NDLERF

The online environment: A precursor to illicit synthetic drug law enforcement

Adjunct Professor Nigel Phair

Monograph Series No. 70

Funded by the National Drug Law Enforcement Research Fund
An Initiative of the National Drug Strategy

The online environment: A precursor to illicit synthetic drug law enforcement

Adjunct Professor Nigel Phair

Funded by the National Drug Law Enforcement Research Fund, an initiative of the National Drug Strategy

Produced by the National Drug Law Enforcement Research Fund (NDLERF)
GPO Box 1936, Canberra, Australian Capital Territory 2601

ISSN: 1449-7476

The research on which this report is based was funded by the National Drug Law Enforcement Research Fund, an initiative of the National Drug Strategy.

Contents

Box and figures

Executive summary

Synthetic drugs are drugs that have been manufactured to pharmacologically resemble naturally occurring drugs. Illicit synthetic drugs are those substances which may not be used for moral, legal or ethical reasons. Drugs are chemical substances that affect the normal functioning of the body and/or brain. Illicit drugs may cause immediate physical effects, but can also hinder psychological and emotional development (UNODC nd).

Criminals use the internet and related mobile technologies in all facets of the trade in illicit synthetic drugs and new psychoactive substance, including to purchase drugs and arrange their delivery, to pay for drug purchases and to launder the proceeds of crime. The best-known of all drug-related sites was Silk Road, which attracted significant media attention both while it was in operation and after it was shut down. The less well-known online drug marketplace, Black Market Reloaded, operated successfully for some time after Silk Road was shut down and, like Silk Road, was accessed via the dark web. Unlike sites on the visible web, information in the dark web is intentionally hidden from traditional search engines and the software crawlers that create search-engine indexes. To access the dark web, users download specialised software that makes their access largely anonymous and difficult for law enforcement to investigate.

The internet not only facilitates the purchase and distribution of illicit synthetic drugs and new psychoactive substances but also payments for such drugs, through a number of non-mainstream financial products. Virtual currencies, the most popular of which is Bitcoin, are gaining in popularity. The benefits of an anonymous global digital currency for criminals involved in illicit drug payments are obvious: no need to post cash overseas, visit currency dealers or pay exorbitant commissions.

Introduction

This project aims to improve law enforcement responses to the growing problem of illicit synthetic drugs by increasing our understanding of the role of the internet in such offending and using that understanding to better target interventions. It examines how criminals integrate internet use into their criminal conduct and how they adapt their practices to the online environment This paper may be useful in the design of procedures and related training packages for law enforcement.

The research involved:

- a review of the literature;
- the use of online intelligence gathering tools and techniques;
- seeking advice from specialist online technologists and security experts;
- analysing the behavioural patterns of legitimate and criminal internet users; and
- an examination of current trends in Australian and international illicit drug law enforcement. European and North American specialist law enforcement personnel, prosecutors, social researchers and policymakers were interviewed in depth on all aspects of the project mandate, with a focus on undercover law enforcement operations, technical communications interception, past arrest data, drug-use patterns, the use of new technologies and potential future online payment methods. A wide array of evidence and opinion was collected on these topics. The research team also spoke with Australian law enforcement agencies. Research in this burgeoning area is not limited to Australia, with many other jurisdictions tackling the same problems.

The National Drug Law Enforcement Research Fund (NDLERF) has supported a number of research projects with a view to improving law enforcement responses to the growing problem of internet-facilitated drug crime. Some of the papers funded by NDLERF that are particularly relevant to this project include:

- Willis K, Anderson J, Homel P & Smith A 2010. *A plan for national implementation of the drug law enforcement performance measurement framework: Companion document to NDLERF Monograph Series No. 34,Developing the capacity and skills for national implementation of a drug law enforcement performance measurement framework.* Canberra: Australian Institute of Criminology Canberra;
- Ransley J et al. 2011. *Reducing the methamphetamine problem in Australia: Evaluating innovative partnerships between police, pharmacies and other third parties.* NDLERF Monograph series No. 39. Sydney: NDLERF; and
- Ritter A et al. 2012. *Evaluating drug law enforcement interventions directed towards methamphetamine in Australia.* NDLERF Monograph series No. 44. Sydney: NDLERF.

The 2013 European Union (EU) drug markets report emphasises the global nature of internet-facilitated illicit drug manufacture and trading. The key issues around the role of the internet identified in the report are presented in Box 1.

Box 1: Key issues identified in the 2016 European Union drug markets report

- The increasing organisational and technical complexity, interconnectedness and specialisation of groups involved in drug markets. It is now common for organised
  crime groups (OCGs) involved with the drug market to diversify across multiple drugs, to engage in other forms of criminality, and to form alliances across ethnic and geographical boundaries.
- Globalisation and technology are accelerating the rate of change in the drug market. The dramatic transformation seen in legitimate commodity markets arising from developments in the global economy and information technology also a ect the illicit drug market.
- Drug market-related activities are concentrated in a number of established and emerging geographical locations. Innovation in synthetic drug production and changes in cannabis cultivation have resulted in greater opportunities for drugs to be produced nearer to consumer markets in the EU.
- A systemic analysis of drug market business models will be helpful for both operational and policy purposes. Understanding the dependencies and potential for interaction between di erent areas of the drug market, and the rationales, roles and organisational models used within it, is of growing importance.

The findings of the EU report are mirrored in this research into internet-facilitated drug crime in Australia. Offending across all drug-related crime, the speed and pace of change in offending patterns and emerging law enforcement issues are of particular importance. This project considers the wider context of internet-facilitated drug-related offending. This wider context will allow connections between offenders, offence types, marketing models and the platforms used to facilitate offending to be drawn, and the jurisdictional and evidential challenges these present for law enforcement to be considered.

Figure 1 outlines the conceptual framework applied in part A of this report to the examination of aspects of the internet that may facilitate drug-related offending (part C re-examines most of these in terms of the challenges they present for law enforcement).

Figure 1: Aspects of the internet that may facilitate drug related offending

Figure 2 outlines the conceptual framework applied in part B of this report to contextualise internet-facilitated illicit synthetic drug offending in relation to other internet-facilitated drug-related offending.

Figure 2: Illicit synthetic drug offending and other drug-related offending facilitated by the internet

Figure 3 outlines the conceptual framework applied in part C of this report to contextualise internet-facilitated illicit synthetic drug offending by focusing on the law enforcement challenges it presents.

Figure 3: Law enforcement challenges presented by internet-based offending

Synthetic drugs are manufactured to resemble naturally occurring drugs pharmacologically. Illicit synthetic drugs are those substances which may not be used for moral, legal or ethical reasons. Drugs are chemical substances that affect the normal functioning of the body and/or brain. Illicit drugs may cause immediate physical effects, but can also hinder psychological and emotional development (UNODC n.d).

The internet and associated technological advancements benefit society and the economy immensely, especially through social activities; however, they also enable illegal endeavours. The internet has been used to promote and commit a variety of cybercrimes and is also used in the production and distribution of illicit synthetic drugs and to disseminate information about drug use. Like many of their international counterparts, Australian law enforcement agencies have a long history of intercepting the importation and supply of illicit drugs including heroin, cocaine, cannabis and synthetics such as MDMA. Traditional investigation techniques honed over decades have been relatively successful; this research argues that the internet—and, in particular, the uptake of mobile internet-enabled devices—has changed this investigative paradigm.

The internet has become the street corner for many drug users and traffickers (Tandy 2004). The online availability of illicit synthetic drugs and 'legal highs' has significantly shifted drug manufacture, supply and use both globally and domestically and this, in turn, raises many questions for policymakers.

Internet-based drug trafficking includes the sale of illicit drugs and, increasingly, the illegal sale of pharmaceuticals containing narcotic drugs and psychotropic substances. The International Narcotics Control Board (INCB) notes that these pharmaceuticals, which have a high abuse potential, have become a significant problem in many countries because they have partly replaced traditional drugs of abuse (INCB nd).

The total size of the online market for illicit synthetic drugs is unknown but several indicators suggest it is expanding quickly. In 2010, about 95 percent of those Australians most likely to report the use of illicit drugs—people aged between 15 and 34 years—also reported they were internet users. To understand how drugs—specifically illicit synthetic drugs—and the internet intersect, a number of issues around drug use and internet use, and how these may overlap, must be evaluated (Barratt 2001).

The study concludes the internet is a viable and active channel for those involved in various activities around illicit synthetic drugs. Criminals can hide their identity and location, and online crimes are not always a high priority for police investigation. Law enforcement responses to internet-facilitated synthetic drug crime are often impeded by jurisdictional issues. The internet allows those who manufacture, supply, distribute and purchase illicit synthetic drugs to source chemicals, identify supply options, research market demand and determine the value of given substances with relative ease. Technology opens up a whole new world of opportunities for bringing illicit synthetic drugs closer to consumers (Schneider 2003). These are challenging circumstances for both national and international law enforcement.

Part A: How the internet facilitates drug-related offending

The internet is a global system of interconnected computer networks that use the standard internet protocol suite (TCP/IP) to serve users worldwide. It is a global mechanism for information dissemination and a medium for collaboration and interaction between individuals, organisations and governments. In 2013, over 2.7 billion people, roughly 39 percent of the world's then population, used the internet. The internet enriches many lives, providing social and economic benefits for both developed and developing nations (ITU 2013). It has increased the productivity of enterprises and better enabled government service delivery. The internet today is a global information infrastructure with a complex and rich history of technological, organisational and community development. The number of applications available to facilitate information dissemination continues to increase.

Mobile and smart devices are at the forefront of the development and adoption of technology by consumers, business and government. The demand for internet access and computer connectivity has led to the integration of computer technology into products that previously functioned without it, such as cars. In 2013, there were almost as many mobile cellular subscriptions in the world as people, with more than half of those in the Asia-Pacific region (3.5b of a total 6.8b subscriptions). Mobile cellular penetration rates stand at 96 percent globally; 128 percent in developed countries and 89 percent in developing countries (ITU 2013). As at 30 June 2015, there were approximately 21 million mobile handset subscribers in Australia (ABS 2016). This number has remained steady since the end of December 2014 and is an increase from 31 December 2012 when there were 17.4 million subscribers with mobile internet connections (ABS 2012).

Anonymity

Anonymous communications

Determining the origin of a communication is very often a key component of investigating illicit synthetic drug transactions on the internet. The distributed nature of the internet, however, combined with the large number of internet service providers (ISPs), often makes it difficult to identify offenders. Anonymous communication can be either a by-product of a service or offered with the intention of avoiding disadvantage to the user. An awareness of this uncertainty of origin is crucial to avoiding incorrect conclusions. There are a range of anonymous online communications methods including:

- public internet terminals and internet cafés;
- network address translation devices and virtual private networks (VPNs);
- wireless networks;
- prepaid mobile services (if the vendor does not verify the purchaser's identification);
- anonymous communication servers; and
- anonymous remailers.

There are many other simple ways to obscure communications, such as sharing the login for a web-based email account (like Gmail) between offenders. One user types a message as a draft that is never sent; another user will log in, read the draft email and then delete it. Many providers offer free email addresses which these require the user to provide personal information when the account is set up but, since this information is not verified, users can register email addresses without revealing their identity.

Anonymous web access

Law enforcement agencies investigating illicit drug production and distribution syndicates gather evidence in a number of ways, including through online activity and by examining computer remnants, which may retain lists of transactions between buyers and sellers. The authenticity of any material retrieved through such processes must be verifiable. Software such as The Onion Router (TOR) and other encrypted platforms make it hard to trace activities on the surface web, let alone on the hidden web; however, the use of TOR should flag to investigators that some type of illegal activity may have taken place and they should broaden their lines of enquiry (Finley 2008).

Encryption

Encryption renders data difficult to read by any unauthorised party by translating plain text into an obscured format using an algorithm. It involves the use of a key that allows the information to be returned to its original readable form by an authorised user. The extent to which illicit synthetic drug offenders use encryption technology to mask their activities is not known.

Like anonymous web access, encryption is not new; but changes in computer technology have transformed the environment. The widespread availability of simple software tools and the integration of encryption technology into computer operating systems make it possible for most computer users to encrypt computer data, thereby increasing the probability that law enforcement agencies will encounter encrypted material. Microsoft's operating systems, for example, allow the encryption of an entire hard disk. There are tools for encrypting communications such as emails and phone calls sent using VoIP; using such encrypted VoIP technology, offenders can protect voice conversations from interception (ITU 2012).

The use of encryption technology by offenders can seriously hinder access to relevant evidence. As a consequence several countries—including Australia, with Section 3LAA of the *Criminal Code Act* 1995 (Cth)—have implemented legislation addressing the use of encryption technology and related investigative instruments of law enforcement.

The Onion Router (TOR)

The TOR Project website states that 'TOR is free software and an open network that helps [the user] defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security'. Conceptually, TOR allows internet users to anonymise their online communications and transactions through a randomised series of encrypted virtual tunnels. The tool is used by online drug traffickers to maintain their anonymity and business continuity and avoid detection by legal entities. The TOR network can be accessed with free, readily available software known as the TOR Browser bundle, which allows anyone who downloads it to run the TOR client on their computer or device and configure the software to run a TOR network node.

There are some drawbacks to using TOR. The encryption process, combined with connection across TOR clients, results in slower internet speeds. Law enforcement has long tried to tackle TOR communications, with the best results obtained from targeting the end-user device rather than intercepting the already encrypted traffic. TOR communications can be disrupted, and some limited footprints of TOR activity can be traced, but both activities can be a significant drain on resources and finances. TOR does not protect against the exploitation of an insecure application to reveal the IP address of, or trace, a TCP stream. In addition, because TOR streams can be linked and sent together over a single circuit, tracing one stream sent over a circuit traces them all (Le Blond et al. 2011). TOR allows users making transactions on the internet to obfuscate their trail, making it difficult to trace (Murdoch & Danezis 2005)

The vexing problem for law enforcement—and for anyone uncomfortable with an open communications pipeline for criminals—is that TOR's positive aspects go hand-in-hand with its negative aspects. Anonymity and secure encryption can be used by criminals as easily as by free-speech activists.

Other Anonymising Techniques

Proxies

One of the fundamental technologies that assists in enabling anonymous communication is referred to as a proxy. When a user accesses the internet from a personal computer, the computer's IP address can be used to track its general location and the sites the user visits. In addition, law enforcement can use the IP address assigned by an ISP to find out who the registered user of that IP address was at the time. Internet users can use web proxies to provide anonymity and mask their activities. These are known as anonymous or open proxies, and the user's internet activities are diverted through these freely accessible parts of the internet for the express purpose of masking their origin.

Those hosting illegal online content often use what are known as reverse proxies to hide the location and protect the content of the host servers. In this case, when the internet user thinks they are visiting a specific drug website, for example, they are probably interacting with a public-facing reverse proxy that takes the request for information, repackages it and sends it to the host server, before taking the response from the server and resending it to the internet user. The use of a reverse proxy obviously provides increased protection for the criminal.

Internet cafes

An obvious way to maintain anonymity is to use a public-access computer or an internet cafe to carry out illegal activities; if law enforcement traces the IP address from which an illegal site is accessed, they will be led to a computer used by many people. Would-be criminals should know, however, that access to and use of such computers can be recorded and monitored, and may ultimately be tracked back to them.

Anonymizer

A popular, paid, set of anonymisation tools available to home and business internet users, Anonymizer helps mask internet activity and secure wi-fi connections. Anonymizer provides less-complete anonymity than TOR but is more user-friendly. In addition to Anonymizer, there are a range of other similar services like GhostSurf and Hide My Ass!, and many other so-called web anonymising services including VPN providers.

Ability to exchange expertise

The internet contains vast amounts of information that can assist in facilitating illicit drug sales, including explanations of how and where drugs may be obtained, or mechanisms that allow the online purchase of drugs. Producers can use the internet to identify suppliers of the precursor chemicals necessary for the production of drugs such as amphetamine derivatives, and to obtain recipes and instructions for producing drugs.

The volume of illicit sales of narcotic drugs and psychotropic substances through websites is rising and the internet is a major source of information about drugs and drug abuse. Internet users can easily obtain information that is potentially harmful, including:

- guides on using and preparing drugs (for example, methamphetamine cookbooks) and expected experiences;

- guides on how to make narcotics with household items, including how to conceal this and avoid law enforcement attention;
- step-by-step instructions on constructing explosive devices and improvised firearms;
- guides to using over-the-counter drugs to produce a desired effect;
- techniques for obtaining precursors (including theft) used to produce narcotics; and
- advice on how to use money transfer services when procuring pharmaceuticals from overseas. (ACBPS 2010).

Some users go online to source information on harm-reduction techniques for drug use, while some individuals seek online support groups and information on positive behavioural change, such as how to identify and address substance-abuse issues. As such, there is great potential for online prevention and intervention efforts; but drug users more broadly may be ignorant of the dangers these chemicals pose and, despite the risks involved in taking illicit synthetic drugs, many people often purchase them online due to naivety or curiosity.

The main players in the increasing use of the internet to source information about illicit synthetic drugs are search engines and, in particular, Google. Search engines essentially filter the information available on the internet. They allow users to quickly and easily find information of interest or value to them without the need to wade through numerous, potentially irrelevant web pages.

Anecdotally, there appears to be an increase in the number of websites set up to capture or steal the identity of visitors searching for illicit synthetic drugs. Similar identity-theft sites operate in areas such as pornography.

Ability to coordinate small transactions on a large scale

The internet is a great enabler for those involved in all aspects of illicit synthetic drugs; web communications are rarely monitored by government agencies, allowing for ease of illegal trade. Like the rest of society, transnational criminals use the internet to communicate and to promote their illicit activities.

More physical objects are now embedded with sensors and enabled for network connectivity, thus enabling them to communicate via the internet; this is known as ‘the internet of things’. The resulting information networks will create new business models, including for those involved in the manufacture, distribution and sale of illicit synthetic drugs. This internet of things will allow behaviour to be monitored and shipments to be tracked, and enhance situational awareness (through the placement of sensors) at different stages of the illicit drug life cycle, thus potentially reducing the risks for the criminal enterprises involved in this activity.

Marketplace

The internet is a cost-effective way to distribute goods on a global scale. It reaches many places and cultures; it provides technical tools that allow anonymity and aid in preventing the interception of communications and transactions; and it is constantly evolving, as is how consumers, businesses and governments view and use it.

A simple search in Google or Bing for keywords like MDMA, mephedrone, GHB and XTC delivers multiple hits for ads and websites where these drugs are offered. These ads detail the different types of drugs offered and often appear on websites which also sell legitimate products and services. There are so many websites and portals offering such substances for sale that global law enforcement agencies can only, at best, be reactive to the problem.

The internet also facilitates the sale of new psychoactive substances (NPS). In recent years, more of these types of drugs have been reported in Europe; in 2009, 2010, 2011 and 2014 the European Monitoring Centre for Drugs and Drug Addiction listed 24, 41, 49 and 101 new substances, respectively. New psychoactive substances, also referred to as designer drugs, ‘research chemicals’ or ‘legal highs’, are substances that are chemically related to existing, prohibited drugs and give a comparable effect.

According to the Pompidou Group, there are three general ways of illicit synthetic drugs are sold on the internet:

- by individuals selling through discussion forums;
- through online shop-fronts; and
- though online marketplaces which connect buyers and sellers.

To the uninitiated it may seem odd that a person would pay someone they have never met face-to-face for goods or services online—particularly for illegal goods— but legitimate online marketplaces have become thriving places of interaction, built on safer payment methods and reputation systems that utilise feedback. The best example of such a marketplace is eBay. It is conceivable, then, that public trust in illegal product marketplaces could be established, assuming issues such as anonymity, reputation, communication and payment can be addressed.

Marketplaces for illicit synthetic drugs are hosted on dark web sites, many of which also offer other illegal goods, such as child abuse material or stolen artefacts, for sale. Many of these marketplaces allow anonymised payment methods, such as Bitcoins, which can also be used for money laundering. Like traditional online marketplaces, they supply and source commodities globally, relying on sophisticated business models and the use of technology.

Distribution of drugs

Orders placed with online illicit synthetic drug marketplaces are typically small and delivered through traditional postal or courier services. The sender usually packs the drugs in vacuum-sealed bags to evade sniffer dogs and takes other steps to ensure the package looks like a legitimate postal item. Small amounts of drugs are conveyed in multiple packages, often to multiple locations, to minimise risk. The buyer may be the end user or a dealer seeking to supply a local market. The internet has played a further part in the illegal drug trade—certain sites post the price of street drugs in various cities, allowing crime groups to ascertain conditions in local drug markets and analyse the types of drugs in circulation, their prices and availability. As for legitimate enterprises, this strategic information allows crime groups to plan diversification of their activities or an expansion of their trafficking routes.

The abundance of formulae and drug-manufacturing advice available online may entice non- or casual drug users to experiment. In addition, details of sources of precursor chemicals and laboratory equipment may contribute to the expansion of home pharmaceutical manufacturing. The concern is that this proliferation of information, which includes accounts of individual experiences, may excite curiosity and potentially normalise such dangerous behaviour (Schneider 2003). The INCB has sought to address this concern by calling on international governments to close down illegal internet pharmacies and seize substances which have been illicitly ordered on the internet and smuggled through the mail (UNODC).

These internet sites act as a platform for social connections between drug users and their friends and associates. Forums that attract this audience also provide information about synthetic drugs and the latest news about them (Pates & Riley 2012).

Online pharmacies

Illegal internet pharmacies, and mail and courier services, continue to flourish as important channels for diversion; shipments are difficult to track and the sheer volume of international mail makes it impossible to physically screen every package. Of substances under international control, benzodiazepines appear to be those most commonly ordered from illegal internet pharmacies. A related concern is that the majority of the drugs supplied by illegal internet pharmacies may be counterfeit (INCB 2012).

The consumption of illicit synthetic drugs is a growing trend. Synthetic cannabinoids, more often referred to as synthetic marijuana, are popular; however users rarely know what to expect because the purchased substance consists of untested research chemicals sprayed on a herbal mixture. These substances are sold through illegal internet pharmacies. A percentage of online pharmacies operate within the law and to ethical standards, but counterfeit chemists dealing in illicit products also thrive on the internet, operating on the pretext of providing legal drugs. Easy access to these websites enhances the supply of illicit synthetic drugs, satisfying an increased demand for them (Council of Europe 2001).

As part of the 9th annual International Internet Week of Action, the US Food and Drug Administration, in partnership with international regulatory and law enforcement agencies, took action against more than 4,402 websites that illegally sell potentially dangerous, unapproved prescription medicines to consumers. The goal of the week of action was to identify the makers and distributors of illegal prescription drug products and to remove these products from the supply chain (FDA 2016).

Drug information websites

Informational drug sites proliferate on the internet, with a variety of websites providing information from a diversity of perspectives. Most of these sites are anti-drug use, set up by community groups and governments. Using search engines to find information about drugs, though, may lead the user to pro-drug websites (Boter et al. 2006). In some cases, especially with newer or emerging drugs such as 2,5-dimethoxy-4-(n)-propylthiophenethylamine (2C-T-7), the only information available on use and effects is on such websites. This illustrates the importance of monitoring these sites for emerging trends in substance use and abuse (Wax 2005).

Websites such as Erowid (www.erowid.org) claim to provide reliable, non-judgemental information about psychoactive plants and chemicals and related issues. Such sites often provide basic information on the chemical components and preparations of substances, the effects of substances and techniques for ingesting them and also offer dosage guidelines and, in some cases, user reports. Other websites which are not focused on substances have also become forums for user reports, such as YouTube.com, where users can post videos about their experiences with substances. The information provided by sites, and the role they play in the larger drug and research community, varies; for example, www.maps.org is the website of the Multidisciplinary Association for Psychedelic Studies, a non-profit research organisation that sponsors policy initiatives and research on the use of psychedelics (Montagne 2008).

Adolescents and young adults increasingly use such websites to find information related to drugs (Boyer et al. 2005). Erowid administrators report each day the website receives an average of 3.8 million file hits (445,000 page hits), with 24 gigabytes of data transferred. They get an average of 55,000 unique visitors a day, viewing about eight pages each.

One of the main concerns around these sites is the accuracy and quality of the information they provide. Many of these websites contain potentially harmful recommendations for managing the adverse effects of various substances. For example, DanceSafe states that the level of risk associated with nitrous oxide inhalation is comparable to the risk of spontaneous combustion (https://dancesafe.org/risk-assessment). Other research, however, argues that much of the information on the effects of drugs, the biological sources of psychoactive compounds and the synthesis and extraction procedures (at least of hallucinogens) is accurate (Erowid nd).

Further, non-drug-using individuals who searched the internet for drug-related information rate the perceived benefits of drug use as higher than those who searched for unrelated information and/or those who reported previous drug use. Those who searched the internet for drug-related information were also more likely to report that using club drugs would help them fit in when in a social situation than those who searched for unrelated information. These results indicate that drug-naïve adolescents and young adults may be especially susceptible to information found on the internet and that this information may serve to normalise drug use, thereby introducing these adolescents to regular patterns and established user communities (Brewer 2003).

The internet is also home to online communities of people involved in substance use, or to music cultures in which substance use is prevalent. The internet has long been used to publicise events and maintain communities built around music and drug use, particularly through closed Facebook groups. Online social networking sites enable users to significantly expand their social networks, and individuals may come into contact with users previously unavailable to them. Specifically, low-risk and high-risk individuals—who may be segregated in their real-life social networks—can now potentially contact one another. This increased networking ability provides drug-using opportunities where no, or few, opportunities previously existed in an individual's social network. Such extended social networks may also contribute to the accelerated spread of new substances of abuse (Tupper 2008).

Differences between local, national, and international drug legislation pose a problem, especially for emerging illicit drugs—specifically where websites offer synthetics drugs which are legal in the jurisdiction where the website is hosted, but illegal in other jurisdictions where the buyers are located. Research on grey-market websites has primarily focused on the sale of prescription drugs over the internet, with studies finding that prescription drugs online can be readily purchased online. A Pew Internet and American Life Survey found 26 percent of adults searched online for information about prescription drugs online and 4 percent of adults used the internet to purchase them, though the majority of these purchases were made with a prescription (Fox 2004).

The Australian Drug Information Network is Australia's leading alcohol and drug search directory. They produce reliable information on alcohol and other drugs, with links to treatment services, research, statistics, guidelines and more.

The deep web and the dark web

The deep web is made up of structured data compiled in databases; the dark web is comprised of restricted access pages that have been hidden from conventional search engines so that those engines cannot index them.

Unlike pages and information on the visible, or surface web, information in the deep web is invisible to the software used by search engine indexes because conventional search engines index pages based on link popularity, something which does not apply in the deep web. There are no links to deep web or dark web pages, so search engine spiders cannot schedule them for indexing as they crawl over other websites (Dragut et al. 2012).

The deep web and the dark web present complicated platforms for users and search engines, making the search for information difficult for those who do not have an understanding of their makeup. Online pharmacies dealing in illicit synthetic drugs are largely protected within the dark web from both law enforcement and curious internet users (who may not even be willing buyers); this helps them connect to a discreet niche market.

Deep web information can only be accessed when a user searches for an item in a specific database. A random search would be tedious because the user would have to manually search through many databases; they would have to know that the database exists.

An efficient search for pages in the hidden web requires understanding of the integrated access concept, which relies on data collection and meta-search. Through collection of data, a web searcher amalgamates records into one database for indexing, and conducts a search in the unified data record.

This method poses a number of problems that affect the time needed for a search as well as the quality of search results. For it to be effective, the pharmacies trading in illicit synthetic drugs must have uploaded content into a central system so that the search engines operating within that system can retrieve structured records of information. The other option is a Meta search. This method involves an integrated system where users query interfaces. When a user queries the system, it translates the query into language that the system understands so that it can retrieve records that match. For this system to be effective, it must retrieve sufficient information from the right databases. Therefore, the current best practise is using databases in a specific field (Dragut et al, 2012).

Not all deep web search engines are created or used for illegal activity. There are search engines which can crawl the deep web databases and present information to the internet public. Some examples include Surfwax, Direct Search, Agrisurf, Zoominfo and TenkWizard among others. They retrieve databases that relate to science and business subjects. On the other hand, there are tools that access government and business databases such as The Labyrinth, MedNets and GPOAcess among others.

Complete Planet is a deep web search engine which contains dozens of databases of information found in pages on the hidden web. They relate to many different topics and subjects. It is a relatively easy way to get into the deep web structured databases as this search engine also polls conventional search engines. The database retrieved by Complete Planet is specific, meaning it relates to structured data about a distinct topic or field. This search engine offers options of using a number of words as the query terms or even phrases. The search engine translates queries into natural or structured queries. With such resources, a user can search the deep web easily and filter the precise location of information about illicit synthetic drugs (Schreeren, 2012).

WWW Virtual Library is another deep web search engine. It contains databases relating to different fields such as education, communication, business and economics, law and recreation among others. This search engine depends on indexes generated from various parts of the world, complied into a network that retrieves data based on the query terms. Some deep web databases are free, making it easy for any person to gather information, while others attract a fee. For instance, the Library of Congress does not charge while others like Dow Jones News Retrieval is a fee based service (Hope, 2007).

The deep web refers to content on the web that cannot be accessed by traditional search engines which users see on the surface or traditional web. Interestingly:

- The deep web contains 7500 Terabytes of information, whereas the surface web contains 19 terabytes of content.
- More than 200,000 deep web sites currently exist.
- 550 billion individual documents can be found on the deep web compared to the surface web's 1 billion individual documents.
- 95% of the Deep Web is publically accessible, meaning no fees or subscriptions. (The Deep Web nd)

Websites on the deep web revolve around major topics and industries just as those on the surface web do. The main industries found on the dark web include news and media, health, government, computing, shopping, employment, business, and even the arts (Yao 2010).

The furthest corners of the deep web, are the segments known as the dark web which contain content that has been intentionally concealed. Most of these websites are subscription-only access. The everyday internet user may not know these sites exist because the sites allow access only to those on their mailing list. (Dragut et al. 2012) A successful search for such pages depends on the user's ability to find them using a query term that matches their structured data.

Restricted-access pages on the dark web block search-engine spiders from indexing them. The search engines are unable to penetrate the restrictive context to index the website's pages (Dragut et al. 2012). If someone searching the web fails to enter the right query term or phrase, their search results will be inaccurate—they will return hits for so much information and so many databases that it will be hard to pinpoint which pages they wish to visit (Yao 2010).

In the dark web internet transactions are largely private, potentially going unnoticed unless the buyer or seller discloses information to third parties. These transactions benefit from search engines being unable to track every detail that is going on in the structured data pages. Online sellers and buyers converse through live chat, which is instantaneous and hard to track. As third parties are unaware of the transactions occurring on dark web pages, these live conversations are also undetected (Godse 2008).

Young people, especially teenagers—who are often early adopters of new technology—use the dark web because it helps them avoid land-based transactions. Many young people have learnt about the dark web, and its plethora of information about drugs, where to get them, and their effects, through trial and error (Godse 2008).

Illicit drug manufacturers use the internet to research production methods and recipes. Dark web forums are used to trade information about demand in the market and the latest trends. Buyers and sellers also use the dark web as a resource centre which helps them stay abreast of trends within this hidden market. The information available may be audio or visual, including documents detailing manufacturing processes or news literature. The search engines that crawl this part of the internet generally operate the same way traditional search engines do (Garbato 2005).

The manufacture of illicit synthetic drugs changes in line with global innovations; such changes also affect law enforcement responses. As there are no restrictions on the dark web to limit information on the manufacture of illicit drugs, illicit drug manufacturers can access hidden databases which provide such information in the form of news or forums on drug manufacture. Since there is a real-world, land-based component to illicit drug manufacture in the form of laboratories, manufacturers require regular information to adjust their products to market trends (Monfries 2012).

Ongoing developments in both the deep web and the dark web are making it more difficult for search engines to find and index pages. This translates to a situation where many sites, legal or illegal, operate without the public's knowledge or awareness. Internet users visiting sites such as Silk Road (now defunct; discussed later in this paper) reflect the growing demand for online drug trading. Silk Road offered over 700 drugs, and its distribution chain involved linking buyers to sellers. Upon completion of a transaction, many sellers delete a buyer's contact details to hide the transaction (Oakes 2011).

The identity of Silk Road buyers is largely unknown and cannot be made available due to the use of TOR software (also discussed later), which provides anonymous access by allowing users to cover their tracks completely (ES Magazine 2012). As previously noted, TOR software allows a user to access the dark web and conduct transactions without leaving any traceable details. It works on computers, phones and other devices; once installed, the user can click through hidden web links anonymously. The software directs user traffic across several servers to enhance the encryption of information (Oakes 2011).

Ongoing cooperation between law enforcement agencies and ISPs would be an important way to learn more about illicit drug-market activity on the dark web and subsequently assist in drug law enforcement (Morris 2002).

The illicit synthetic drug network involves not only buyers and sellers but extends to shipment companies, suppliers and Bitcoin sellers (further discussed later). When these elements interact on the dark web via encrypted communication, it is very difficult for law enforcement agencies to identify those responsible and interdict their activities. Internet Relay Chat (IRC), an application-layer protocol that allows users to communicate via text, helps anonymise communications—often taking place in ordinary chat rooms, but also through encrypted sessions that hide conversations. Generally only those who are invited and who know how to access them, know where to find these chat channels (Hutson & Miller 2020).

Just as criminals may rely upon the anonymity of the dark web, so too can the law enforcement and government intelligence agencies. They may use it to conduct online surveillance and undercover operations or to create anonymous tip lines.

Silk Road

Silk Road was an anonymous online marketplace. It was not the only such online marketplace, but remains the most widely known (Cristin 2012). It was first mentioned in mainstream media following a June 2011 Gawker article. Unlike older drug marketplaces that used closed forums, instant messaging and private groups, Silk Road was a marketplace where buyers and sellers could interact with each other in an open, active community.

In October 2013, US federal investigators closed down the Silk Road website and marketplace, arresting the alleged operator Ross William Ulbricht. According to the FBI, the site generated up to US$1.3b in sales in Bitcoins and made more than US$80m in commissions (ABC News 2013). Silk Road was a product of the underworld on the web, an online marketplace with many types and varieties of legal and illegal drugs for sale (Oakes 2011). Its popularity was significant: the site was launched in February 2011, and by July 2012 had over 150,000 customers with sales translating to millions of dollars (Christin, 2012).

Items offered for sale on Silk Road were grouped by categories. There were approximately 220 distinct categories ranging from digital goods to pornographic material, to various kinds of narcotics and prescription medicine (Chen 2011). The website ran on a combination of internet and encryption technologies that allowed anonymous buying and selling of illegal products. It could only be accessed by those who installed The Onion Router, or TOR, software and who had a user account on the site (Dingledine et al. 2004). Silk Road did not use traditional payment methods such as credit cards, instead utilising Bitcoins. Bitcoins are a special electronic currency, developed to use in a decentralised manner to ensure no central authority manages it (Brezo & Bringas 2012). Bitcoins can be purchased using any currency, with transactional exchanges of Bitcoins between organisations and buyers worldwide (Mt Gox 2012). Bitcoin transactions are difficult for law enforcement agencies to track due to the encryption of all Bitcoin transactions.

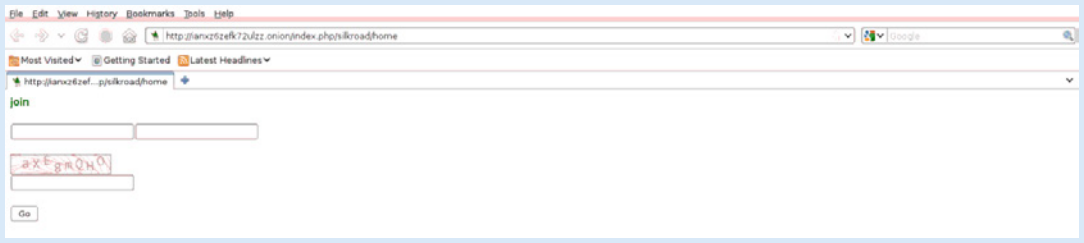
Silk Road was a private listing service visible only to users with approved access. The site relied on feedback and client testimonials in a similar way to eBay, Amazon and other ecommerce websites. Upon successful shipment of products, clients would leave feedback for the seller. Silk Road's simple user-friendly design was one that many people would not have associated with the illicit sale of drugs, however its categories and the images it displayed were evidence of a complex marketplace. Many sellers did not attempt to hide that they were dealing in narcotics (Christin 2012).

Silk Road was successful because it did not retain any transaction details such as purchase and shipment information, or details of buyers and sellers, on the site (Oakes 2011). Like many other online marketplaces, consumers bore the risk of the transaction since Silk Road was an intermediary, and there was no guarantee of a refund should a delivery fail. This in combination with the use of Bitcoins made for an unpredictable environment, with online criminals setting up seller profiles and ripping buyers off (Christin 2012).

To interdict supply, law enforcement agencies disrupted Silk Road's activities by interfering with the major networks it relied on. For instance, any disruption to the TOR software left Silk Road's users vulnerable to traffic analysis; in fact, were TOR disrupted, buyers and sellers would be unable to access Silk Road since it operated exclusively through TOR. Attacks on Mt. Gox would also destabilise Silk Road activities, since buyers did not then have an exchange point for Bitcoins (Christin 2012).

Silk Road's high level of anonymity was a key element in its development. TOR also provided anonymity, while at the same time providing its users with comparatively low latency and a high throughput (McKoy et al. 2008). The use of TOR meant Silk Road clients could access the site through the pseudo-domain '.onion', which can only be resolved through TOR, and consequently would not be traceable by their IP address (Christin 2012). Installing and using TOR and buying Bitcoins involved a certain degree of risk, but those who were willing to take the risk could easily use the website.

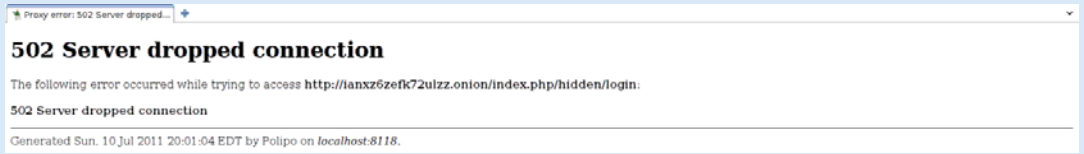
Figure 4: The Silk Road registration page



Source: Gwern.net 2011

On some occasions, the user would see an error page stating Silk Road was down for maintenance (Figure 5); however, after a wait of one or two minutes the user would be redirected to the Silk Road homepage. This was an additional way of protecting the anonymity of the website's users.

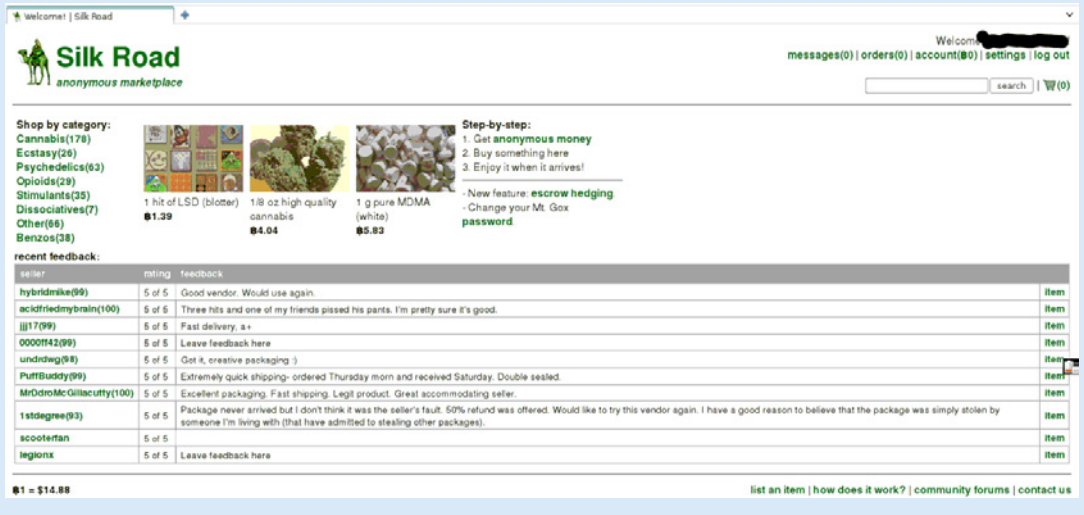
Figure 5: Silk Road error page



Source: Gwern.net 2011

Creating an account as a buyer was a fairly easy process, similar to that of other ecommerce sites. After the account was created, the user could log in and view the products being sold (Figure 6). These ranged from books to clothes and other accessories, but the main products sold were illegal drugs and forged or fake IDs and licenses.

Figure 6: The Silk Road marketplace



Source: Gwern.net 2011

Registering a seller account was a different story. In the website's early days, registering as a seller was the same process as registering as a buyer but, due to anonymous threats, the website procedures were changed and users were required to make an upfront deposit, which was used to pay website fees.

> Not all of the Silk Road listings are public. Silk Road supports *stealth listings*, which are not linked from the rest of Silk Road, and are thus only accessible by buyers who have been given their URL. Stealth listings are frequently used for *custom listings* directed at specific customers, and established through out-of-band mechanisms (e.g., private messaging between seller and buyer). Sellers may further operate in *stealth mode*, meaning that their seller page and *all* the pages of the items they have for sale are not linked from other Silk Road pages. While Silk Road is open to anybody, stealth mode allows sellers with an established customer base to operate their business as invitation-only (Christin 2012).

Since the basic idea behind Silk Road was to maintain the anonymity of both buyer and seller, Silk Road dealt only in Bitcoins, which are useful in peer-to-peer transaction systems that do not involve third parties. Silk Road was historically one of the largest users of Bitcoins.

In order to make a transaction on Silk Road, the user first needed to select what they intended to buy from the listings. Once an item had been selected, the buyer would procure Bitcoins from an online exchange like Mt. Gox; escrow payments were then released to the seller, which acted as a guarantee from the buyer to the seller (Christin 2012). Once the purchase was complete, the seller shipped the product to the buyer. To maintain anonymity, Silk Road advised buyers to have the items delivered to an address other than their residential address. Buyers could leave feedback on the seller's profile once they received their order.

The popularity of, and folklore around, Silk Road facilitated a paradigm shift in the sale of illicit synthetic drugs, particularly for those who wished to purchase small amounts or who lived in rural and regional areas, where traditional access to such substances was difficult. Its closure left a vacuum in the market which, based on market dynamics, will be filled by existing websites and new entrants seeking to profit from this illegal activity. This will impact law enforcement as policing agencies globally attempt to keep pace with changes in supply.

Silk Road 3.0 has appeared online, with a major security overhaul, and is open for business. Silk Road 3.0 has the second largest number of listings and the second most drug listings. ((Black Market Reloaded. Nd)

Black Market Reloaded

Much like its more popular 'brother', Silk Road, Black Market Reloaded (BMR) was a trading platform run through the TOR network. The website was developed and hosted on a black/hidden server and accessed via TOR, meaning it was not accessible from legitimate search engines. Users logged into the site using the TOR browser, as the site did not load from regular browsers like Mozilla, Safari, Internet Explorer or Chrome (Jeffries 2012).

Although Silk Road received a greater share of the media attention around online synthetic drugs, BMR was a larger problem for global law enforcement agencies. All communication between the BMR server and visitors was TOR encrypted, along with any communication between customers and sellers, making it practically impossible to for law enforcement to locate it (Hout & Bingham 2012).

Like Silk Road, the products available at BMR were widely varied and ranged from illicit and prescription drugs to forged identity documents and credit card information. It operated as a mediator between buyers and sellers, ensuring smooth transactions and no scams. Payment was made in Bitcoins exclusively. BMR had a smaller market ratio compared with Silk Road, but its community grew. Although it is impossible to provide an exact figure, it is estimated users of BMR were counted by the thousands and perhaps the tens of thousands. At one point, there were approximately 16,000 new registered members every month, making BMR the fastest-growing illegal store on the dark web. The number and variety of goods offered for sale was astounding, with 5,000 or more individual offers on the site at one point.

BMR and Silk Road were different in a number of ways. For example, Silk Road had a no-trade policy on certain types of illegal goods such as guns, assassinations, different types of data (most frequently credit card

information or counterfeit identity) and several other categories. BMR, as a more open-ended community, allowed trade in all these categories but many users posted on its forums about being cheated by fraudulent sellers. Vendors on BMR commonly offered different types of drugs (either prescription or illicit), illegal material such as child pornography and weapons ranging from handguns and assault rifles to heavy artillery guns and rocket launchers (Jeffries 2012).

Stolen information was extremely popular on BMR, and many users utilised the services of stolen credit card vendors to buy fake identities, forged passports, counterfeit driver's licenses and other documents. There were even several offers of real identities, complete with government-issued passports, identity cards and all accompanying material. Users were most frequently defrauded by vendors offering assassinations. The majority of such offers, which ranged in price from $USD12,500 up, were fake, with half of the sum to be paid in advance. Gullible buyers would pay this advance and the assassin, in most cases, did not complete the contract. Judging by the responses on the BMR forums, this was seen as normal by most users. Many BMR users reacted to the website's notoriety with laughter, and some revelled in that notoriety.

Farmer's Market

Farmer's Market was another underground illicit drug marketplace. Its merchandise included marijuana and ecstasy, among other drugs. The site attracted thousands of users from over 30 nations The US Drug Enforcement Administration (DEA) investigated the Farmer's Market for two years, which culminated in the closure of the site and the arrest of a number of its operators and users. The site ran on TOR to enhance the anonymity of transactions and allowed a number of payment methods, such as Western Union, PayPal, I-Golder and even cash. Between 2007 and 2010, two of those arrested in the DEA's operation managed over 5,200 orders for illicit drugs valued at about US$1m (Central District of California 2012).

A 60-page indictment explains how the operators of the Farmer's Market sold drugs online without raising suspicions. They used a storefront, forums on the internet and a variety of payment methods. It initially operated as Adamflowers, with a secure email service known as Hushmail; the site later moved to TOR. Payments made in cash were via a third party which later sent the money to Farmer's Market. The presence of this third party eliminated any evidence of direct transactions between the site and buyers. In the eight months from July 2010, one of those arrested received about $81,000, mostly via PayPal transactions (Wired 2011).

Pondman

Pondman (www.pondman.nu) and four other chemical distribution websites were investigated by the DEA-led Operation Web Tryp in 2004. Estimates from the DEA revealed unexplained profits of $20,000 per week for one of the websites (US DEA, 2004). The operation investigated internet websites distributing highly dangerous designer-drug analogues under the guise of 'research chemicals' and primarily shipped to the US from China and India. These sites were known to have thousands of customers worldwide and sold substances that led to the fatal overdose of at least two individuals, s well as 14 non-fatal overdoses.

Pondman claimed to be a supplier of landscaping items, fish and pumps. However, the website contained a link that drove page traffic to a section offering a variety of controlled substances. Pondman gained wider attention after the death of an 18 year old client. The operator of the Pondman site, David Linder, was prosecuted following the operation and sentenced to 410 years in prison for a number of offences, including trading in controlled substances (McCandless 2005).

Evidence leading to his arrest included the discovery of the postal address of a company owned by Linder on a package containing the controlled substance 5-Methoxy-N, N-diisopropyltryptamine (5-MeO-DIPT; United States District Court for the District of Arizona 2008).

Untraceable monetary-equivalent payment systems

Online Payments

The internet has revolutionised business transactions. As the number of internet users has grown, so too has the number of online payment options. The ability to pay online has been an essential part of the growth in e-commerce. While all available online payment methods allow the electronic transfer of money from one party to the other, they do so in different ways and provide varying degrees of anonymity and trust. These payment options require users to have accounts or to use electronic currency.

The proliferation of online payment methods has also assisted in the growth of the online illicit drug economy. While traditional payment methods—especially credit cards—are widely used in online transactions, the unique aspects and demands of online commerce (namely, the need for real-time value transfer and customer-not-present transactions) have placed pressure on these methods. And, just as in the offline world, trust in the financial service or instrument is essential to the large-scale adoption of that product.

Paypal

The concept of protecting one's online financial identity from the entity one is transacting with is considered to be responsible for PayPal's growth as an online payment method. But although those transacting online do not have access to each other's details, it is wrong to assume the transaction is anonymous. Far from it: PayPal maintains records of all transactions as well as the corresponding bank and/or credit-card accounts associated with the PayPal account as well as detailed computer identifiers, all of which can be supplied to law enforcement agencies upon lawful request.

PayPal has its own policy on anti-money laundering which is available on their website; their *Anti-Money Laundering and Counter-Terrorist Financing Statement* forms part of their customer agreement and also commits PayPal to preventing the financing of terrorism or other illegal or suspicious activities through its online accounts. This policy (and related systems) has made it very difficult to use PayPal accounts to launder money. Thus, PayPal is not a trusted solution for online criminal enterprises; criminals use it at their own peril.

Credit cards

The traditional banking system has been slow to catch up with the concept of anonymous online transactions, although some credit card companies have enhanced buyers' privacy by issuing distinct card numbers for specific transactions. This prevents sellers from knowing the real identity of a buyer. Again, records of such transactions are maintained and accessible by police.

Most online credit card transactions are made by providing the card details (card number, expiry date and the three-digit security number on the back of the card). The transaction reaches the trader's server, relaying the credit card information for authorisation by the merchant account provider. Once approved, data is transmitted to the issuing bank, which transfers money from the customer's account into the trader's account through an automatic clearing house. The ecommerce site then forwards details of the success or failure of the transaction to the customer.

Credit cards suffer from a trust issue with merchants: 'card not present' fraud—that is, fraud carried out against online merchants where the card is not physically present—is a significant risk to online merchants, with criminals using stolen card data to conduct transactions. By the time the merchant learns of the fraud by way of chargeback, they have provided the goods or services to the bogus customer.

Cash

As the saying goes, cash is king and has been the traditional form of currency of illegal purchases. Cash payments enable buyers of certain goods to hide their identity, which is why cash dominates many offline criminal businesses—but cash is not easily transferred online and works best in a face-to-face environment.

International money transfers

International money transfers, or wire transfers, through firms such as Western Union and Moneygram are a faster and more trusted alternative to physically moving large amounts of cash around the world outside the mainstream banking system. International wire transfers address many of the problems of cash payments.

Wire transfer services are a legitimate way of transferring money to anyone worldwide. Unfortunately, the system has had its share of difficulties with illegal activities. It is frequently used by criminals and money launderers because of the anonymity it offers, as money can be sent anywhere through one of its offices or over the internet with little information needed.

Despite government efforts to ensure such services are not used for money laundering and the like, wire transfers are clearly seen as a less-regulated part of the financial system than mainstream banks. To be fair, Western Union has made some effort in this space, but these are unlikely to make a tangible difference to the level of criminal abuse of the system. As a consequence, wire transfers are still used by criminals and remain the payment method-of-choice for international scammers.

Virtual payment systems

The demand for anonymous online payments has led to the development of virtual payment systems and virtual currencies enabling anonymous payment. Virtual currencies may not require transactors to provide identification and validation, which prevents law enforcement agencies from tracing money transfers to offenders. The use of such anonymous currencies by criminals restricts the ability of law enforcement to identify suspects by tracing money transfers—for example, in cases related to illicit synthetic drugs.

Money transfers are relatively unregulated, and the internet offers offenders the possibility of cheap and tax-free money transfers across borders. The use of virtual currencies and the existence of online casinos presently cause difficulties in the investigation of internet-based money-laundering techniques.

Peer-to-peer transactions (discussed below) have become much more prevalent in recent years. They make for a potentially troublesome scenario. Peer-to-peer transactions involve the transfer of funds from one person to another, either via the internet or mobile phone, without the involvement of a bank or financial institution. The system leaves itself open to abuse by operating in this manner; it becomes very easy for criminals to conduct illegal activities, like money laundering, without fear of detection.

Mobile Online Payment Systems

Mobile payment transactions can take place in a number of ways. These include:

- through a carrier-based system where a user purchases an item or service using a wireless device and each purchase reflects on the bill, such as a credit or debit billing service;
- a customer may use their mobile phone to access funds, with the phone acting as the card since the details are within the phone; or
- a user may transfer funds to different accounts or pay bills through remote access.

These processes require the user to authorise transactions before the account-holder's bank initiates the transfer; the bank communicates with an individual using short message prompts. There are many providers of mobile online payments, with some requiring registration before access.

Payments using short text messages use a wireless network that connects the mobile device to the service provider and the financial institution. Upon issuing a payment prompt using a code, the service provider sends a message back requesting confirmation of the transaction before proceeding. This ensures only the owner of the phone can initiate payments since the confirmation requests an identification password. When approved, the service provider sends a message to the trader.

The proliferation of smart phones and tablet devices will see a jump in the use of these technologies to make payments, with devices able to seamlessly integrate with online payment methods such as PayPal and Google Wallet.

Near field communication

Near field communication (NFC) allows two electronic devices to transfer data between one end of the communication channel to the other, at close range. This technology enhances payment and ticketing services. NFC technology is also popularly used to verify identity and for access (as a door key). NFC payments using mobile phones require a microchip installation in the phone. The phone must be within 10cm of the reader device for communication to take place.

The service requires the use of a specific app provided by the service provider or financial institution and customised with the consumer's details. Companies and individuals are increasingly turning to NFC technology as it provides contactless communication. The technology is increasingly used in chip and pin credit cards. It allows for purchases of up to $100 to be made without the use of a PIN. Examples include:

- payWave—used for Visa cards where the card is held in close proximity to a Point of Sale machine.
- PayPass—used for MasterCard cards and operates in the same way as PayWave.

Interestingly, encryption is used for every purchase, protecting the transaction and card data. These two products are also being used on mobile smart devices and are in competition to other near field payment channels such as Apple Pay, which links a user's credit card to their Apple smart device.

Electronic cash

Offerings such as paysafecard, store gift cards and pre-paid credit cards, provide the ability to pay for goods and services anonymously online, outside the mainstream banking system. While all require some form of physical interaction at the initial point of sale, the verification and 'know your customer' regime at a convenience store or supermarket will invariably be less robust than one carried out at a banking institution. Furthermore, by establishing the account using cash, another means of identification and control is removed from the system.

Virtual Currencies

Micropayments were a key driver of the development of various virtual currencies, making the use of credit cards problematic. With the growth of micropayments virtual currencies, including 'virtual gold currencies', were developed.

E-gold

The first such virtual currency, known as e-gold, was founded in 1996. Virtual gold currencies were account-based payment systems. The value of the virtual currency is allegedly backed by gold (or other precious metal) deposits. Users could open e-gold accounts online, often without registration. Some providers even enabled direct peer-to-peer transfers or cash withdrawals. E-gold permitted users to exchange money for precious metals like gold and silver, which the company deposited in various financial institutions.

E-gold permitted users to withdraw money in any currency, making this system viable for transfers between account holders in different parts of the world. The process involved depositing money into an e-gold account, to be subsequently withdrawn by the recipient in any currency. Due to lax account creation and authentication procedures, e-gold became an anonymous way to send and receive money. Speedy transfer required two consenting parties.

E-gold was originally a digital gold currency company operated by Gold & Silver Reserve Inc. The proprietors were indicted by the US Department of Justice in 2007 on four counts, including money laundering. In 2010 e-gold reopened to users who already had accounts, on the condition that users submit additional information, under the oversight of a court-appointed claims administrator and the US government. Users able to adequately verify their identity were provided with refunds. Following the initial success of e-gold, a rash of similar companies and schemes were established including e-silver, e-platinum and so on.

Bitcoin

Bitcoin is an online currency and software that offers worldwide payments, instant peer-to-peer transactions and very low processing fees. Bitcoins are issued by the network and the system itself operates without any central authority. The software is community-driven and developed by open-source programmers. The Bitcoin economy is highly volatile, with a history of strong fluctuations. National currencies can be exchanged for Bitcoins via dedicated web services. Bitcoin purchasers buy a specific unit of coin depending on the amount they wish to spend (Nakamoto 2009).

Bitcoin is a cryptographic protocol that creates unique pieces of digital property that can be transferred from one person to another. The protocol also makes it impossible to double-spend a Bitcoin, meaning you can't spend the same Bitcoin twice. As well as having a unique digital fingerprint, Bitcoins are also listed in a public ledger of all Bitcoin transactions known as the blockchain. The blockchain is maintained by a distributed network of computers around the world. Transactions are conducted using the public keys—a cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient—the identities of the buyers and sellers are veiled to each other and to the public, even though the transaction is recorded publicly (Grant 2014).

The process may be explained like this: Person A receives 20 Bitcoins from a Bitcoin address where they have publicly advertised for donations. Anyone can find Person A by looking at the blockchain - a public ledger of all Bitcoin transactions that have ever been executed - in a search engine. If Person A wants to buy drugs with their 20 Bitcoins, and the drug dealer's Bitcoins are subsequently traced, they will point back to Person A.

Person A could create several different accounts and pass their 20 Bitcoins through those accounts before finally going to the drug dealer. Chances are, however, the trail would still lead back to Person A because those accounts have not been used for anything else.

Suppose Person A puts the 20 Bitcoins into an account created by a laundering service. Then Person A and Person B do the same thing. The service sends the 20 Bitcoins to Person B and your coins to person A, who then spends the money on drugs. Now the trail looks the same as the above scenario, except the trail leads to you instead of person A.

The Bitcoin network involves a number of people who devote server space to the data collected by Bitcoin online payments. When a user makes a transaction on the Bitcoin system, these volunteers—also referred to as miners—receive information and crack cryptographic messages resulting from the transaction. The fastest miner is paid in Bitcoins which can be redeemed in any currency. The number of miners makes it hard to trace transactions, as the information is encrypted. The transfer of information across different servers also limits third-party interference, as any third party would need to understand the secret codes to hack into databanks.

Peer-to-peer transactions such as those involving Bitcoins have become much more prevalent in recent years and could potentially be problematic. Peer-to-peer transactions involve the transfer of funds from one person to another, either via the internet or mobile phone, without the involvement of a bank or financial institution,

a system vulnerable to abuse and one that has the potential to be exploited by criminals engaged in illegal activities like money laundering, without any fear of reprisal or detection (Strauss 2012).

A major disadvantage of this payment option is consumer uncertainty. The Bitcoin environment is unpredictable and there is no dispute-resolution mechanism. If sellers fail to ship products after receiving payment in Bitcoins, the buyer shoulders the loss. Bitcoins are difficult to track as almost no information is associated with transactions, and the lack of third-party control means rogues can transfer money into Bitcoins without revealing their identity. In addition, there are no regulatory guidelines around the use of Bitcoins as there are around other virtual currency payments (FBI 2012).

Bitcoin provides ecommerce with a currency that financial institutions and the government cannot regulate. There are more than 15 million Bitcoins in circulation (with a believed cap of 21 million) and the total worth of the currency is over US$5b.

Factors that control acceptance of online payments

In online transactions, parties on both sides must form a relationship of trust. From the merchant's perspective, details pertaining to the transaction should remain private while, on the buyer's end, personal information used in the transaction should not reach third parties. Online consumers are wary of leaving personal information within easy reach for fraudsters. Merchants also desire assurance that the funds paid are 'real' and will not be reversed; buyers desire assurance that the merchant will supply the goods or services upon receipt of the funds paid.

Online payment methods should have clear dispute resolution mechanisms. Some online payment methods such as PayPal have efficient dispute resolution mechanisms; others offer none and complainants must address grievances in court.

Money laundering and online casinos

Those involved in drug distribution networks use the internet to facilitate money laundering in various ways. Virtual gambling sites and online casinos, for example, are becoming extremely popular and, while they provide entertainment for some, for others they are an opportunity for money laundering and other illegal activity.

It is very easy to create accounts for online casinos, requiring only an unverified name and email address. Those who register often use a PayPal account or a credit card to pay for chips. In order to launder money via online casinos, a person can open several different accounts in fictitious names. The accounts are funded with money gained by illicit means. The person can buy and sell using these accounts as if they were making purchases from others. They may also direct the proceeds to an account from which they can withdraw the funds from either the bank or ATM. It would be almost impossible to trace the origins of the funds.

Hackers have been able to install malicious code and keystroke loggers onto the computers of players; the accounts of these players have then been hijacked and all of their game assets sold off. This problem is common on many of the virtual gambling sites around the world; players are taking a risk when they sign up to these sites. Most gambling sites operate in jurisdictions which have weak or no legislation to regulate their activity.

Social networking and promotion

Teens and young adults are consistently those most likely to go online, even as the number of internet users has grown (and despite great increases in use by certain age cohorts, such as those aged 65 and older; Lenhart et al. 2010). Negative public depictions of drug users contribute to their ongoing stigmatisation and marginalisation; this may drive young people to the internet to research and source illicit synthetic drugs.

Those whose uptake of internet technologies is highest are also those most likely to use party drugs. The 2007 National Drug Strategy Household Survey (NDSHS) revealed 28 percent of Australian adults aged 20 to 29 had used some type of illicit drug in the previous 12 months, compared with 17 percent of 14 to 19 year olds, 17 percent of 30 to 39 year olds and seven percent of those aged 40 or older. The 2013 NDSHS revealed 42 percent of people in Australia had illicitly used a drug at some point in their lifetime.

Compared to teenagers that spend no time on social networking sites in a typical day, teens that do are five times likelier to use tobacco, three times likelier to use alcohol and twice as likely to use marijuana (CASA 2011).

One of the primary benefits of the internet, especially with regard to the distribution of illicit substances, is the ability for users to maintain online anonymity (or, at least, to perceive they do). One of the most common ways to avoid internet surveillance is to use a public-access computer in a library, cybercafe or school. Discussions on illicit drug-related web forums often advise users never to post incriminating personal details from a home computer, as IP addresses can be identified by law enforcement agencies should they decide to conduct an investigation.

A hashtag search on Instagram can find a broad array of illicit synthetic drugs, be it stolen, extracted, grown, prescribed, synthesised or harvested. Whilst the transactions don't happen on Instagram, the advertising does. Those advertising 'brand name' illicit drugs use pre-paid phones and web-based email accounts to interact with potential buyers.

Illegal internet pharmacies use social media to promote their websites. This puts many people, particularly young people, at risk of accessing potentially dangerous products. Social media embraces web and mobile technologies to facilitate interactive communication between individuals, communities and organisations. The use of social media has grown exponentially. One of every seven people in the world has a Facebook page and nearly four in five active internet users visit social networks and blogs. As of January 2016, there were 15 million Australian Facebook users or accounts (approximately 62% of the population).

Part B: Drug offending facilitated by the internet

Illicit Synthetic Drugs

In the context of international drug control, a drug is any of the substances listed in Schedule I and II of the *Single Convention on Narcotic Drugs* (UNTC 1961), whether natural or synthetic. The United Nations drug control conventions do not distinguish between licit and illicit drugs; they apply the terms licit or illicit to the use of drugs, rather than to substances. Illicit drugs are drugs which are under international control, which may or may not have licit medical purposes but are also produced, trafficked and/or consumed illicitly.

The *Convention on Psychotropic Substances* (UNTC 1971) brought synthetic substances, amphetamine-type stimulants (ATS), sedative-hypnotic agents and hallucinogens into the public policy arena. The UN and its member states have acknowledged the risk posed by synthetic drugs—a risk which has increased due to the number of outlets where clandestine chemists can purchase precursor chemicals and laboratory equipment and the availability of detailed chemical descriptions and manufacturing instructions on the internet.

In March 2013, the International Narcotics Control Board announced new psychoactive substances (NPS) were the fastest-growing category of drugs in the world and identified more than 1,000 compounds that had entered the market since 2008 (Dwoskin 2012). A global assessment of amphetamine, methamphetamine and ecstasy revealed annual use of these drugs exceeds that of cocaine and heroin combined; the combined global wholesale and retail market in ATS is estimated at US$65b (UNODC 2008). Illegal drugs generate considerable profits. The single most lucrative sector of the illicit drug market is international drug trafficking. The profits generated by trafficking groups are used to fund other criminal activity and political insurgency (UNODC 2007).

Australia is a popular market for imported illicit synthetic drugs. Australians pay more: in 2011–12, the price of a gram of amphetamine in ranged from $150 to $800, compared with between $150 and $400 in 2010–11. The price for a kilogram of crystal methamphetamine ranged between $200,000 and $330,000 in 2011–12, compared with $120,000 to $350,000 in 2010–11. The price for a single tablet of MDMA, however, remained relatively stable; in 2011–12, a single tablet of MDMA cost between $20 and $60, a high price by European standards. Interestingly, over the last decade, the median purity of amphetamine in Australia has fluctuated greatly, ranging between 0.1 percent and 71.4 percent (ACC 2002).

Synthetic drugs often have properties and effects similar to known hallucinogens or narcotics but a slightly altered chemical structure, and may be developed to evade restrictions on illegal substances. Such products are often packaged as ‘incense’ or ‘bath salts’ and can be obtained for as little as $10 in a number of online forums and marketplaces. In the US, the most common ingredients of bath salts are 3,4-methylenedioxypyrovalerone (MDPV) and 4-methylmethcathinone (mephedrone). MDPV is a dopamine and norepinephrine reuptake inhibitor with no approved medical use. Mephedrone is a derivative of phenethylamine that increases serotonin, norephinephrine and dopamine and is similar to cathinone, which in turn is similar to some amphetamines (Van Pelt 2012). Another kind of ‘designer drug’ is synthetic cannabinoids, also known as synthetic marijuana. These mimic the effects of delta-9-tetrahydrocannabinol (THC), the primary psychoactive constituent of marijuana, and are often sold as herbal incense products (New York State Department of Health nd).

Illicit synthetic substances that mimic the effects of other drugs such as marijuana and cocaine can make users seriously ill, causing seizures and hallucinations and, in some cases, death. As more drug users experiment with them, the results have become evident at hospitals: there has been a sharp spike in the

number of users presenting with problems ranging from labored breathing and rapid heartbeat to extreme paranoia and delusions, and these symptoms can persist for days (New York State Department of Health nd).

The manufacture and trafficking of synthetic drugs such as amphetamine, methamphetamine, ecstasy and LSD is a global and constantly changing phenomenon. The internet plays a large role in the marketing of these drugs and is a platform for this type of crime (Interpol nd). The popularity of the internet makes it difficult to control or limit the production, sale and use of illicit drugs. Internet users can learn how to produce, use and buy drugs from the comfort of their homes. An (admittedly small) survey of 100 adult drug-dependent inpatients in a residential drug treatment program found 29 percent knew they could use the internet to purchase drugs, while 11 percent reported they had used the internet to buy drugs or find a drug dealer (Interpol nd). A 2007 survey of young internet users found 23 percent had searched the internet for information related to drugs and/or alcohol (Interpol). Both these studies are relatively dated, particularly in relation to the internet, and the increased pervasiveness of the online environment in society would suggest these figures have increased over time.

The internet not only makes it easier to acquire synthetic drugs; some websites also promote synthetic highs and direct new users toward drug experiences. Synthetic drug users share their highs and other experiences on various forums, accelerating new users' learning curves on synthetic drug use (Van Pelt 2012). The illicit synthetic drug supply chain involves obtaining precursor chemicals and equipment from various sources. The necessary chemicals may not necessarily be proscribed until they are mixed together to form the illegal substance (Cherney et al. 2005). Identifying those who operate synthetic drug sites can be difficult. Anyone who wants to hide their association with a website can register a domain without revealing their identity, or use a domain privacy service. Such privacy services, for example TOR, specialise in concealing the identities of internet users (Oakes 2011).

GHB and analogs

Gamma-hydroxybutyrate or GHB is a central nervous-system depressant and a popular club drug most commonly used by teenagers and young adults. GHB is also known as liquid ecstasy, soap, scoop, Georgia homeboy, grievous bodily harm, liquid X and goop. Some amateur chemists obtain much of the manufacturing information and precursor chemicals they need from the internet. Although GHB is available on the internet, most of the products sold on the Internet as GHB are actually GHB analogs—drugs with chemical structures closely resembling GHB. Some internet vendors sell GHB kits, which contain two chemicals: gamma-butyrolactone or GBL, a GHB analog, and either sodium hydroxide or potassium hydroxide. When combined, these produce GHB. Other sites sell both chemicals, but not as a kit. Other GHB analogs like 1,4-butanediol (BD), gamma-hydroxyvalerate (GHV) and gamma-valerolactone (GVL), are also sold. When ingested, these analogs are either metabolised to GHB in the human body or have physical effects similar to those of GHB. GHB analogs are often marketed as nutritional supplements, or as household products like nail polish remover. Many suppliers promote GHB or its analogs as a muscle-growth supplement and advertise bodybuilding supplies and health supplements along with these chemicals (US Department of Justice 2008).

Illicit synthetic drug manufacture

Drug precursors are chemicals used in the manufacturing of illicit synthetic drugs. Many precursors are widely used in the global chemical industry to produce a variety of legitimate products but, due to their possible use in illicit synthetic drug production, are regulated by government.

Within Australia, the diversion of cold and flu tablets containing pseudoephedrine for the manufacture of methamphetamine is a significant concern, and illicit internet pharmacies are a global problem requiring international action. A number of websites sell drug components and precursors—for example the precursor compound GBL, which as explained above is rapidly metabolized in the body to GHB. Other websites

provide information on how to identify, cultivate or buy plants and fungi containing high concentrations of psychedelic alkaloids, such as DMT or psilocin, and refine or prepare them for ingestion. Some sites, such as Shamanic Track (http://deoxy.org/shaman.htm) even offer travel advice for locations where hallucinogens can be obtained and experienced. Many of these sites offer a variety of products including seeds, herbs, plant extracts and growing supplies.

Precursor chemicals

Precursor chemicals are essential to the manufacture and processing of illicit synthetic drugs. For example, methamphetamine is made using precursor chemicals like ephedrine and others, like anhydrous ammonia, pseudoephedrine and red phosphorous, illegitimately diverted from legal sources (Roll et al. 2009).

The diversion of narcotic drugs, psychotropic substances and precursors from licit domestic distribution channels is the main supply for illicit markets. Narcotic drugs and psychotropic substances are diverted mainly in the form of pharmaceutical preparations. Ephedrine and pseudoephedrine are trafficked for use in the illicit manufacture of ATS (INCB 2012). The dichotomoy of licit and illicit applications of the same chemical makes control of these substances difficult. Supply is necessary for legal use while, at the same time, diversion for illicit drug production must be prevented (Roll et al. 2009). As a result, governments worldwide have placed strict restrictions on the purchase, importation and sale of precursors to reduce the possibility of diversion. Monitoring and controlling precursors and other chemicals used in illicit drug manufacturing is key to reducing drug abuse (Walters et al. 2009). Preventing the theft and/or diversion of precursor chemicals for illegal use requires the cooperation and coordination of all those affected, whether directly or indirectly, not just policymakers.

Online sale and supply of precursor chemicals has increased due to insufficient security measures, as well as increased awareness of the supply chain, wider availability, easy public access and ignorance (Commission of the European Communities 2010). The production and trafficking of synthetic drugs including methamphetamine, amphetamine, lysergic acid diethylamide (LSD) and ecstasy has been a constant and global phenomenon. Due to the synthetic nature of the products—with precursors traded legitimately internationally, unlike plant-based illicit substances like heroin and cocaine—the manufacturing base is not limited to any particular geographical zone and ranges from large-scale commercial laboratories to small sole-use operations.

A total ban on the public sale of precursors via the internet could impact on production, as could labelling precursors to indicate that purchase of the chemicals is subject to legal definition and registration. The government should develop a system that forces verification of a buyer's identity, as most purchasers at present remain anonymous (Hanson & Venterelli 2011).

Criminal groups have responded to legislative changes that make it more difficult for traffickers to divert ephedrine and pseudoephedrine in Australia by modifying and adapting the ATS manufacturing process. In 2010–11, Australian authorities detected 702 illicit laboratories, the largest number ever (INCB 2012). In April 2011 Australian law enforcement dismantled an organised crime syndicate in Sydney and seized the largest quantity of safrole in Australian history—more than 2,800 litres of low-concentration safrole oil, which had been falsely declared as liquid hair products and cleaning products originating from China. The overall safrole content equated to approximately 288 litres of pure safrole. This is enough to manufacture of 2.3 million ecstasy tablets (INCB 2012).

Legal highs

New synthetic psychoactive substances that are chemically engineered to avoid international controls are increasingly being used by Australian drug users. Many countries, particularly in Europe, North America and Oceania, have reported the use of such substances as an emerging trend. The most notable of these

substances included the methcathinone analogue 4-methyl-methcathinone (also known as mephedrone) and methylenedioxypyrovalerone (MDPV), which are often sold as bath salts or plant food (UNODC 2012).

Synthetic drugs exist in a legal grey area because manufacturers tweak their recipes to circumvent illegal drug classifications and national drug control legislation. A new synthetic drug emerges in the European market every week and hundreds come into Australia. Legal highs are a growing international concern and authorities are increasingly challenged by the emergence of new ATS analogues, which mimic the effects of MDMA or ecstasy and methamphetamine.

The increasing prevalence of legal highs poses serious challenges for Australian health, law enforcement and regulatory agencies due to the large number of substances available, the confusion around their legal status and the complexity involved in their manufacture and supply; it is also a notable trend in terms of developing drug abuse patterns. While cannabis is still the illicit drug of choice in the region, evidence suggests that new ATS drugs are becoming more popular among younger age groups (INCB 2012).

The addition of these substances to the traditional illicit drug catalogue of ATS, cannabis, heroin and cocaine has changed the global illicit drug market, with an increasing number of users reporting drug analogues and novel substances as their drug of choice. Governments worldwide face the challenge of bringing new psychoactive substances under national control. These substances are often difficult to identify in a timely manner, given how quickly the new substances enter the market, their inconsistent chemical composition and the lack of technical and pharmacological data and reference material available on them, along with a lack of sufficient forensic and toxicological capacity in some jurisdictions.

A number of Australian jurisdictions have implemented reforms to address the potential harms associated with these emerging substances. Recommendations include the banning eight 'families' of synthetic drugs, making it easier for police to prove a synthetic drug is illegal and allowing the NSW Minister for Fair Trading to issue snap six-month bans on the sale of products (Olding 2013).

Other illicit drugs

Marijuana

Many internet sites sell marijuana seeds, cultivation kits and paraphernalia, or provide very detailed information about cannabis cultivation. Some also offer free seed samples or provide detailed information about how to smoke or inhale marijuana (via joint, pipe or vaporizer) and instructions on how to roll various types of joints (Interpol 2008).

The drug paraphernalia advertised for sale on the internet are marijuana related. Most paraphernalia are disguised as everyday items, sometimes by using an ordinary object as a shell. Some of the most popular drug paraphernalia sold online are 'stealth pipes' or 'incognito pipes,' which look like ordinary copper tubing or household plumbing fixtures but are made to conceal or administer drugs. Other pipes resemble lip-balm containers, highlighters, markers, lipstick cases, miniature flashlights, cigars, bullets, cigarette lighters, key chains, cigarette packs, makeup brushes and mascara tubes. Some sites feature instructions for making drug-use paraphernalia. Some sites featureg bong designs, with detailed instructions for making various types of bongs using household items such as mason jars, glass bottles, toilet paper rolls, PVC pipes or tin foil (US Department of Justice, 2008).

MDMA

MDMA—also known as ecstasy, E, X, and Adam—is a stimulant and low-level hallucinogen. It is popular among teens and young adults and commonly used at raves and dance clubs. MDMA use is promoted and glamorised on many internet sites and bulletin boards where users discuss their MDMA experiences. Drug

legalisation and club or party sites often describe MDMA as a relatively benign drug with few negative side effects, although it is a dangerous drug that can cause severe hyperthermia (overheating), dehydration and, occasionally, death.

There is an abundance of information on the internet about the manufacture of MDMA, and many rave-culture participants access this information or share it in chat rooms. Manufacturers use the internet to identify suppliers of precursor chemicals, obtain recipes and instructions on MDMA production, and discuss production processes with other users. For example, the US DEA arrested two chemistry doctoral students, one in Georgia and one in Arizona, who had used instructions found on the internet to produce MDMA, methamphetamine and precursor chemicals; the students communicated with each other about their progress via email (Us DoJ 2008).

Psilocybin/psilocin

Hallucinogenic psilocybin mushrooms are also known as magic mushrooms. Although the chemicals psilocybin and psilocin, and the mushrooms that contain these chemicals, are illegal, the spores necessary to grow the mushrooms are not. Therefore psilocybin mushroom spores can be legally purchased on the internet. Complete growing kits and the supplies required for harvesting the mushrooms, including detailed instructions, can be easily purchased online.

LSD

LSD —also known as acid, boomers and yellow sunshine—is a hallucinogen used by both young and old. Although LSD synthesis is a complex chemical procedure that requires the knowledge and skills of a trained chemist, recipes for making LSD are readily available on the internet. There are also bulletin boards andr newsgroups where people can communicate with one another about LSD. In these forums, users share information by posting 'tripping' experiences and exchanging tips regarding the best ways to ship and distribute the drug to avoid detection by law enforcement. Bulletin boards and chat rooms also are used to arrange LSD sales.

Heroin

High-purity heroin that can be snorted or smoked rather than injected is becoming popular among middle- to upper-class teens and young adults. Seeds for growing opium poppies are sold on the internet and information on opium poppy cultivation and extraction of raw opium is also available. Most information available on the internet about heroin use relates either to snorting or to injecting, with injecting being the method most endorsed. Heroin is dangerously addictive and, in some cases, deadly; it is promoted for use in 'coming down' from the effects of MDMA after raves and to provide relief from stress and physical pain (US Department of Justice 2008).

Cocaine/Crack

Cocaine use is often glamorised and information about its use is readily available on the internet. Information about cocaine use is promulgated through chat rooms, bulletins or newsgroups that specifically discuss the different ways powdered cocaine and crack cocaine can be used such as snorting, injecting, smoking or ingesting it. Information on a multitude of related topics can be found, including dosage levels, legal considerations, the history of cocaine use, the differing psychological and physical effects of using powdered cocaine and crack cocaine, and the best paraphernalia to use for snorting, injecting, or smoking cocaine. There are instructions for converting powdered cocaine to freebase or crack cocaine and, in addition, online services that provide information on crack cocaine dealers in major metropolitan areas. Cocaine price and purity reports for most states can also be found online.

The use of the internet to facilitate the production, sale and use of illegal drugs is likely to increase as its influence expands, particularly as smart phones and tablet devices are increasingly utilised by teens and young adults and new technologies are developed. As the number and proficiency of users grows in coming years, drug-related threats to young internet users can also be expected to proliferate (Us Department of Justice 2008).

International Trends

The popularity of synthetic drugs has become a global issue.

Asia

Asia continues to be a manufacturing hub and a growing illicit market for ATS, particularly methamphetamine. Seizures of methamphetamine in East and South-East Asia accounted for almost half of total global seizures in 2010. Since then, most countries in the region have reported increasing seizures of methamphetamine. Furthermore, evidence shows the illicit manufacture of ATS has expanded from traditional manufacturing countries such as China and Myanmar to Cambodia, Indonesia, Malaysia, the Philippines and Thailand. Substances used in the illicit manufacture of ATS such as ephedrine and pseudoephedrine continue to be trafficked in the region in large quantities (INCB 2012). Control of precursor trafficking in East and South-East Asia is a challenge, particularly of pharmaceutical preparations containing ephedrine and pseudoephedrine.

New psychoactive substances, including substances not under international control such as ketamine, are gaining popularity in the illicit markets of East and South-East Asia. The Republic of Korea has reported the seizure of products containing synthetic cannabinoids sold under the brand name ‘spice’ and products containing MDPV sold as ‘bath salts’. These substances are increasingly smuggled into the country by mail and used as substitutes for cocaine or ecstasy (INCB 2012).

D-methamphetamine hydrochloride and methamphetamine are commonly available in East Asia. Trafficking groups operating in South Korea, Taiwan and the Philippines, as well as Japan, are the main suppliers of illegal synthetic drugs to local markets and amphetamines are often their main commodity (CIA 2011).

China has attempted to control the sale of precursor chemicals over the internet and has strict laws and restrictions around online transactions involving precursor chemicals (Brownfield 2011), but these efforts have not prevented the advertising of precursor chemicals on websites, blogs and social networking sites. India, too, is a potentially significant transhipment country: its proximity to regions where drugs are traditionally grown and its increasing industrialisation (and associated potential for the diversion of precursor chemicals) add to the problem.

In March 2012, Royal Malaysian Customs officers seized 73 kilograms of methamphetamine from a shipment of roses in Ampang, in the province of Selangor (BSI 2012).

Europe

Abuse of illicit drugs in Europe has remained relatively unchanged in recent years, although it is at high levels. The emergence of new psychoactive substances—so-called designer drugs or legal highs—poses a major challenge.

Mephedrone accounts for an increasing proportion of the illicit drug market in some European countries. Although not regulated internationally, mephedrone is controlled in most EU member states; yet it continues to be offered for sale on the internet, although on few sites and at high prices. In 2010–11 over 120 websites in the UK that advertised mephedrone and naphyrone were closed down. In 2010, mephedrone was the most frequently seized synthetic substance in Hungary, and an increase in the prevalence of users injecting mephedrone and other cathinones was reported during 2010–11 (INCB 2012).

The number of internet-based retail sites selling psychoactive products that ship to EU member states increased from 170 in January 2010 to 314 in January 2011 and 690 in January 2012. About a third of these were hosted on servers in the United States and a fifth of them on servers in the UK. About two thirds of the sites identified post a disclaimer or product warning, and such sites are increasingly introducing measures to restrict access and protect the identity of buyers and sellers (INCB 2012).

The Netherlands is the major source of amphetamines in the EU, although laboratories have also been discovered in countries like Britain, Germany, Belgium and France (Bryan 2009).

North America

North America is the biggest illicit drug market in the world and has the highest reported drug-related mortality rate. As in other regions, North American traffickers continue to develop designer drugs, the chemical composition of which is engineered to prevent them from falling under existing control regimes for substances with analogous properties. The two categories of designer drugs most commonly abused are synthetic cathinones and synthetic cannabinoids (INCB 2012).

Illicit large-scale methamphetamine manufacturing continues to expand in Mexico, with falling prices and increased purity levels spurring the increased availability of the drug in the US. Illicit drug manufacturers in North America have continued to innovate in developing substances (such as Khat) and circumventing existing controls on the ingredients required for manufacture. New psychoactive substances, marketed as spice, plant food, bath salts and so-called legal highs, which have effects analogous to cannabis, ecstasy and amphetamines, are increasingly available through commercial outlets and on the internet (INCB 2012).

Mexican trafficking groups on the west coast of the US have been implicated in the production and distribution of methamphetamine. Recently the production of methcathinone, which is reportedly stronger than methamphetamine, has become widespread in the US (Isralowitz & Myers, 2012).

Canada, though a primary consumer of synthetic drugs, also produces such drugs. Precursor chemicals are regularly used to produce drugs, often drugs that are controlled in the US but not regulated in Canada (Room & Pagli, 2009).

The expansion of criminal groups engaged in the production and trafficking of illicit synthetic drugs often starts with the trafficking of precursor chemicals (CIA 2010). Illicit synthetic drug users use the internet to exchange information on illicit drug use and its benefits and, hence, production increases.

The manufacture of synthetic drugs—mainly amphetamine and methamphetamine—is growing rapidly in the US (CIA 2010). There are many laboratories in the US; however, Canada is still at the forefront. Many of these drug labs are controlled by Asian organised crime groups (Glenny 2009).

Canadian law enforcement efforts have reduced the amount of ephedrine, pseudoephedrine and other precursor chemicals available via the internet, but the problem still exists (Hendley 2010).

Part C: The current study

Detecting illicit drugs on social media using automated social media intelligence analysis

The analysis addressed in this section was conducted by Dr Paul Watters. While traditional crimes adapt to technology, the technologies themselves also increase in scope and reach. Web 2.0 technologies, including social media—often accessed by mobile devices—have radically transformed the user mix and the functionality available to them. It is essential to consider how social media technologies could be used to enhance criminal activity online and could include an investigation of how illicit drugs are being openly traded on social media.

In addition to understanding how the gathering and analysis of social media source material could be automated to assist in the detection of illicit drug trading, the analysis considers how individuals and criminal organisations targeting a specific country might better be identified by making use of social media connectedness (which is also an asset to organised crime organisations) to identify those who may be buying or selling illicit drugs locally. The Automated Social Media Intelligence Analysis (ASMIA) methodology was applied to two different but related problems to better understand how social media is being used in the illicit drug trade, especially for advertising and distribution.

ASMIA works by either passively monitoring or actively searching a number of sources using query terms constructed from noun and verb phrases which are combined to form terms. When a term returns a hit, the hit may relate to a target (such as an individual, organisation or drug). The algorithm applied can be described as follows (with examples related to illicit drug trade detection).

- Identify the data source(s) to be monitored, eg Google ads, Facebook ads, Google search, Facebook profiles, Pipl. Determine whether the data source is better suited to passive monitoring or active searching. For example, a sample of Google ads can be continually regenerated by repeatedly refreshing a search.
- Develop a list of terms to be searched or monitored. A term list might be a list of targets—such as individuals, groups or drugs and chemicals—and their online attributes; for example, it could be a list of illegal drug names, persons of interest known or suspected to sell drugs online or links to such persons' Facebook pages. A term list can be either a simple list, or it may be derived from an ontology or a directed graph. An ontology is a taxonomic tree that presents knowledge in a form that can be used for reasoning and inference. For example, an ontology could be constructed to show the possible precursor pathways for all illegal drugs and these could be added to the term list. Ontologies for legal drugs already exist (see https://www.ncbi.nlm.nih.gov/labs/articles/23277001/). The relatedness of entities can be visualised in a directed graph, weighted to indicate the strength of the relationship between two entities; this can then be used to make inferences. For example, a group of drug dealers may all be linked through intermediaries to a chemical company from which they purchase precursors. An expert system or reasoning engine to use ontologies and/or directed graphs to make inferences; an expert system could reason that someone seeking to buy sulfaminic acid and anthranilic acid (both available from alibaba.com) might intend to produce ice.
- Analyse, process and report on prevalence, at some regular internal, the relationships between entities and

the scale of the activity. For example, a million Google ads seeded with terms from the term list could be used to report annully on the prevalence of illicit drug advertising.

The results of two investigations, both using active search and a range of search terms that are of particular relevance to the illicit drug trade targeting Australians, are below.

ASMIA Investigation 1: Ecstasy and ketamine distribution and advertising

A Google search result was selected as the data source for prevalence analysis, and active monitoring was used. Two synthetic drugs, ecstasy and ketamine, were selected to ascertain prevalence; these have been used by nine percent and one percent of the Australian population, respectively. Street names for these were sourced from the American Council for Drug Education and included roll, XTC, Adam and X for ecstasy and Special K and Vitamin K for ketamine. These terms were all used as noun phrases (without modifiers). Verb phrases selected were synonyms associated with distribution (such as acquisition, bargain, closeout, deal, good deal, investment, purchase, steal and value) or sale (such as advertise, auction, bargain, barter, be in business, boost, clinch the deal, close, close the deal, contract, deal in, dispose, drum, dump, exchange, handle, hawk, hustle, market, merchandise, move, peddle, persuade, pitch, plug, puff, push, put across, put up for sale, retail, retain, snow, soft sell, soft soap, spiel, stock, sweet talk, trade, traffic, unload, vend, wholesale). The term list was then searched using boolean operators, and potential avenues for advertising and distributing synthetic drugs identified in the results. A wide variety of results were returned, which could be broadly categorised as follows.

True positives

Genuine offers to buy or sell illicit drugs were widespread. For example, a search for 'buy ketamine OR sell ecstasy' returned a link to a list of illicit drugs (primarily synthetic) on an Australian classifieds website (promoted as the 'greatest suppliers of Mephedrone, Heroin, Ketamine, methylone, oxycontin, e, MDMA, MDVP'). These were listed both by street name and full chemical description. The following substances were listed for sale:

- 4-MEC;
- mephedrone (4-MMC);
- ecstasy (Such as : Sky,Gum,Go,Cros,XL);
- bulytone (bk-MBDB);
- MDAI;
- analgesic chemical CB1 and CB2;
- CP 47 497;
- CP-55 940;
- HU-210;
- HU-331;
- ephedrine HCl powder;
- JWH-018 / JWH-200 JWH-250;
- TFMPP;
- 2C-E, 2C-I, 2C-P, 2C-B, 2C-T-2;
- DOC, DOI;
- Bromo DragonFly;
- TCB-2;

- 5-Meo-DMT;
- 4-Aco-DMT;
- 4-Ho-MIPT;
- 4-Meo-PCP;
- naphyrone;
- heroin;
- methylone (bk-MDMA);
- BENZO anger;
- Pure Magic;
- Bonsai;
- Smoke;
- Chocolate;
- Special New Formula;
- Special gold;
- methedrone (BK-PMMA, methoxyphedrine);
- fluoromethamphetamine 2-(2-FMA);
- pyrrolidinopropiophenone (a PPP);
- MDPV (methylenedioxypyrovalerone, MDPK);
- Testosterone;
- JWH-073, 1-butyl-3-(1-naphthoyl) indole;
- Hydrocodone;
- dimethocaine (larocaine / DMC);
- morphine;
- JWH-018, 1-pentyl-3-(1-naphthoyl) indole;
- Heroine;
- fluoroamphetamine 4-(4-FA, 4-FMP, or flux); and
- ketamine.

An e-mail address was provided and the location of the site was stated as Canberra. The advertised delivery timeframe was a maximum of two days. Similar posts from the listed email address were made in February 2012, providing evidence of at least six months of trading.

False positives

These appeared to arise from word-sense disambiguation errors. For example, searches for 'buy ecstasy' returned links to Rolls-Royce's website (the Rolls-Royce mascot is known as the Spirit of Ecstasy).

Trading advice

The usernames and photos of individuals who post to social media (such as Yahoo, 4chan and grasscity.com) about their experiences of buying, selling and using drugs, could potentially be catalogued and cross-referenced.

Legal alternatives

Ads for so-called legal alternatives to ecstasy were commonplace on social media sites; clicking on a link might redirect a user to another page (such as buyecstasypills.com) where supposedly 'safe and legal' drug

alternatives could be purchased and shipped to Australia. The 'rave pills' advertised at buyecstasypills.com contain amino acids, caffeine, kava, citrus aurantium, pyridoxine hcl, and riboflavin; while some of these substances are legal, it may be illegal under Australian law to possess and/or import others.

Another example of such a drug alternative is kava. Since 2007 it has been illegal to import kava into Australia without a license, other than by Pacific Islanders for ceremonial purposes in accompanied luggage. Any company involved in selling kava online is, therefore, unlikely to have TGA approval.

Social media could also be used to find evidence of the use and distribution of illicit drugs. It may be possible to index content on users' social media pages to identify such evidence (Xtreme Herbs' Facebook page has over 8000 likes).

Market segmentation

Some advertising targets specific Australian demographics—for example, ketamine and mephedrone were advertised for sale on a 'tradie' website with a contact form at the bottom. Other advertisements, purportedly of traders located in Darwin who provided email and web addresses, specifically targeted Australians. One such advertiser also offered ecstasy, MDMA, methamphetamine, MDPV and Fentanyl for sale; Google returned 334 posts by the advertiser to Australian, New Zealand and other sites, but further investigation revealed the advertiser was based in Belgium.

Definitions

Some sites provided descriptions of drugs and their associated street names, including terms like MDMA, X, beans, pills, rolls et cetera.

Usage advice

Some sites provided advice on how to use drugs like ecstasy 'safely', or answered medical/health queries such as 'Will it kill my baby if I take ecstasy while pregnant?'.

Biochemistry

Several sites provided research findings and/or biochemical information about drugs and precursors.

Summary

There is strong evidence of open advertising, targeted at Australians, of illicit drug sales even in a limited sample of search results. Combining basic noun and verb phrases to create search terms produces useable results but term disambiguation will remain a problem, as will categorising content in which such advertisements might be found. One of the challenges for automated analysis will be to reduce false positives, links to medical information sites et cetera and focus solely on true positives, especially those targeting specific markets like Australia.

ASMIA Investigation 2: Social network advertising

How social media advertising was targeted at users who acknowledge their interest in illicit substances was investigated. The analysis was undertaken as follows.

1. An account was opened with a major social networking site and the hometown/current location set to Australia.
2. A number of amphetamine precursors and other stimulants common within Oceania (derived from Schloenhardt 2007) were entered into a term list as noun phrases.
3. The terms were entered sequentially into a search; if more than one page was returned for a term, the first was added to the fictional social media user's list of interests (this list is used to generate advertising relevant to the user's interests).
4. Over a three-month period, all advertisements generated in response to the term list that might be associated with the sale or distribution of illicit drugs were logged.

Step 3 yielded some interesting results. For example, a search for phentermine (a Schedule 4, script-only medication in Australia) resulted in a top hit for a community page. The community page in turn contained a user-contributed link to www.ipharmastore.net, an online store that sells phentermine for US$226.86 per pack without a script; the site lists a local Melbourne phone number reportedly linked to PC repair phone scams (see http://whocallsme.com/Phone-Number.aspx/0399886362). This site may be based in the Philippines; their website states they are licensed by the Department of Health, Bureau Food and Drugs rather than by any Australian authority.

While many individual pages were associated with each of the terms, there was no advertising targeted toward the sale and distribution of illicit drugs. Perhaps this reflects a greater level of vetting of online advertising on social networks, as opposed to user-contributed content.

Part D: Law enforcement challenges

Policing the internet

The ability of law enforcement agencies to carry out investigations involving digital data is limited by a lack of computer forensic equipment and expertise. While many agencies have dedicated cells that investigate a range of online crime, with specific emphasis placed on investigating instances of online child exploitation, generalist investigators do not have the tools, and are not sufficiently or consistently taught the techniques, to conduct thorough online investigations or collect electronic evidence in a manner acceptable to courts.

Regardless of offenders' efforts to remain anonymous online, there will always be a need for human interaction at some stage of the distribution/supply chain. Law enforcement intervention can occur at this touchpoint, using traditional investigative methodologies and techniques to interdict.

The various online avenues for the supply of illicit synthetic drugs require innovative approaches to both investigating the supply of these drugs and reducing demand. Law enforcement interaction with these online marketplaces requires new tactics of public presence, intelligence gathering and infiltration to collect evidence.

Challenges

Understanding the new challenges and legal responses required to combat the sale of illicit synthetic drugs on the internet will prove challenging for many governments both domestically and internationally. The underlying reason for these challenges is the fact that, despite a number of similarities between digital evidence and other categories of evidence, there are also major differences. Some of the general principles, such as the requirement that the evidence be authentic, complete, reliable and accurate, and that the process of obtaining the evidence take place in line with legal requirements, still hold. Alongside the similarities, however, there are a number of aspects that make digital evidence unique and therefore require special attention when dealing with digital evidence in criminal investigations.

Jurisdiction

Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. Although jurisdiction is an aspect of sovereignty, it is not coextensive with it. The laws of a nation may have an extraterritorial impact, extending the jurisdiction beyond the sovereign and territorial limits of that nation. This is particularly problematic as the internet does not explicitly recognise sovereignty and territorial limitations. There is no uniform, international jurisdictional law of universal application and such questions are generally a matter of conflict of laws, particularly private international law. An example would be where the contents of a website are legal in one country and illegal in another. In the absence of a uniform jurisdictional code, legal practitioners are generally left with a conflict-of-law scenario.

The internet's international nature makes jurisdiction a much more tricky area than before, and courts in different countries have taken various views on whether they have jurisdiction over items published on the internet or business agreements made online. This can cover areas from contract law, trading standards and tax—through rules on unauthorised access, data privacy and spamming to more political areas such as freedom of speech, censorship, libel and sedition.

The collection of electronic evidence

Digital data can be highly fragile and is easily modified or deleted. To avoid a negative impact on reliability, the collection of digital evidence is often subject to certain technical requirements. The shutdown of a computer system will, for example, result in a loss of all memory stored in the RAM system memory unless special technical measures to prevent this process are applied. In cases where data is stored in a temporary memory, the technique of collecting the evidence can be different from the process of collecting traditional digital evidence. This may be critical if the suspect is using encryption technology.

A fundamental principle of computer forensics is the need to maintain the integrity of digital evidence. Data integrity may be defined as where the digital data has not been altered in an unauthorised manner since it was created, transmitted or stored by an authorised source. Protecting the integrity of data is necessary to ensure reliability and accuracy. Policies and procedures for handling digital evidence are necessary to maintain an effective quality system. This includes keeping case records and the use of computer forensic technologies and procedures by qualified experts (ITU 2012).

When dealing with cybercrime the competent investigation authorities and the courts need to deal with electronic evidence. Dealing with such evidence presents a number of challenges but also opens up new possibilities for investigation and for the work of forensic experts and courts. Digital evidence plays an important role in various phases of cybercrime investigations.

Digital evidence can be divided into two categories: computer-generated records and records that are merely computer-stored. The difference hinges upon whether a person or a computer created the records' substantive contents. Computer-stored records are documents that contain the writings of some person(s) and happen to be in electronic form. Email messages, word-processing files and internet chat-room messages are common examples. The key evidentiary issue is demonstrating these are a reliable and trustworthy record of the human statement. In contrast, computer-generated records contain the output of computer programs, untouched by human hands. Common examples are log files, telephone records and ATM transaction receipts. The key evidentiary issue is demonstrating that the computer program generating the record is functioning properly. A third category of IT evidence can be adduced: records that are both computer-stored and computer-generated. A common example is an email that contains both human statements—for example, the body of the message—and computer-attached data—for example, headers.

Digital evidence has a number of characteristics. These include:

- design—computer systems will only create and retain electronic records if specifically designed to do so;
- volume—the large volume of electronic records causes difficulties with storage and prolongs the discovery of a specific electronic record;
- co-mingling—electronic records relating to a specific wrongdoing are mixed with unrelated electronic records;
- copying—electronic copies can be immediately and perfectly copied after which it is difficult, and in some cases impossible, to identify the original from the copy. In other cases, a purported copy may be deliberately or accidentally different from the original and hence evidentially questionable;
- volatility—electronic records can be immediately and deliberately or accidentally altered and expunged; and
- automation—electronic records may be automatically altered or deleted (SAI Global 2003).

The collection and preservation of digital evidence requires multifaceted investigative skills. The techniques used to collect evidence stored on a digital device and those employed to intercept a data-transmission process are significantly different.

Although new investigation instruments like real-time collection of content data and the use of remote forensic software to identify an offender are under discussion and have already been implemented by some countries, search and seizure remains one of the most important investigation instruments. As soon as the offender is identified and law enforcement seizes IT equipment, computer forensic experts can analyse the equipment to collect the evidence necessary for prosecution.

The ability of investigators to search for data or seize digital evidence, and the ability of courts to deal with it, is not limited to investigations surrounding illicit synthetic drugs and the internet. Due to the increasing integration of computer technology in people's everyday lives, digital evidence is becoming an important source of evidence even in traditional investigation (ITU 2012).

In addition to the procedures relating to the presentation of digital evidence in court, the ways in which digital evidence is collected require special attention. The collection of digital evidence is linked to computer forensics (ITU 2012). In those cases where no other sources of evidence are available, the ability to successfully identify and prosecute an offender may depend upon the correct collection and evaluation of electronic evidence. This influences the way law enforcement agencies and courts deal with such evidence. While traditional documents are introduced by handing out the original document in court, digital evidence in some cases requires specific procedures that do not allow conversion into traditional evidence, for example by presenting a printout of files and other discovered data. Having legislation in place that deals with the admissibility of evidence is therefore seen as vital in the fight against cybercrime.

Computer forensics is the systematic analysis of IT equipment for the purpose of searching for digital evidence. The constantly increasing amount of data stored in digital format highlights the logistical challenges of such investigations. Obtaining digital evidence is typically more complicated than approaching a person of interest and asking them to hand over their computers and media. More often than not files containing incriminating evidence are deleted, or in some cases attempts may have been made to destroy the device containing the data through physical damage or exposure to magnetic fields.

Legal requirements can often be difficult; investigators must not only ensure their work is within the scope of the warrant, but a suspect may be able to claim legal privilege over part of the evidence. Unlike paper files, which can be easily examined, and from which privileged documents can easily be excluded, electronic documents cannot be easily removed from a forensically imaged hard drive without disrupting other parts of the hard drive (directories and allocation tables would need to be modified). Even if this were successful, it would then be near-impossible to confirm the image matches the original hard drive, as the main method for confirming congruency between pieces of digital evidence is to generate a cryptographic hash of each, and then compare the two hash values.

Although computer forensics largely deals with computer hardware and digital data, it is not necessarily always automated, and remains to a large extent manual work. This is especially true with regard to the development of strategies and the search for possible evidence within search and seizure procedures. The amount of time necessary for such manual operations and the ability of offenders to automate their attacks underline the challenges that law enforcement agencies face, especially in investigations involving a large number of suspects and large data volumes. However, some processes, like the search for suspicious keywords or the recovery of deleted files, can be automated using special forensic analysis tools.

In addition to hardware analysis, software analysis is a regular task in cybercrime investigations. Computer software is necessary to operate a computer system. In addition to the operating systems, additional software tools can be installed to gear the functioning of computer systems to the demands of the user. Forensic experts can analyse how software tools function to prove that a suspect was capable of committing a specific crime.

Depending on the requirement of the specific investigation, computer forensics could for example include analysing the hardware and software used by a suspect, supporting investigators in identifying relevant evidence, recovering deleted files, decrypting files and identifying internet users by analysing traffic data. Traffic data is data generated by computers during the communication process in order to route a communication from its origin to its destination. Whenever a user connects to the internet, downloads emails or opens a website, traffic data is generated. For cybercrime investigations, the most relevant origin and destination traffic data are IP addresses that identify the communication partners in internet-related communication (ITU 2012).

Part E: Conclusion

Online payments have changed over the years. People have moved from traditional methods like cash and credit cards to advanced payment options like e-cash and virtual money transfer. Online payments are faster, efficient and private, unlike traditional methods like credit card payments that leave behind a lot of information on the internet. However, due to a lack of trust in modern methods at a time when user security is of great importance, many internet users rely on traditional methods. Online transactions can lead to cases of fraud and identity theft, and this makes it difficult for companies dealing with online products like e-cash to dominate the market.

Some online marketplaces have taken advantage of online payments to conduct illicit activities; one of these is the sale of synthetic drugs. Nevertheless, online payments allow sellers and buyers to complete transactions away from the prying eyes of the internet public, due to enhanced security and data authentication that ensure users maintain integrity. The present methods show an improvement from previous innovations in the same field. Further, statistical reports show a rapid growth of online transactions in the new millennium, as more people move to the internet for business activities as well as social interactions.

The internet is globally prominent because it is cumbersome to monitor all transactions being undertaken through such a medium. Many people have embraced it as a medium of communication; target groups are internet savvy, which allows those peddling illicit drugs and other synthetic drugs an avenue where they can conduct their business without being traced. This trade is encrypted, and this means only a few targeted individuals understand the content of such information. The internet also allows secret communication; there are two sides involved and this means information can be easily disseminated without raising any eyebrows.

International actors have attempted to alleviate the vice. For instance, governments are teaming up with NGOs to ensure vice is eradicated by educating young people and other affected individuals on the dangers of the illicit drugs and other synthetic substances offered in the market. International bodies such as Interpol are working with local governments worldwide with the aim of controlling the menace. It is clear that, although the trade is gaining currency, much has been done to bring it to manageable levels, but it remains to be seen whether the sale of these drugs via the internet will be wiped out in the long run.

Recommendations

- Internet Service Providers should proactively work with law enforcement to investigate the online supply of illicit synthetic drugs.
- All mail entering Australia, including items handled by international courier companies, should be targeted for inspection.
- Internet pharmacies through which internationally controlled substances are sold and that operate within their jurisdiction should be registered and require for dispensing preparations containing internationally controlled substances.
- Governments that detect the illegal sale of internationally controlled substances through the internet should immediately submit any information on such a sale to the government of the states involved.
- Law enforcement officers, members of the judiciary and staff of regulatory agencies should be extensively trained to strengthen their control of illicit synthetic drugs and psychotropic substances and enable them to take action against the illegal sale of internationally controlled substances via the internet.
- There should be greater participation in and resourcing of international networks which share knowledge of and build expertise in illicit synthetic drugs.

- Awareness of the public health dangers associated with many new psychoactive substances should be raised; and, in particular, the misconception that those substances are safe since they are not controlled should be dispelled.
- There should be a prolonged social media campaign to increase young people's knowledge of illicit synthetic drug-related harms and provide information which will lead to them avoiding and/or reducing their use.
- There should be anonymous and safe public places for users to test tablets.
- A multidisciplinary expert group, with representatives from health, NGOs, police, prosecutors and customs, should be created. Members should have expert knowledge of drugs, intelligence, internet and computers.
- There should be further research to document trends, drugs and the modus operandi which link internet-related drug trafficking—particularly those related to the dark web.
- Online marketplaces such as the Silk Road and Black Market Reloaded should be disrupted through undercover operations and technical measures.
- The individuals behind the Bitcoin exchange should be identified.
- State/territory and national legislation should be introduced outlawing almost all synthetic cannabinoids and giving respective fair trading authorities the power to issue on-the-spot bans on products in adult shops, tobacconists and other stores.
- Research should be benchmarked to monitor social media, hospital records, law enforcement seizures and purity statistics to determine the scope of the illicit synthetic drug problem in Australia in out-years.

Case study

The following case study is an example of the illicit synthetic drug market facing Australia and the response to it by law enforcement. Between 27 March 2012 and 28 June 2012 Australian Customs and Border Protection (Customs) officers working at the Melbourne and Sydney gateway facilities examined a total of 12 mail articles addressed to a Melbourne man. Each mail article was found to contain narcotics, with presumptive testing indicating the presence of either MDMA, cocaine or amphetamine. The Australian Federal Police (AFP) subsequently executed a search warrant at the man's address and found additional drugs and related paraphernalia.

The AFP seized and analysed a computer. The unbranded midi-tower computer was identified with the following:

- TOR client software;
- Mozilla Firefox Portable was located within a folder labelled
- 'Tor Browser'. Internet browsing bookmarks recovered showed the web address for the Silk Road online marketplace; and
- an HTML document titled 'Output 1—Facilitation of the legitimate movement of goods across the border, while interception prohibited and restricted import and exports'. This file is a report published by Customs comparing the number, type and weights of drugs detected between 2002 and 2005.

The AFP analysed the Sony laptop computer and identified the following:

- 34 image files depicting crystal, powder, green vegetable matter and paper-like substances believed to be narcotics. These substances all appear with a piece of paper beneath them containing the words 'SHADH1 AUS';
- a document titled 'The Construction & Operation of Clandestine Drug Laboratories';
- a document titled 'The Organic Chem Lab Survival Manual 3rd Ed';
- a text document with the heading 'Making Methamphetamine at home'; and
- recovered internet search terms including: 'dhl handed over to customs'; 'silk road busts; 'silk road Tor address'; 'silk road forum address'; and 'does australia post record tracking checks'.

References

ABC News 2013. *Silk Road shut down after notorious online marketplace's alleged owner arrested.* http://www.abc.net.au/news/2013-10-03/online-marketplace-silk-reoad-closed-after-proprietor-arrested/4995088

Australian Bureau of Statistics 2012. *Mobile handset subscribers*. http://www.abs.gov.au/ausstats/abs@.nsf/Products/8153.0~December+2012~Chapter~Mobile+handset+subscribers?OpenDocument

Australian Bureau of Statistics 2016. *Mobile handset subscribers*. http://www.abs.gov.au/AUSSTATS/abs@.nsf/Previousproducts/8153.0Main%20Features5June%202015?opendocument&tabname=Summary&prodno=8153.0&issue=June%202015&num=&view=

Australian Crime Commission. *Illicit Drug Data Report 2011–12*. http://www.crimecommission.gov.au/sites/default/files/files/IDDR/2011-12/IDDR-2011-12-FINAL-HR-020513.pdf

Australian Customs and Border Protection Service. 2010. *Submission to the Parliamentary Joint Select Committee on Cyber-Safety - Inquiry into the safety of children and young people on the internet.*

Australian Institute of Health and Welfare 2014. National Drug Strategy Household Survey detailed report 2013. Drug statistics series no. 28. Cat. no. PHE 183. Canberra: AIHW.

Barratt M 2001. *Beyond Internet as a Tool: A Mixed-Methods Study of Online Drug Discussion*. PhD thesis

Barratt M 2012. *Silk Road: eBay For Drugs*. http://onlinelibrary.wiley.com/doi/10.1111/j.1360-0443.2011.03709.x/full

Black Market Reloaded. Nd. *The 3 Biggest Darknet Markets 2016.* http://blackmarketreloaded.org/the-3-biggest-darknet-markets-2016/

Bogenschutz MP 2005. *Drug information libraries on the internet*. Journal of Psychoactive Drugs 32(3): 249–258

Boyer EW, Shannon M & Hibberd PL 2005. The Internet and psychoactive substance use among innovative drug users. *Pediatrics* 115(2): 302–305

Boyer EW, Shannon M & Hibberd PL 2006. Web sites with misinformation about illicit drugs. *English Journal of Medicine* 345(6): 469–471

Brownfield W 2011. *Drug and Chemical Control*. New York, NY: Diane Publishing

Brezo F & Bringas PG 2012. *Issues and Risks Associated with Cryptocurrencies such as Bitcoin*. SOTICS 2012: The Second International Conference on Social Eco-Informatics

Bryan L 2009. *Searching for Safety: Addressing Search Engine, Website, and provider Accountability for Illicit online Drug Sales.* American Journal of Law 35(1): 125–184

Central District of California 2012. *Creators and operators of on-line narcotics marketplace on the tor network arrested on first of its kind federal indictment charging drug trafficking in 34 countries and 50 states.* http://www.justice.gov/usao/cac/Pressroom/2012/045.html

Central Intelligence Agency 2010. *The World Factbook 2009*. https://www.cia.gov/library/publications/the-world-factbook/docs/history.html

Central Intelligence Agency 2011. *The World Fact Book 2010.* https://www.cia.gov/library/publications/the-world-factbook/fields/2086.html

Chen A 2011. *The underground website where you can buy any drug imaginable.* http://gawker.com/5805928/the-underground-website-where-you-canbuy-any-drug-imaginable

Cherney A, O'Reilly J & Grabosky P 2005. *The Governance of Illicit Synthetic Drugs* NDLERF Monograph No. 9

Christin N 2012. *Travelling the Silk Road: A measurement analysis of a large anonymous online marketplace.* http://arxiv.org/pdf/1207.7139v1.pdf

Council of the European Union 2011. *European Pact against Synthetic Drugs*. http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/jha/125709.pdf

Commission of the European Communities 2010. *Regulation of the European Parliament and of the Council on the marketing and use of explosive precursors*. http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2010/sec_2010_1040_en.pdf

Dingledine R, Mathewson N & Syverson P 2004. Tor: The second-generation onion router. *Proceedings of the 13th USENIX Security Symposium.* http://static.usenix.org/event/sec04/tech/full_papers/dingledine/dingledine.pdf

Dragut E, Meng W & Yu C 2012. *Deep Web Query Interface Understanding and Integration.* San Rafael, CA: Morgan & Claypool Publishers

Dwoskin E 2013. *To stop designer drugs, an early warning system is born.* http://www.businessweek.com/articles/2013-04-11/to-stop-designer-drugs-an-early-warning-system-is-born

ES Magazine (n.d.). *The other internet*. http://encrypted.cc/ES-250512-P2.pdf

European Monitoring Centre for Drugs and Drug Addiction and EUROPOL. *2016 EU Drug Markets Report: In-depth analysis.* http://www.emcdda.europa.eu/start/2016/drug-markets

Federal Bureau of Investigations. *Intelligence Assessment, 2012. Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity.* http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

Finley L 2008. *Hawking hits on the information highway: The challenges of online drug sales for law enforcement.* New York, NY: Peter Lang

Food and Drug Administration (FDA) 2016. *FDA targets unlawful internet sales of illegal prescription medicines during International Operation Pangea IX* http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm505921.htm

Fox S 2004. *Prescription drugs online*. Washington DC: Pew Internet and American Life Project. (P. I. a. A. L. Project o. Document Number)

Garbato K 2005. *13 lucky steps to writing a research paper.* Cleverland Park, Kansas: Peedee Publishing

Ghodse H 2008. *International drug control into the 21st century.* USA: Ashgate Publishing Limited

Glenny M 2009. *Canada: The New Global Drug Lord.* http://www2.macleans.ca/2009/08/18/canada-the-new-global-drug-lord/

Gordon SM, Forman RF & Siatkowski C 2006. Knowledge and use of the internet as a source of controlled substances. *Journal of Substance Abuse Treatment* 30: 271–274

Government of New York. *What is a synthetic drug?* http://www.health.ny.gov/professionals/narcotic/docs/synthetic_drugs_faq.pdf

Grant R 2014. *Bitcoin for idiots: An introductory guide*. http://venturebeat.com/2014/02/17/bitcoin-for-idiots-an-introductory-guide/

Gwern.net. 2011. Using Silk Road. http://www.gwern.net/Silk%20Road

Hanson G, Venturelli P & Fleckenstein A 2011. *Drugs and Society*. Burlington: Jones & Bartlett, Publishers

Hendley N 2010. *Crystal death: North America's most dangerous drug*. Canada: Five Rivers Chapmanry

Hope M 2007. *Searching the web: A think aloud investigation into college student's online behaviour*. Ann Arbor, MI: ProQuest Information and Learning Company

Hout M & Bingham T 2013. *'Silk Road', the virtual drug marketplace: A single case study of user experiences*. https://www.gwern.net/docs/sr/2013-van-hout.pdf

Hutson B & Miller M 2010. *Beware the Darknet.* http://www.procysive.com/info_wp/Beware_the_Darknet.pdf

International Narcotics Control Board 2009. *Guidelines for governments on preventing the illegal sale of internationally controlled substances through the internet*. http://www.incb.org/documents/Narcotic-Drugs/Guidelines/internet/NAR_guide_Internet_guidelines_English.pdf

International Narcotics Control Board 2012. *Report of the International Narcotics Control Board for 2012*. http://www.incb.org/incb/en/publications/annual-reports/annual-report-2012.html

International Telecommunications Union 2013. *The world in 2013, ICT facts and figures.* http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf

International Telecommunications Union 2012. *Understanding cybercrime: Phenonema, challenges and legal response.* http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CybcrimeE.pdf

Interpol 2008. *Synthetic drugs.* http://www.interpol.int/public/Drugs/synthetic/default.asp

Interpol nd. *Synthetic drugs and precursor chemicals*. http://www.interpol.int/Crime-areas/Drugs/Synthetic-drugs-and-precursor-chemicals

Isralowitz R & Myers P 2011. *Illicit Drugs*. California, CA: ABC-CLIO

Jeffries A 2013. *Drugs, porn and counterfeits: the market for illegal goods is booming online.* http://www.theverge.com/2013/4/29/4281656/silk-road-black-market-reloaded-tor-marketplaces

Le Blond et al. 2011. *One bad apple spoils the bunch: Exploiting P2P applications to trace and profile Tor users.* http://hal.inria.fr/docs/00/57/41/78/PDF/btor.pdf

Lenhart et al 2010. *Social Media and Mobile Internet Use Among Teens and Young Adults.* http://www.pewinternet.org/files/old-media/Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplines.pdf

McCandless D 2005. *Bad trip for online drug peddlers*. http://www.wired.com/medtech/health/news/2005/07/68049

McCoy D, Bauer K, Grunwald D, Kohno T & Sicker D 2008. *Shining light in dark places: Understanding the Tor network*. http://homes.cs.washington.edu/~yoshi/papers/Tor/PETS2008_37.pdf

Monfries A 2012. *Party drugs popular with online shoppers*. http://www.news.com.au/national-old/party-drugs-popular-with-online-shoppers/story-e6frfkvr-1226239065881

Montagne M 2008. Drugs on the internet I: Introduction and web sites on psychedelic drugs. *Substance Use & Misuse* 43(1):17-25

Morris S 2002. *Web drug dealers rattle cyber cops*. http://www.guardian.co.uk/technology/2002/mar/02/drugs.internationalnews

Murdoch J & Danezis G nd. *Low-cost traffic analysis of Tor*. http://www.cl.cam.ac.uk/~sjm217/papers/oakland05torta.pdf

Murguia E, Tackett-Gibson M & Lessem A 2007. *Real drugs in a virtual world: Drug discourse and community online*. New York: Lexington Books

Nakamoto S 2009. *Bitcoin: A Peer- to Peer Electronic Cash System*. http://bitcoin.org/bitcoin.pdf

Pates R & Riley D 2012. *Harm reduction in substance use and high-risk behaviour.* Malden, MA: Wiley Blackwell

Pompidou Group nd. *Drug related cybercrime and associated use of the internet*. https://www.coe.int/T/DG3/Pompidou/Source/Documents/P-PG-(2013)4Cybercrime-internet.pdf

Oakes L 2011. *Synthetic DRUG Sales Booming on Web. StarTribune.* http://www.startribune.com/local/129596073.html?refer=y

Office of National Drug Control Policy 2006. *Synthetic drug control strategy: A focus on methamphetamine and prescription drug abuse.* Washington, DC: DIANE Publishing

Olding R 2012. *Anguish sparks search for more data on 'legal highs'*. http://www.smh.com.au/national/anguish-sparks-search-for-more-data-on-legal-highs-20130531-2nh3m.html

Reynolds GP et al. 2012. Deprenyl is metabolized to methamphetamine and amphetamine in man. *British Journal of Clinical Psychology* 6(6): 542–544

Roll J, Rawson R, Ling W & Shoptaw S 2009. *Methamphetamine addiction: From basic science to treatment.* New York, NY: Guilford Press

Room R & Paglia A 2009. The international drug control system in the post Cold War era: Managing markets or fighting a war? *Drug and Alcohol Review* 18(3): 305–315

Standards Australia International 2003. *Handbook 171: Guidelines for the management of IT evidence.*

Schneider J 2003. Hiding in plain sight: An exploration of the illegal(?) activities of a drugs newsgroup. *The Howard Journal* 42(4): 374–389

Strauss K 2012. *Cyber Laundering: How can we combat money laundering over the internet?* http://www.academia.edu/1369342/Cyber-laundering_-_How_can_we_combat_money_laundering_over_the_internet

Swift J 2012. *Travelling the Silk Road to the deep web's darkest corner.* <http://jjie.org/silk-road-deep-webs-darkest-corner/88570>

Syracuse University, Health Services nd. *Synthetic drugs pose great risk to college students*. http://health.syr.edu/education/synthetic-drugs.html

Tandy K 2004. *DEA announces arrests of website operators selling illegal designer drugs*. http://www.justice.gov/dea/pubs/pressrel/pr072204.html

The Deep Web. *Statistics*. https://hewilson.wordpress.com/what-is-the-deep-web/statistics/

The National Center on Addiction and Substance Abuse. 2011. *National Survey of American Attitudes on Substance Abuse XVI: Teens and Parents.* http://www.centeronaddiction.org/newsroom/press-releases/2011-national-teen-survey-finds

European Monitoring Centre for Drugs and Drug Addiction 2010. *Methamphetamine: A European Union Perspective in the Global Context* 13(2): 240–248

Tupper KW 2008. *The globalization of ayahuasca: Harm reduction or benefit maximization?* International Journal of Drug Policy 19: 297–303

United States Department of Justice 2008. *Information bulletin: Drugs, youth and the internet.*

United States Drug Enforcement Administration 2004. *DEA announces arrests of website operators selling illegal designer drugs.* http://www.justice.gov/dea/pubs/pressrel/pr072204.html

United Nations Office on Drugs and Crime 2008. *Get the facts about drugs.* http://www.unodc.org/documents/drugs/getthefacts_E.pdf

United Nations Office on Drugs and Crime 2012. *International Narcotics Control Board warns of illegal online pharmacies selling drugs to youth.* http://www.unodc.org/unodc/en/frontpage/2012/February/narcotics-control-board-warns-of-illegal-online-pharmacies-selling-drugs-to-youth.html

United Nations Office on Drugs and Crime 2009. *UNODC warns of growing abuse of synthetic drugs in the developing world.* http://www.unodc.org/unodc/en/press/releases/2008-09-09.html

United Nations office on Drugs and Crime 2007. *World drug report 2007*. http://www.unodc.org/unodc/en/data-and-analysis/WDR-2007.html

United Nations Office on Drugs and Crime 2012. *World drug report 2012.* http://www.unodc.org/unodc/en/data-and-analysis/WDR-2012.html

Van Pelt J 2012. *Synthetic Drugs: Fake substances, real dangers.* http://www.socialworktoday.com/archive/070212p12.shtml

Walters J 2011. *Synthetic drug control strategy: A focus on methamphetamine and prescription drug abuse.* Collingdale: Diane Publishing

Wax PM 2005. Just a click away: recreational drug web sites on the internet. *Pediatrics* 109(6): e96

Wired.com 2011. *United Sates District Court For the Central District of California*. http://www.wired.com/images_blogs/threatlevel/2012/04/WILLEMSIndictment-FILED.045.pdf

Yao J 2010. *Web based support*. New York: Springer-Verlag London Limited