmacies in a legitimate way, which may be one factor leading to the compromise of web servers for the purpose of illicit advertisements.

Modeling offenders' decisions using CSA

"CSA" extends the rational choice approach, using the notion of "scripts" from cognitive psychology [3]. It is a systematic framework for breaking down and examining the criminal process, and mapping situational prevention measures to every step of crime commission. In addition, crime scripts are useful in identifying the most significant steps of criminal operations (i.e. chokepoints) that can be targeted with more intense or persistent measures.

There are a number of studies that use CSA to understand criminal cases in mostly the physical [41–45], but also in the digital, domain [46–48]. In particular, Lavorgna [48] uses CSA to examine the trade in counterfeit drugs. While the focus was on drugs sold online, the developed script did not focus on the electronic aspects of the trade, other than noting that this is where the drugs were advertised and ordered. In addition, the crime prevention recommendations are limited to awareness raising and consumer education, while noting that technology may also play a role [48]. By examining these technical aspects in more depth, we further develop the work by Lavorgna [48] to identify what these technical countermeasures could be.

CSA is particularly useful when it comes to informing situational countermeasures. At a high level, Levi and Maguire [43] and Savona [49] show the importance of using situational measures to fight organized crime through crime scripts. Morselli and Roy [44] examine two stolen-vehicle exportation operations through CSA, identifying key brokers whose removal would result in a significant disruption to the underground market. While these crime types take place in the physical world, the idea that key brokers and chokepoints for intervention could have implications for other actors and steps involved in the crime commission process is also highly relevant to crime in the online environment.

Willison [46] examines a case of insider threat in computer-related crime, where a city employee accessed the city's financial systems to create fraudulent invoices. The crime script examines the various actions that allowed the criminal to be successful, and situational measures to prevent future occurrences of the specific crime are outlined. Hutchings and Holt [47] use CSA to understand the economy based around the market for stolen goods. This economy includes the sale of tools and services to steal data, the buying and selling of the data itself, the transferring of data into currency such as the sale of plastics and the advertising of drop services to receive card-not-present fraudulent purchases, and money laundering services. Chiu *et al.* [41] examine illicit drug manufacturing labs using data from transcripts of 30 Australian courts. Using information from the transcripts to build a crime script, they characterize (i) the manufacturing and storage locations, (ii) the resources used (i.e. chemicals and equipment), and (iii) the actions and interactions among the various actors. Finally, they identify measures for effective intervention at every step of the crime commission process, organized by location, target, and offender involvement.

An examination of online criminal processes to formulate disincentives

We now take a structured approach, informed by the empirical analyses by Leontiadis *et al.* [1, 50], to examine the crime scripts for the illicit online pharmaceutical trade, and to understand the processes enabling their operation and profitability. Considering the considerable reliance of our work on previous measurement studies, we briefly examine the methodologies used in the cited work.

Methods

Leontiadis *et al.* [1] gathered data for 218 prescription drug-related search terms every day for nine months. Over 7000 compromised web servers redirected visitors to a few hundred online pharmacies, to the detriment of legitimate pharmacies and websites providing health resources. This work not only provided an initial assessment of the problem, but it also empirically mapped the criminal online infrastructure and operation, which is critical for the construction of crime scripts.

The authors also considered the possibility that the potential measurement biases imposed through query selection biases would affect their findings. However, they were able to invalidate this hypothesis by running a comparative analysis between their primary set of 218 queries and two additional—much more extensive—sets of queries.

In their later work, Leontiadis *et al.* [50] collected inventory and pricing data over a period of six months on 256 unlicensed online pharmacies identified as advertising through search-redirection attacks. In essence, the authors continued the daily execution of the 218 queries, identifying the unlicensed pharmacies at the end of the redirections chains. Then for each of those pharmacies identified daily, they scraped the complete content, feeding it into a custom-made parser capable of extracting information on the advertised drugs. Related information includes (i) brand names, (ii) active ingredients, (iii) dosages, (iv) number of units per package, and (v) prices. Using this information, Leontiadis *et al.* were able to derive structural characteristics of this illicit online ecosystem, such as pricing and inventory selection strategies.

Overall, using the empirical data availed through the aforementioned research, we are able to derive crime scripts. These scripts are then mapped to situational crime prevention measures capable of disrupting the criminal operations, including decreasing the profitability, and increasing the risks.

CSA scenes in the illicit online prescription drug trade

The two key components that enable the illicit online pharmaceutical trade are: (i) the illicit advertising, namely search-redirection attacks, responsible for driving potential customers (i.e. web traffic) to the unlicensed online pharmacies and (ii) the unlicensed pharmacy, which is the process responsible for monetizing the received web traffic.

In the context of CSA, the two processes are termed "scenes," and we list their key sub-processes (termed "script actions") in Fig. 2. We note that while the two processes function independently, they should be considered as complementary to each other. The output of the illicit advertising is used as the input for the pharmacy operation, and we indicate this "communication" with a dotted arrow in Fig. 2. The complementary nature is evident when considering the multitude of uses for the hijacked web traffic. For example, the same traffic can be directed to other illicit online markets and to websites that can potentially infect their visitors with malware. Similarly, unlicensed online pharmacies can attract potential customers though means, such as email spam [34, 51], and organic search results [4].

Script actions for search-redirection attacks

Search-redirection attacks can be used to direct potential customers to illicit online pharmacies. This crime script allows for a detailed analysis of the criminal procedures. The search-redirection attack works in five steps. Initially, the criminals (i) identify vulnerable websites, and they (ii) compromise them by injecting malicious code altering the functionality of those websites. The compromised websites then (iii) manipulate search engines into associating the compromised websites with drug-related terms, even if these terms are completely irrelevant to the original content of those websites, (iv) hijack incoming traffic originating from search engine results, and (v) redirect web traffic to online pharmacies, often through one or more "traffic brokers." We now examine each of the five steps of the criminal process, identifying the commonly employed criminal methods.

Identifying vulnerable websites

Online criminals mainly employ scanners and search engines to identify vulnerable websites or hosting providers [52–54]. Through both methods, attackers look for specific characteristics of the hosting operating systems, web servers, and web content that are exploitable, allowing them to gain unauthorized access. The motivation behind the use of these techniques is the reduction of criminal operational costs. They are automated and capable of identifying a large portion of potential victims at low marginal cost. Florêncio and Herley [55] discuss the validity of this threat model from an economic perspective, showing that online criminal operations need to be effective at a large scale. However, while Florêncio and Herley [55] associate the reduction of expected criminal gains with the "sum-of-efforts" of defenders, this argument is not applicable in this case, due to the well-known vulnerable state of these websites. If the argument was applicable, reducing the number of vulnerable websites would actually increase the risk of victimization for those remaining [56]. The process of identifying vulnerable websites is precise in nature, as it reveals the websites that are known to lack the required defenses [54]. We may therefore assume that the majority of vulnerable websites identified with the aforementioned techniques are eventually compromised.

Compromising vulnerable websites

Methods of compromise become more sophisticated as they adapt to deployed countermeasures; however, the characteristics of compromised websites (i.e. the targets of criminals) are similar across time. Vasek and Moore [57] examine the risk factors that correlate

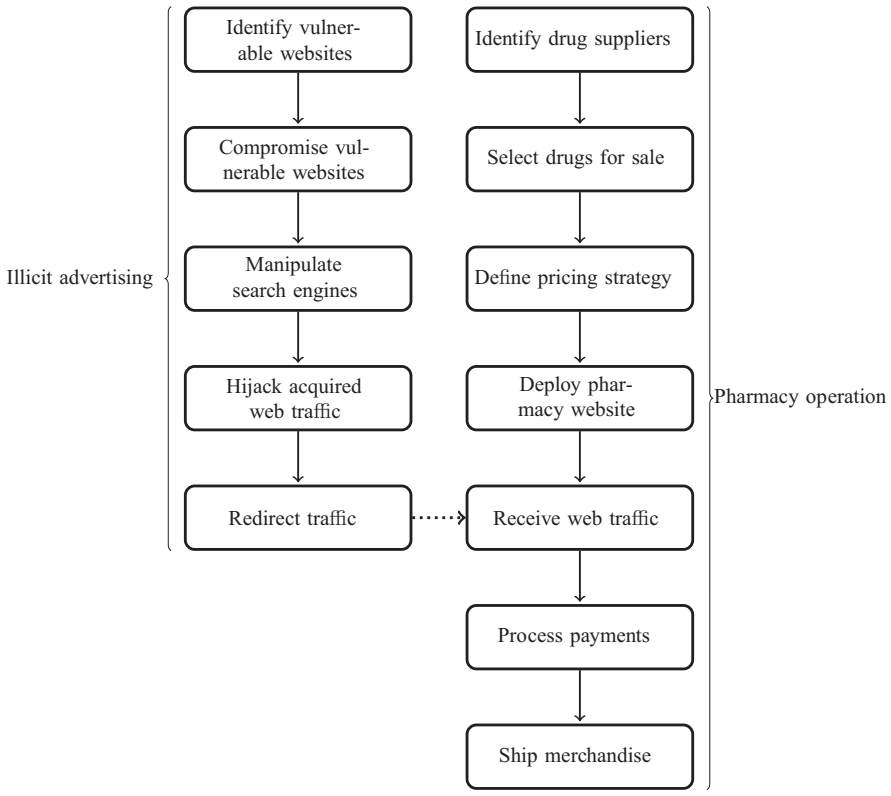

Figure 2. Components of the crime commission process in the illicit online prescription drug trade.

with a website being vulnerable to compromise and used for search redirection. Factors positively correlated with search-redirection attacks included running a Content Management Software (CMS) system (an application that simplifies the publication and editing of web content, examples include Joomla and WordPress [51]), particularly one that is popular, often exploitable, and out of date. Another risk factor is the website being hosted on a specific set of server types. In the same context, Soska and Christin [58] demonstrate a highly automated method to predict if a website will be compromised within a one-year horizon, based on an adaptive set of extracted features, with a recall rate of 66%. Another characteristic of compromised websites is their ranking (i.e. position) in search results. As the compromised websites inherit the popularity of the infected domains, online criminals have the incentive to specifically target vulnerable websites with high ranking, such as educational websites under the.EDU top level domain, so that they appear at the top of the search results [1].

Once these requirements for compromise have been met, the miscreants use tools available online, such as Metasploit [59], to deploy their attack, taking control of the vulnerable websites, and injecting their malicious code. Within the scope of a search-redirection attack, this malicious code manipulates search engine results, and hijacks the web traffic directed to the compromised websites.

Manipulating search engine results

One of the two key "responsibilities" of a compromised website is to manipulate the search engine crawlers into associating the legitimate-but-compromised website with drug-related queries. Examining the methods for accomplishing this goal, Leontiadis *et al*. [1] identified two prevalent techniques: "cloaking" and "pharmacy storefront injection." Cloaking is the act of serving substantially different web content, depending on the characteristics of the requestor. In the case of a search-redirection attack, the compromised website can detect the presence of a search engine crawler (which crawls the web and retrieves the content of websites, which are then associated with search queries), and provide a version of the compromised website that is filled with drug-related terms and links to other compromised websites (an act termed as "link farming" [60]). However, when the request is initiated from a non-crawler entity (i.e. normal web traffic), the compromised server either (i) presents the original content of the compromised website to avoid detection, or (ii) redirects the traffic to a different web location under the control of the attackers. The exact behavior is dependent on the variant of injected malware, and is often triggered using the information in the referrer field of the HTTP request.

A relatively new variant of the search-redirection attack injects a pharmacy storefront on an attacker-defined location within the compromised web server. In this case, the web server presents the illicit content regardless of the referrer information. This approach reduces the risks, and increases the benefits, to the attackers in two ways. First, it does not involve cloaking, a tactic that is usually against the terms of use of search engines [61–63]. Therefore, the chances of being the focus of a search engine intervention are lower than with the previous method. Second, it overcomes a deployed countermeasure that involves hiding the referrer information when a request originates from a search result page. This piece of information has been the cornerstone for previous attack variants, and withholding it nullifies the effects of the attack. However, by injecting a pharmacy storefront, online criminals effectively overcome the deployed countermeasures [50].

Traffic hijacking

The second "responsibility" of a compromised website is to take control over the incoming web traffic originating from search results. This function—which we call, in short, hijacking—makes the online criminals capable of directing the illicitly acquired web traffic to the online pharmacies. On the technical level, this is accomplished either through special directive injected in the configuration of the web server software, or by injecting specially crafted JavaScript (JS) and HTML functions into the compromised website(s).

Through the first method, the web server issues a HTTP 302 redirection, when the web traffic meets certain requirements based on the attack variant. A HTTP 302 redirection will forward traffic to another webpage. The requirements for redirection include an appropriate referrer value (implicit redirection), or a click on an embedded storefront (explicit redirection). Detecting this compromise requires auditing the web server configuration files and the outbound links. The second method accomplishes the same objective, but through the injection of malicious JS libraries, which in turn generate the appropriate HTML redirection code [52]. In this case, the attacker manipulates certain broadly used JS libraries, and detection is more complicated.

Traffic redirection

At this stage, the online criminals can leverage their control over the traffic targeting the compromised websites, and direct it to a destination of their choice, and, potentially, of their control. We have identified two criminal methodologies to redirect traffic: (i) using one or more traffic brokers that act as intermediate redirectors before reaching one or possibly more unlicensed pharmacies, and (ii) without traffic brokers, redirecting traffic directly from compromised websites to unlicensed pharmacies. Brokers are not used exclusively to funnel traffic to unlicensed pharmacies, but they are also rather an important resource for other types of gray online markets.

Leontiadis *et al*. [1] found that the vast majority of compromises (74.9% on average) make use of one or more brokers to redirect traffic to one or more pharmacies. "Dedicated brokers" that redirect traffic to a single pharmacy (per broker) are 61.1% of the total, and are linked to an average of 18.9 compromised URLs. On the other hand, "shared brokers" being 33.8% of the total, redirect traffic to 2.8 pharmacies (per broker), and are linked to an average of 11.8 infected URLs. Both types of traffic brokers enable the dynamic management of the pool of compromised websites, by making it possible to redirect to an alternative pharmacy location, when the one previously used is taken down. Shared brokers can also distribute the hijacked traffic to a large set of potential destinations, by allowing the dynamic redirection of traffic to a different pharmacy location at any point in time.

Script actions for unlicensed pharmacy operation

The procedural components of operating an unlicensed pharmacy are shown in Fig. 2. These include identifying drug suppliers, selecting drugs for sale, defining the pricing strategy, deploying the pharmacy website, receiving the web traffic, processing payments, and shipping merchandise. This analysis is mainly based on the research findings by Leontiadis *et al*. [50]. However, using findings from related work, the payment processing [64, 65], and shipping infrastructure [10] are also described.

Identifying drug suppliers

The drug suppliers are the entities responsible for producing and providing the drug stock of online pharmacies. Each supplier can

provide a diverse set of drugs, with distinct differences among them. Therefore, the availability of drugs at the unlicensed online pharmacies can be an estimator of the number of available drug suppliers. Empirical examination of the inventories of 256 unlicensed online pharmacies using the search-redirection attack as their advertising technique revealed concentrations of drug suppliers [50]. Overall, 50% of the pharmacies are linked to just eight drug suppliers.

However, this observation is not limited to the specific type of unlicensed pharmacies. In the aforementioned work, Leontiadis *et al.* [50] also examined a separate set of 256 pharmacies appearing in a list of about 10 000 "not recommended" pharmacies, described as such by the National Association of Boards of Pharmacy [25]. Pharmacies in that list lack any evidence of proper licensing, posing a potential health risk to whomever choses to purchase drugs from such businesses. In addition, pharmacy websites from this list use various methods of advertising that rarely overlap with the advertising methods employed by the main set of 256 pharmacies in Leontiadis *et al.*'s study. Nevertheless, the authors' examination of this additional set of pharmacies highlighted the presence of similar concentrations. Similarly, Gelatti *et al.* [10], using a different methodology, found that orders for prescription drugs placed at different unlicensed online pharmacies, were fulfilled by a small, fixed set of drug manufacturers.

Selecting drugs for sale

While an unlicensed online pharmacy may sell any possible subset of the drugs available through its supplier, it is a for-profit business operating in a shady environment. Therefore, it needs to be competitive among its shady, as well as its legitimate, counterparts. Unlicensed pharmacies can be competitive through a combination of two strategies: drug selection and drug pricing. It is noteworthy that licensed pharmacies are rarely able to engage in either strategy; they must fill every prescription for any possible FDA approved drug, and the amount of dispensed drug units is strictly defined in the prescription. Examining more than 1.02 million drug combinations that appear in 256 unlicensed pharmacies and one licensed online pharmacy, Leontiadis *et al.* [50] identified the drug selection strategies designed to achieve (i) greater variability of available drugs, (ii) greater availability of drug with potency for abuse, and (iii) targeted coverage of medical conditions that generate long-term profit from drug sales.

Defining pricing strategies

The second marketing strategy revolves around drug pricing. Generally, the pharmacy operators engage in a three-tiered approach that makes them competitive compared to licensed pharmacies [50]. Overall, they offer: (i) generally lower prices, (ii) fake generics, and (iii) volume discounts. In addition, unlicensed pharmacies offer deep discounts for widely used drugs compared to the less popular ones.

Deploying pharmacy websites

Online pharmacies are simply e-commerce websites that need to satisfy two prerequisites in order to be operational: (i) host content on a web server or at a web hosting provider and (ii) register a domain name. Their choices in both accounts are essential for being and staying operational. There are multiple ways to host a website. These include utilizing a web hosting provider as a service, or setting up a web server operated from a home or office. For more illicit operations, botnets are commonly utilized to host the questionable content [66]. Using a hosting provider is a common avenue both for legitimate and illicit purposes. For the latter, online criminals can benefit from the delayed—or complete lack of—response from service providers to law enforcement requests for taking down illicit content. That is especially important in cases where the time-to-take-down is critical for the success of the criminal operation [67].

LegitScript and KnuJoN [68] reveal that domain name providers (i.e. registrars) can also be considered as enablers of the operation of unlicensed online pharmacies. Registrars have the legal authority to discontinue the operation of domains engaged in illegal activities. However, they do not always have the financial incentive to do so. LegitScript and KnuJoN [68] found that four registrars, hosting the majority of unlicensed pharmacies at the time, acted as "safe havens" for these illicit operations, by ignoring requests for illicit domain takedowns. Levchenko *et al.* [69] make similar observations and highlight the capacity of criminals to exploit the systemic weaknesses to their benefit.

Receiving web traffic

Once the infrastructure and required collaborations are in place, the online pharmacies are ready to handle incoming web traffic representing potential customers. Search-redirection attacks, as outlined earlier, provide an illicit mechanism to receive web traffic, as industry has effectively put a stop to legitimate advertising of unlicensed pharmacies through search engines. Other vectors for traffic acquisition include email [51] and social networking spam [70]. A longitudinal analysis of online pharmacies using search-redirection attacks to attract potential customers has shown that a variety of ways to receive web traffic is used. These include using dedicated traffic brokers, using shared traffic brokers, or not using a broker at all [50].

Processing payments

When customers complete their orders, payments are often processed off-site through affiliate networks [65]. In addition, the payment processors, in 95% of cases, deliver the revenue through popular payment networks such as Visa, MasterCard, and American Express [64]. Generally, there are five parties involved in each transaction: (i) the cardholder who issues the payment (i.e. the customer), (ii) the issuing bank (i.e. the customer's bank), (iii) the payment network (e.g. Visa), (iv) the acquiring bank (i.e. the merchant's bank), and (v) the merchant, who receives the payment. McCoy *et al.* [65] and Levchenko *et al.* [69] have identified that the acquiring banks are the most crucial component in the payment infrastructure. Only a small number of them are willing to accept the risk of processing high-risk transactions for online pharmaceuticals, especially when there is increased pressure from the payment networks targeting those transactions.

Shipping the merchandise

LegitScript and KnuJoN [71] attempted to evaluate the legitimacy of online pharmacies advertising through search engines by placing a number of orders for prescription drugs. They found that drugs are shipped directly from the suppliers located mainly in India (via Barbados and Singapore, and packaged in Turkey), in violation of federal laws. More recently, Gelatti *et al.* [10] performed a similar analysis, ordering prescription drugs online, and having them shipped to Italy. They similarly found that, where the information was available, India was the main origin of the received packages. Other locations of origin included Turkey, the UK, and Vanuatu. Both analyses point to the fact that online pharmacies ship their merchandise through international locations, in order to exploit the well-established jurisdictional (e.g. [12]) and policing (e.g. [31])

limitations. In addition, they present no indication that any of the orders placed originated from within the USA.

Situational crime prevention measures targeting search-redirection attacks

We examine situational crime prevention measures capable of affecting the criminal opportunities for engaging in search-redirection attacks. This examination is performed from two distinct perspectives: before and after the occurrence of website compromise, which facilitates the illicit operation. We make this distinction as the situational measures affect distinctly different opportunities at each stage. Measures targeting the infrastructure of traffic brokers are also considered.

Measures applicable "before" website compromise

The situational measures in this category are specifically designed to prevent the compromise of vulnerable websites.

Utilize webmasters for website hardening. The vulnerable websites are the main driving force of this type of illicit advertising. Therefore, providing proper incentives or education to website owners in keeping their web space secure would effectively reduce the target availability. This would consequently increase the efforts required by the online criminals to succeed in their illicit goals. Considering the expected lack of interest of webmasters in implementing security countermeasures [72], such incentives would need to highlight the mandatory nature of taking action in this direction—e.g. by imposing fines.

CMS and web server hardening. Certain aspects of CMSs enable website compromises. We note the argument that hiding the version information of the CMS being used can reduce the potential for compromise [73]. However, this argument not only lacks empirical support [57], but it also interferes with the maintenance efforts of web administrators [54]. Instead, incentives for adequate penetration testing [74, 75], and inclusion of self-updating mechanisms that fix identified vulnerabilities could reduce the number of compromised websites. In addition, vulnerability reward programs are a cost-effective method for fixing software problems, especially when they are appropriately structured to provide rewards proportional to the severity of identified problems [76]. In essence, vulnerability reward programs provide incentives for independent researchers to discover and submit vulnerabilities to the respective software vendors in exchange for monetary rewards, instead of selling this information to the black market.

Utilize search engines to increase the effort and risks of compromise. Search engines are a key facilitator of this criminal operation, and can be utilized in a number of ways to deflect offenders, conceal vulnerable websites, extend guardianship for high-value targets, and reduce anonymity for suspect queries.

In relation to deflecting offenders, the use of search engines by offenders to identify vulnerable websites can be thwarted through the active identification and blocking of queries capable of revealing possible target websites from the search engines. Vulnerable websites can be concealed using the same methods as the offenders for identifying vulnerable websites (i.e. queries). Search engines can completely remove such websites from their indexes or decrease their ranking while they remain vulnerable. In terms of the latter type of action, Edwards *et al.* [77] suggest that search engines can prevent the spread of hosted infections by demoting—or "depreferencing"—compromised websites. While their analysis covers websites that are—potentially—already compromised, the predictive power of the methodology suggested by Soska and Christin [58] may provide an effective approach to conceal vulnerable websites with high potential for compromise.

High-value targets for website compromise include those that have a high ranking in search results. Search engines have the capacity to extend guardianship for such targets by taking routine precautions to identify vulnerabilities and attempts for compromise at these locations. Finally, anonymity for suspect queries could be reduced by permitting target-revealing queries only for users that have been authenticated (i.e. signed-in), while blocked for mischievous purposes for anonymous users.

Measures applicable "after" website compromise

Once a website has been compromised, resulting in search engine manipulation, the effort of the following situational measures shifts towards reducing the rewards to the offenders.

Utilize search engines to conceal victimized targets. Search engines can reduce the benefits of compromise, by first detecting and then removing or depreferencing compromised websites. Based on the attack variant, The heuristics to detect compromise are cloaking and injected storefront detection. The second heuristic can be implemented either through link analysis, as demonstrated in Leontiadis *et al.* [50], or by identifying unexpected content, considering the historical profile of the investigated websites.

Utilize webmasters to identify compromise. Webmasters should have the proper incentives (e.g. accountability), and receive proper education and assistance to regularly maintain and monitor their online property for indicators of compromise. This would be a distributed effort toward effectively stopping traffic redirection to malicious destinations.

Measures disrupting traffic brokers

The majority of the compromised websites, victims of the search-redirection attack, are linked to traffic brokers [1]. Therefore, these actors represent an important part of the criminal infrastructure. Crime prevention measures that can disconnect the traffic brokers from the rest of the criminal infrastructure may have significant disruption effects [obviously, whenever traffic brokers are not used for traffic redirection, such measures are irrelevant, and the focus should then be on the appropriate points of the criminal operations instead (e.g. through search engine intervention)] . The Internet service providers and the domain registrars, being the "place managers" that facilitate the operation of brokers—by providing them with IP addresses and domain names—meet this operational requirement. An intervention at this level would result in an increase in the operational risk (by increasing the possibility of punishment), and the efforts of criminals (by making it harder to find a "friendly" hosting provider). While offenders may displace to "bulletproof" hosting providers, these are generally more expensive, reducing the overall profit margin for offenders.

It is important to note that before making a request to the service providers to discontinue the services and resources of brokers, there is a need for empirically based investigative work for the proper identification of the traffic brokers. Leontiadis *et al.* [1] provide well-defined methodologies capable of meeting this requirement, and identifying the few Internet service providers and domain registrars that support the operation of traffic brokers.

Situational crime prevention measures targeting unlicensed online pharmacies

The situational prevention measures targeting the operation of unlicensed online pharmacies are inherently divided in four categories. These include measures that limit the supply of prescription drugs, measures that affect the availability of pharmacy websites, measures that prevent or reduce the network traffic reaching operational pharmacies, and measures that interfere with the processing and fulfillment or orders placed at unlicensed pharmacies.

Measures limiting prescription drug supply

Measures that reduce the availability of illicit prescription drugs include increasing the risk of operating drug labs and enabling traceability of precursor chemicals and specialized equipment. These should have a severe effect on the operation of unlicensed pharmacies and the financial benefits for online criminals.

Engage society to increase risk of apprehension. Chiu *et al.* [41] recommend, in relation to laboratories manufacturing methamphetamine, that the public should be encouraged to make reports to the police about their location. Given the small number of prescription drug manufacturing labs, an extension of this countermeasure is to provide monetary incentives to report their operation. These incentives should exceed the expected revenue of the criminal operations, to minimize the potential of bribery. The effectiveness of such measures can be significantly limited if a lab operates in a lawful context, but employees manage to illicitly acquire and sell certain portions of the legally produced drugs, or if the criminal groups controlling the operation of labs are able to provide much stronger—financial or otherwise—incentives to deter potential whistleblowers.

Enable traceability of precursor chemicals. Enabling proper identification of the well-known set of chemicals used to produce counterfeit drugs, can allow tracing of confiscated drugs back to their producers [78]. This action would potentially increase the risks associated with access to these chemicals, and the costs of illicit drug manufacturing.

Enable traceability of specialized equipment. Being able to identify the owners of specialized equipment used only for production of prescription drugs would result in an increase in the effort of producing the illicit substances, a subsequent increase in the operational costs, and an overall increase in the risk of apprehension [41]. Considering the small number of "large players" who manufacture the majority of illicitly traded drugs—eight in total associated with 50% of online pharmacies [50]—these measures have the potential to be highly effective.

Measures affecting the availability of pharmacy websites

The operation of unlicensed pharmacies has similar characteristics as the traffic brokers discussed earlier. Therefore, requesting the domain registrars to disrupt the operation of online pharmacies by the provision of services is also applicable in the present discussion.

Measures reducing potential customers

Methods to disrupt the criminal infrastructures sending traffic to unlicensed pharmacies through the search-redirection attack are outlined in the previous section. However, as it is noted elsewhere, unlicensed pharmacies also attract potential customers through organic search results and email spam. Existing mechanisms to disrupt these methods include search engines excluding such results [16], and the enforcement of email blacklists [79]. However, alternative measures explored here are aimed at reducing the likelihood that consumers will choose to visit unlicensed pharmacies by educating them about the potential health impacts and providing affordable health care through legitimate means.

Educate consumers. While it is well documented that drugs purchased online from unlicensed pharmacies can have severe effects on the health of consumers [13, 14], even people with medical knowledge are evidently unaware of those risks [5], or they choose to ignore such risks for various reasons (e.g. reduced cost, lack of medical insurance) [6, 12]. Therefore, large-scale campaigns providing information about the pitfalls of purchasing drugs online from questionable locations (e.g. [80]) can potentially protect consumers and reduce the profitability of unlicensed pharmacies.

Provide low-cost health care. Providing low-cost health care is aimed at improving public health and access for those on low incomes [81]. In relation to the illicit online prescription drug trade, the availability of affordable medicine is a potential countermeasure to prevent those with health problems resorting to online sales for financial reasons [16]. However, providing low-cost health care is a much debated and tedious task, and recent efforts in this direction [82] are to be evaluated for their long-term effectiveness.

Measures affecting orders placed at unlicensed pharmacies

The purpose of situational measures in this category is to prevent the processing of payments at unlicensed online pharmacies, and the delivery of their illicit goods.

Deny payments. Payments networks (e.g. Visa) that process credit card payments, have the potential to identify transactions benefiting unlicensed pharmacies, and force merchant banks—through financial disincentives—to sever their business relationships with the illicit pharmacy operators. In this case, there are limited options for the latter party to overcome this hurdle. For example, the offending merchants may have to use an alternative acquiring bank, which is not always an option. Also, the merchants may have to fraudulently mislabel the transactions (as non-drug related), in order to avoid detection, by the payment networks. It has been shown that measures in this direction can financially stifle offending enterprises, and provide counter-incentives for banks to cooperate with the online criminals [65]. It is noted that online pharmacies may displace their payment methods to accept digital currencies, such as Bitcoin.

Disrupt the market by confiscating illicitly imported drugs. Extensive inspection of packages received at international ports of entry under the jurisdiction of US CBP from locations known to ship the illicit merchandise may have a dual effect. While protecting customers from potential health risks [10, 13, 14], this intervention will also cause substantial financial loss to criminals through the unsatisfied requests of refunds from customers [65].

Discussion on the efficacy of suggested situational measures

The previous sections examined in detail the criminal processes enabling the illicit online prescription drug trade, namely search-redirection attacks and the operation of unlicensed pharmacies. This

CSA is based on empirical examination and measurements of the illicit operations, and it provides an understanding of the online criminal infrastructures and the interactions among their components. The CSA then informed the subsequent identification of situational prevention measures capable of increasing the criminal efforts and risks in engaging is such activities, while concurrently reducing the associated criminal profits.

In a version of the world where infinite resources were available to combat the problem of illicit online pharmacies, we would not need to worry about the effectiveness of these recommendations per unit of cost. However, implementing all aforementioned measures in the present version of the world that includes multiple stakeholders, opportunity costs, and individual agendas, we need to consider the feasibility of each of those measures.

Leontiadis' [83] approach in evaluating situational prevention measures is through a "complexity-effectiveness" analysis, which can be considered as the non-monetary equivalent of a cost–benefit analysis. Leontiadis defines the complexity of a situational prevention measure as the estimated number of actors participating or implementing the measure. In addition, he defines effectiveness as the estimated reduction of criminal activity, at a given level of complexity.

For example, this research identifies a small number of actors, relative to the overall number of pharmacies, that if targeted may have a disproportionately large effect on the operation of other areas of the illicit online pharmacy trade. These actors are the drug manufacturers, eight of whom supply half of the online pharmacies, and the traffic brokers, who funnel redirected traffic to unlicensed pharmacies. Hence, a complexity-effectiveness analysis of measures targeting these actors would reveal them as being a rather good choice for an intervention. This is similar to the findings of Morselli and Roy [44] who identified key brokers whose removal would result in a significant disruption to the stolen-vehicle market.

Applying this type of analysis to search engines and payment systems, we arrive to similar conclusions. Search engines enable online criminals in terms of identifying their victims (e.g. vulnerable websites), and of funneling web traffic into illicit businesses. Further on payment networks allow online criminals to monetize this stream of potential customers, giving them further incentive to continue operating their illicit business. Both types of actors share important characteristics. They are limited in number (at least the most popular ones), and they are overly important for the function of the illicit operations. These characteristics make them very effective whenever they take an action that limits the opportunities for offending. Search engines and payment networks are therefore, in a sense, part of the critical infrastructure of these online crimes.

However, when assessing the effectiveness of the various service providers, we can see how much less effective they can be. These service providers enable online criminal activity by providing necessary resources, such as Internet locations (i.e. websites). However, this group of actors is greater in numbers, and while specific actors may be more powerful in terms of their market share, we cannot argue that employing only the specific subset of actors for implementing a set of countermeasures will have similar effectiveness as with, e.g. search engines. In such case, online criminals can displace to a different service provider and continue with their illicit operation.

Concluding remarks

Contrary to traditional crime, the characteristic features of online crime often make it immune to traditional intervention approaches that would normally act as deterrents. Specifically, it is performed within a globalized virtual environment, the Internet, which allows for a certain degree of anonymity—or at least perceived anonymity. In this case, anonymity enables miscreants to profit illicitly or fraudulently without the fear of attribution, prosecution, and punishment [84]. In addition, even when a criminal action can be attributed to specific actor(s), jurisdictional complications often allow such actions to remain unpunished.

The global scale of online criminal operations is evidently a significant hardship from the perspective of law enforcement. International cooperation is necessary for targeting criminal operations taking place beyond the jurisdiction of the victimized population. However, while these are online crimes, there is a strong physical component, and it is the drug manufacturing stage that arguably poses the greatest risk in terms of targeted and informed law enforcement action. Online criminals may have the incentive to diversify the physical locations of their infrastructures, whenever this is applicable. However, physical relocation of the resources required to manufacture drugs for sale may impose a significant financial burden to online criminals.

Historically, the different components of online crime have been targeted in isolation, either by law enforcement, or through technical solutions. This approach has only short-term or superficial effects, as it usually does not affect the critical components of the criminal infrastructures. The overall problem is not that there is no incentive to target those components, but the fact that they often require complex methods to bring them out of obscurity. The methodology we suggest here takes instead an empirical approach in studying online crime, looking for the processes most vulnerable to intervention.

The methodological approach taken in this work provides an understanding of the structure of online criminal networks, identifies the associated critical resources providing opportunities to profit illicitly, and provides points for intervention using situational crime prevention. Measures that lack empirical support, or that do not, target critical resources are often futile. We argue that policy makers and technology providers need to work in tandem to get the upper hand in disrupting online crime. In addition, through this work, we suggest that the research community engaged in measurements of online crime can receive significant gains by combining their work with well-established concepts from different scientific domains. Indeed, this article applies traditional criminological crime prevention concepts, and effectively adapts them to the unique characteristics of digital crime.

Conflict of interest statement. None declared.

Funding

This work was supported by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSS&T/CSD) Broad Agency Announcement 11.02; the Government of Australia; and SPAWAR Systems Center Pacific [contract number N66001-13-C-0131].

Acknowledgments

The work would not have been possible without the invaluable assistance of Nicolas Christin, Tyler Moore, Alfred Blumstein, Pedro Ferreira, Richard Clayton, and Ross Anderson. We also thank the two anonymous reviewers whose comments and suggestions helped improve and clarify this manuscript. The opinions, findings, and conclusions or recommendations expressed are those of the authors and do not reflect those of the aforementioned agencies.

References

1. Leontiadis N, Moore T, Christin N. Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade. In: *Proceedings of the 20th USENIX Security Symposium*, *San Francisco, 2011*.
2. Cornish DB. Crimes as scripts. In: *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis*. Tallahassee, 1994.
3. Cornish DB. The procedural analysis of offending and its relevance for situational prevention. In: Clarke RV (ed.), *Crime Prevention Studies*. Monsey: Criminal Justice Press, 1994, 151–96.
4. Leontiadis N, Moore T, Christin N. A nearly four-year longitudinal study of search-engine poisoning. In: *Proceedings of the 21st ACM Conference on Computer and Communications Security*, *Scottsdale, 2014*.
5. Ivanitskaya L, Brookins-Fisher J, O'Boyle I *et al*. Dirt cheap and without prescription: how susceptible are young US consumers to purchasing drugs from rogue Internet pharmacies? *J Med Internet Res* 2010;**12**:E11.
6. Henney JE, Shuren JE, Nightingale SL *et al*. Internet purchase of prescription drugs: buyer beware. *Ann Internal Med* 1999;**131**:861–62.
7. Comprehensive Drug Abuse Prevention and Control Act of 1970. http://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1236.pdf.
8. Castronova JR. Operation Cyber Chase and other agency efforts to control Internet drug trafficking the "virtual" enforcement initiative is virtually useless. *J Leg Med* 2006;**27**:207–24.
9. Beccaria C. *Dei delitti e delle pene (On crimes and punishments)*: Il Caffè, 1764.
10. Gelatti U, Pedrazzani R, Marcantoni C *et al*. You've got m@il: Fluoxetine coming soon!': accessibility and quality of a prescription drug sold on the web. *Intl J Drug Policy* 2013;**24**:292–401.
11. Wilson T. Researchers link storm botnet to illegal pharmaceutical sales. 2008. http://www.darkreading.com/researchers-link-storm-botnet-to-illegal-pharmaceutical-sales/d/d-id/1129540 (19 October 2015, date last accessed).
12. Henney JE. Cyberpharmacies and the role of the US Food and Drug Administration. *J Med Internet Res* 2001;**3**:E3.
13. Bessell TL, Anderson JN, Silagy CA *et al*. Surfing, self-medicating and safety: buying non-prescription and complementary medicines via the Internet. *Qual Safety Health Care* 2003;**12**:88–92.
14. Bessell TL, Silagy CA, Anderson JN *et al*. Quality of global e-pharmacies: can we safeguard consumers? *Eur J Clin Pharmacol* 2002;**58**:567–72.
15. Orizio G, Merla A, Schulz PJ *et al*. Quality of online pharmacies and websites selling prescription drugs: a systematic review. *J Med Internet Res* 2011;**13**:e74.
16. Liang BA, Mackey T. Searching for safety: addressing search engine, website, and provider accountability for illicit online drug sales. *Am J Law Med* 2009;**35**:125–84.
17. Littlejohn C, Baldacchino A, Schifano F *et al*. Internet pharmacies and online prescription drug sales: a cross-sectional study. *Drugs Educ Prevention Policy* 2005;**12**:75–80.
18. United States Congress House. In: *Proceedings of Congress and General Congressional Publications*. Washington, DC: United States Government Printing Office, 2002.
19. Eckholm E. Abuses are found in online sales of Medication. *New York Times*, July 9, 2008.
20. LegitScript. Setting the record straight. n.d. http://www.legitscript.com/about/setting-the-record-straight (10 June 2015, date last accessed).
21. Miller CC. Google is said to have broken internal rules on drug ads. 2011. http://www.nytimes.com/2011/05/14/technology/14google.html (10 June 2015, date last accessed).
22. Office of the Deputy US Attorney General. Google forfeits $500 million generated by online ads & prescription drug sales by Canadian online pharmacies. 2011. http://www.justice.gov/opa/pr/google-forfeits-500-million-generated-online-ads-prescription-drug-sales-canadian-online (10 June 2015, date last accessed).
23. LegitScript. LegitScript: The leading source of Internet pharmacy verification. n.d. http://www.legitscript.com/ (10 June 2015, date last accessed).
24. Taylor P. Microsoft, Yahoo follow Google in fight against rogue online pharmacies. 2010. http://www.securingindustry.com/pharmaceuticals/microsoft-yahoo-follow-google-in-fight-against-rogue-online-pharmacies/s40/a501/ (18 June 2015, date last accessed).
25. National Association of Boards of Pharmacy. Not recommended sites. 2014. http://www.nabp.net/programs/consumer-protection/buying-medicine-online/not-recommended-sites/ (10 June 2015, date last accessed).
26. United States 106th Congress Senate Committee on Health E, Labor and Pensions. *E-drugs: Who Regulates Internet Pharmacies?* Washington, DC: US Government Printing Office, 2000.
27. US Department of Justice. International Internet drug ring shattered. 2005. http://www.justice.gov/dea/pubs/pressrel/pr042005.html (10 June 2015, date last accessed).
28. US Department of Justice. Operation Cyber X Press Conference. 2005. http://www.justice.gov/dea/pubs/pressrel/pr092105b.html (10 June 2015, date last accessed).
29. Interpol. Pharmaceutical crime: Operations. 2014. http://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations/ (10 June 2015, date last accessed).
30. Moore T, Clayton R. The impact of incentives on notice and take-down. In: *Workshop on the Economics of Information Security*, *Hanover*, *2008*.
31. United States 107th Congress House Subcommittee on Oversight and Investigations. *Continuing Converns over Imported Pharmaceuticals*. Washington, DC: US Government Printing Office, 2001.
32. US Food and Drug Administration. Imported drugs raise safety concerns. 2011. http://www.fda.gov/Drugs/ResourcesForYou/Consumers/ucm143561 (10 June 2015, date last accessed).
33. United States 118th Congress Senate Subcommittee on Investigations. *Buyer Beware: The Danger of Purchasing Pharmaceuticals over the Internet*. Washington, DC: US Government Printing Office, 2004.
34. Kanich C, Kreibich C, Levchenko K *et al*. Spamalytics: an empirical analysis of spam marketing conversion. In: *Proceedings of the 15th ACM Conference on Computer and Communications Security*. New York, 2008: 3–14.
35. Clarke RV, Cornish DB. Modeling offenders' decisions: a framework for research and policy. *Crime Justice* 1985;**6**:147–85.
36. Cornish DB, Clarke RV. Understanding crime displacement: an application of rational choice theory. *Criminology* 1987;**25**:933–47.
37. Clarke RV. Situational crime prevention: its theoretical basis and practical scope. *Crime Justice* 1983;**4**: 225–56.
38. Newman GR, Clarke RV. *Superhighway Robbery: Preventing E-commerce Crime*. Devon: Willan Publishing, 2003.
39. Felson M, Clarke RV. *Opportunity Makes the Thief: Practical Theory for Crime Prevention*. London: Home Office, 1998.
40. Smith RG, Wolanin N, Worthington G. *e-Crime Solutions and Crime Displacement. Trends & Issues in Crime and Criminal Justice No. 243*. Canberra: Australian Institute of Criminology, 2003.
41. Chiu YN, Leclerc B, Townsley M. Crime script analysis of drug manufacturing in clandestine laboratories: implications for prevention. *Br J Criminol* 2011;**51**:355–74.
42. Lacoste J, Tremblay P. Crime and innovation: a script analysis of patterns in check forgery. *Crime Prevention Stud* 2003;**16**:169–96.
43. Levi M, Maguire M. Reducing and preventing organised crime: an evidence-based critique. *Crime Law Soc Change* 2004;**41**:397–469.
44. Morselli C, Roy J. Brokerage qualifications in ringing operations. *Criminology* 2008;**46**:71–98.
45. Hancock G, Laycock G. Organised crime and crime scripts: prospects for disruption. In: Bullock K, Clarke RV, Tilley N (eds), *Situational Prevention of Organised Crimes*. Devon: Willan Publishing, 2010, 172–92.
46. Willison R. Understanding the perpetration of employee computer crime in the organisational context. *Inform Organ* 2006;**16**:304–24.
47. Hutchings A, Holt TJ. A crime script analysis of the online stolen data market. *Br J Criminol* 2015;**55**:596–614.
48. Lavorgna A. The online trade in counterfeit pharmaceuticals: new criminal opportunities, trends and challenges. *Eur J Criminol* 2015;**12**:226–41.
49. Savona EU. Infiltration of the public construction industry by Italian organised crime. In: Bullock K, Clarke RV, Tilley N (eds), *Situational Prevention of Organized Crimes*. Collumpton: Willam Publishing, 2010, 130–50.
50. Leontiadis N, Moore T, Christin N. Pick your poison: pricing and inventories at unlicensed online pharmacies. In: *Proceedings of the Fourteenth ACM Conference on Electronic Commerce*, *Philadelphia*, *2013*.

51. Pitsillidis A, Kanich C, Voelker GM *et al*. Taster's choice: a comparative analysis of spam feeds. In: *Proceedings of the 2012 ACM Conference on Internet Measurement Conference*, New York, 2012, 427–40.
52. Li Z, Alrwais S, Wang X *et al*. Hunting the red fox online: understanding and detection of mass redirect-script injections. In: *Proceedings of the 35th IEEE Symposium on Security and Privacy*, San Jose, 2014.
53. Long J. *Google Hacking for Penetration Testers*. Burlington: Syngress, 2011.
54. Moore T, Clayton R. Evil searching: Compromise and recompromise of Internet hosts for phishing. In: *Financial Cryptography and Data Security Workshop*, *Barbados*, *2009*.
55. Florêncio D, Herley C. Where do all the attacks go? In: Schneier Bs (ed.), *Economics of Information Security and Privacy*. New York: Springer, 2013, 13–33.
56. Camp LJ, Lewis S. *Economics of Information Security*. Norwell: Springer, 2004.
57. Vasek M, Moore T. Identifying risk factors for webserver compromise. In: *18th International Conference on Financial Cryptography and Data Security*, *Barbados*, *2014*.
58. Soska K, Christin N. Automatically detecting vulnerable websites before they turn malicious. In: *23rd USENIX SECURITY Symposium*, *San Diego*, *2014*.
59. Rapid7. World's most used penetration testing software. 2014. http://www.metasploit.com/ (10 June 2015, date last accessed).
60. Gyöngyi Z, Garcia-Molina H. Link spam alliances. In: *Proceedings of the 31st International Conference on Very Large Data Bases*, *Trondheim, Norway, 2005*.
61. Google. Cloaking. 2014. https://support.google.com/webmasters/answer/66355 (10 June 2015, date last accessed).
62. Microsoft. Bing Webmaster Guidelines. 2014. http://www.bing.com/webmaster/help/webmaster-guidelines-30fba23a (10 June 2015, date last accessed).
63. Yahoo! Content quality guidelines. 2014. https://help.yahoo.com/kb/search/content-quality-guidelines-sln2245.html (10 June 2015, date last accessed).
64. McCoy D, Pitsillidis A, Jordan G *et al*. Pharmaleaks: understanding the business of online pharmaceutical affiliate programs. In: *Proceedings of the 21st USENIX Conference on Security Symposium*, Berkeley, 2012.
65. McCoy D, Dharmdasani H, Kreibich C *et al*. Priceless: the role of payments in abuse-advertised goods. In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, *Raleigh, 2012*.
66. Nadji Y, Antonakakis M, Perdisci R *et al*. Beheading hydras: performing effective botnet takedowns. In: *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, *Berlin, 2013*.
67. Moore T, Clayton R. Examining the impact of website take-down on phishing. In: *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, *Pittsburgh, 2007*.
68. LegitScript, KnuJoN. Rogues and registrars. 2010. http://www.legitscript.com/download/Rogues-and-Registrars-Report.pdf (10 June 2015, date last accessed).
69. Levchenko K, Pitsillidis A, Chachra N *et al*. Click trajectories: end-to-end analysis of the spam value chain. In: *IEEE Symposium on Security and Privacy*, *Oakland, 2011*.
70. Grier C, Thomas K, Paxson V *et al*. @ spam: the underground on 140 characters or less. In: *Proceedings of the 17th ACM Conference on Computer and Communications Security*, *Chicago*, *2010*.
71. LegitScript, KnuJoN. Yahoo! Internet pharmacy advertisements. 2009. http://www.legitscript.com/download/YahooRxAnalysis.pdf (10 June 2015, date last accessed).
72. Herley C. So long, and no thanks for the externalities: the rational rejection of security advice by users. In: *Proceedings of the 2009 Workshop on New Security Paradigms*, *Oxford, 2009*.
73. Damron J. Identifiable fingerprints in network applications. *USENIX; login* 2003;**28**:16–20.
74. Austin A, Williams L. One technique is not enough: a comparison of vulnerability discovery techniques. In: *International Symposium on Empirical Software Engineering and Measurement*, *Alberta, 2011*.
75. Finifter M, Wagner D. Exploring the relationship between Web application development tools and security. In: *USENIX Conference on Web Application Development*, *Portland*, *2011*.
76. Finifter M, Akhawe D, Wagner D. An empirical study of vulnerability rewards programs. In: *USENIX Security*, *Washington, D.C.*, *2013*.
77. Edwards B, Moore T, Stelle G *et al*. Beyond the blacklist: modeling malware spread and the effect of interventions. In: *Proceedings of the 2012 Workshop on New Security Paradigms*, *Bertinoro, Italy*, *2012*.
78. Morelato M, Beavis A, Tahtouh M *et al*. The use of forensic case data in intelligence-led policing: the example of drug profiling. *Forensic Sci Intl* 2013;**226**:1–9.
79. Chachra N, Savage S, McCoy D *et al*. Empirically characterizing domain abuse and the revenue impact of blacklisting. In: *Workshop on the Economics of Information Security*, State College, 2014.
80. American Medical Association. Illicit online pharmacies resort to hacking to gain customers. 2011. http://www.amednews.com/article/20110905/business/309059964/7/pdf (10 June 2015, date last accessed).
81. Balabanova D, Mills A, Conteh L *et al*. Good health at low cost 25 years on: lessons for the future of health systems strengthening. *Lancet* 2013;**381**:2118–33.
82. United States 111th Congress. *The Patient Protection and Affordable Care Act*. Washington, DC: US Government Printing Office, 2010.
83. Leontiadis N. *Structuring Disincentives for Online Criminals*. Pittsburgh: Carnegie Mellon University, 2014.
84. Armstrong HL, Forde PJ. Internet anonymity practices in computer crime. *Inform Manag Comput Sec* 2003;**11**:209–15.