European Monitoring Centre
for Drugs and Drug Addiction

INSIGHTS EN

ISSN 2314-9264

The internet and drug markets

21

European Monitoring Centre
for Drugs and Drug Addiction

The internet and drug markets

EMCDDA project group
Jane Mounteney, Alessandra Bo and Alberto Oteo

21

Legal notice

Luxembourg: Publications Office of the European Union, 2016
ISBN: 978-92-9168-841-8
doi:10.2810/324608

This publication should be referenced as:

European Monitoring Centre for Drugs and Drug Addiction (2016), The internet and drug markets, EMCDDA Insights 21, Publications Office of the European Union, Luxembourg.

References to chapters in this publication should include, where relevant, references to the authors of each chapter, together with a reference to the wider publication. For example:

Mounteney, J., Oteo, A. and Griffiths, P. (2016), 'The internet and drug markets: shining a light on these complex and dynamic systems', The internet and drug markets (European Monitoring Centre for Drugs and Drug Addiction: Insights 21), Publications Office of the European Union, Luxembourg.

European Monitoring Centre
for Drugs and Drug Addiction

Praça Europa 1, Cais do Sodré, 1249-289 Lisbon, Portugal
Tel. +351 211210200
info@emcdda.europa.eu | www.emcdda.europa.eu
twitter.com/emcdda | facebook.com/emcdda

Contents

5 Foreword

7 Executive summary

11 Acknowledgements

13 CHAPTER 1
The internet and drug markets: shining a light on these complex and dynamic systems
Jane Mounteney, Alberto Oteo and Paul Griffiths

19 SECTION I
Dark net cryptomarkets

23 CHAPTER 2
Cryptomarkets and the future of illicit drug markets
Judith Aldridge and David Décary-Hétu

33 CHAPTER 3
Tor and links with cryptomarkets
Andrew Lewman

41 CHAPTER 4
Staying in the shadows: the use of bitcoin and encryption in cryptomarkets
Joseph Cox

49 CHAPTER 5
Reputation is everything: the role of ratings, feedback and reviews in cryptomarkets
Joseph Cox

57 SECTION II
Dark net markets — key actor perspectives

61 CHAPTER 6
Silk Road: insights from interviews with users and vendors
Eileen Ormsby

69 CHAPTER 7
The emergence of deep web marketplaces: a health perspective
Fernando Caudevilla

77 CHAPTER 8
The drug trade on the deep web: a law enforcement perspective
Joost van Slobbe

85 CHAPTER 9
How the use of the internet is affecting drug trafficking practices
Anita Lavorgna

93 SECTION III
Surface web markets and social media

97 CHAPTER 10
A method for exploring the number of online shops selling new psychoactive substances: initial I-TREND project results
Magali Martinez, Daniela Kmetonyová and Vendula Běláčková

107 CHAPTER 11
Online supply of medicines to illicit drug markets: situation and responses
Lynda Scammell and Alessandra Bo

115 CHAPTER 12
Social media and drug markets
Danica Thanki and Brian Frederick

125 SECTION IV
Insights and implications

127 CHAPTER 13
What is the future for internet drug markets?
Jane Mounteney, Paul Griffiths and Liesbeth Vandam

135 Glossary

Foreword

The EMCDDA has been monitoring the drug situation for the last 20 years. In that time, the nature and range of drugs available has changed considerably and, in more recent years, the manner in which people acquire drugs has also undergone a change. There has been a shift from face-to-face purchases to also acquiring drugs through unseen, and often unmonitored, parts of the world wide web. Almost any kind of illegal drug can be purchased online and delivered by mail, without the buyer making direct contact with the drug dealer.

In this first detailed exploration of the subject, we collate the most recent evidence from a range of experts, each with his or her own unique perspective. Our compilation will add to the collective knowledge available on this part of the supply chain and highlight the gaps for future research. It does not claim to be complete or up to the minute. What it is, however, is our inaugural in-depth analysis of a facet of the drugs phenomenon that the agency has not yet explored extensively.

Searching on the internet today can be compared to dragging a net across the surface of the ocean. While a great deal may be caught in the net, there is still a wealth of information that is deep and, therefore, missed. Similarly, drug markets can make use of the various levels of the web in order to operate. There is the surface web, often used for illicit medicines and new psychoactive substances, and also the deep web, with its dark net markets or cryptomarkets, supported by innovative technologies to protect privacy. Furthermore, the proliferation of social media and development of web technologies that allow greater user interaction have the potential to influence customer and user involvement in drug markets.

We are delighted to release this investigation into the world of online drug markets. Although at present, it appears that only a minority of drugs are purchased in this manner, it seems likely that online drug markets could in the near future disrupt drug dealing in the same way that eBay, Amazon and PayPal have revolutionised the retail experience.

This report is destined for both readers with a previous specialised knowledge and those trying to gain insight into a new and rapidly evolving topic. Along with information on what the deep web is, how it operates, the role of 'The Onion Router' in the anonymous sale and purchase of illegal drugs, the role of encryption and cryptocurrencies, the content raises certain questions. For example, how will illicit drugs be marketed and trafficked in the future? Are the current tools and responses fit for purpose? How can the EMCDDA address the challenges of monitoring such a dynamic and fast-changing environment?

Alexis Goosdeel
Director, EMCDDA

Executive summary

Background

The last decade has seen the emergence of new internet technologies that have acted as important facilitators of online drug markets. Historically, illicit drug retail markets have operated in physical spaces, with associated practical limitations and boundaries. The development of virtual markets changes the dynamics of the selling and buying process, potentially opening the market up to a wider audience.

Drug markets operating on the surface, or clear, web appear to be primarily associated with the distribution of either non-controlled substances or substances for which legal controls differ between countries and jurisdictions (medicines, lifestyle products, new psychoactive substances, precursor chemicals). Online pharmacies have flourished, broadening their supplies from lifestyle products to performance enhancement products and prescription drugs. A rapid expansion of the online market for new psychoactive substances has been observed over the last decade, with these substances sold as both 'research chemicals' and 'legal highs' in online shops. Alongside these markets, the growth of social media has seen the emergence of forums and mobile applications where drugs are discussed, advertised and sometimes sold.

This publication aims to unravel some of the complexities surrounding online markets: what they are, how they operate, the technologies underlying them and how they interact with the traditional drug market. Expert contributions come from a number of individuals who attended a meeting in Lisbon to share experiences and knowledge on the topic of the internet and drug markets. They represent a wide range of international expertise on both the deep web and the surface web, providing insights from IT, research and monitoring, law enforcement and drug user perspectives.

Dark net markets

Recently, attention has shifted to the sale of drugs and other illicit products and services in what have become known as dark net markets or cryptomarkets, which exist in what is in effect a 'hidden' part of the internet that is not accessible through standard web browsers. Dark net markets represent a notable innovation in the online drug trade and one of the main appeals is the relative anonymity they provide to users wishing to purchase illicit goods and services. A range of strategies are used to hide users' identities and conceal the physical locations of servers. These include anonymisation services, such as Tor (The Onion Router), which hide a computer's IP address when accessing the site; decentralised and relatively untraceable cryptocurrencies, such as bitcoin and litecoin, for making payments; and encrypted communication between market participants. Reputation systems play a central role in the functioning of dark net markets. They help regulate vendors and are used by buyers to inform their purchasing decisions.

Both demand reduction and supply reduction interventions on the surface web have been gathering pace. The deep web, however, has provided new opportunities and challenges for both health and law enforcement professionals. A number of studies cited by authors in this publication suggest that Silk Road may have helped users reduce the harm caused by illicit drug use, particularly compared with street-based drug marketplaces. Examples include the sale of high-quality products with low risk for contamination, vendor-tested products, sharing of trip reports and online discussion of harm reduction practices. There appears to be a growing interest in the provision of health-related interventions directly to users of the deep web, and 'DoctorX', for example, has offered a range of services to dark net market users, including information, advice and drug-testing services.

For law enforcement agencies, online monitoring represents a new approach to tackling drug markets, and they continue to build experience in this area. Law enforcement strategies have focused on market disruption, which includes reducing trust around anonymity, as well as the identification, arrest and prosecution of sellers in cryptomarkets. At the EU level, Project: ITOM (Illegal Trade on Online Marketplaces) has established an EU cybercrime network, with one of its tasks being to establish effective ways to combat the illegal trade within online marketplaces.

Surface web markets

Several studies have explored the online supply of new psychoactive substances, or so-called legal highs, through shops on the internet. The I-TREND (Internet Tools for Research in Europe on New Drugs) project aimed to develop a software-automated tool for monitoring online shops using a less resource-intensive method than had been available previously. This showed the need to take duplicate sites into consideration to understand the reality of online supply. In some cases, online shops target individual countries, with the type of shops available and the substances offered influenced by cultural factors and structural characteristics of national drug markets.

The online sale of medicines has expanded since the early 2000s and, although various platforms have been used, online pharmacies have been a primary source of distribution. In the early days, the most popular products supplied on the web were natural and herbal medicinal products, smoking cessation aids, and beauty and sexual performance enhancement products. More recently, the market for enhancement drugs such as muscle builders and diet pills has been expanding. Although there is increasing concern about the potential role of illegally operating online pharmacies in the supply of psychoactive medicines for misuse, there is little evidence to suggest they are an important source of medicines for illicit drug markets at present.

Social media

The growth of social media has revolutionised methods of communication and social interaction with each other. Drug-related content exists across social media: on social networking sites, in drug-themed apps, on video- and picture-sharing services and in drug forums. Furthermore, virtual social networks provide opportunities for drug-related encounters and there is evidence that this is happening particularly among small groups of men who have sex with men. There is also some evidence of drug selling through social media, often using drug slang.

There remains insufficient evidence, however, about the role of social media in the supply of drugs. There is also a need to identify ways in which the research and monitoring community and prevention and treatment agencies can harness social media to better understand drug use and to improve demand reduction responses.

A multiplicity of interconnected marketplaces

A wide range of factors appear to be driving change and development in internet drug markets; most are linked to technology, globalisation and market innovation. There is a consensus that the internet has changed drug markets by expanding possibilities for drug supply and trafficking. Research indicates that drug markets have become hybrid markets that combine the traditional social and economic opportunity structures with the new opportunities provided by the internet. Furthermore, not only has the internet opened the

way for new criminal actors, but it has also reconfigured relations among suppliers, intermediaries and buyers.

Drug trafficking patterns are constantly changing. Identifying patterns of criminal behaviour and matching them to different cyber-hotspots could have important implications for tackling offenders and potential offenders in the internet age. More criminological research is needed to take into consideration transformations in technology, society and crime caused by the internet, and to allow new preventative thinking on reducing criminal opportunities in cyberspace.

Acknowledgements

The EMCDDA would like to thank the following expert contributors who provided the content for this publication: Judith Aldridge, Fernando Caudevilla, Joseph Cox, David Décary-Hétu, Brian J. Frederick, Daniela Kmetonyová, Anita Lavorgna, Andrew Lewman, Magali Martinez, Eileen Ormsby, Lynda Scammel and Joost van Slobbe. We are also grateful to all of the experts who contributed to our technical report entitled 'The internet and drug markets' (available at emcdda.europa.eu/publications/technical-reports/internet-drug-markets) which inspired this EMCDDA Insights.

EMCDDA contributors (in alphabetical order): Alessandra Bo, Andrew Cunningham, Charlotte Davies, Michael Evans-Brown, Paul Griffiths, Jane Mounteney, Alberto Oteo, Alessandro Pirona, Blanca Ruiz, Danica Thanki and Liesbeth Vandam.

CHAPTER 1

The internet and drug markets: shining a light on these complex and dynamic systems

Jane Mounteney, Alberto Oteo and Paul Griffiths

Background: drug market dynamics

The last decade has seen the emergence of new internet technologies that have acted as important facilitators of online drug markets. Historically, illicit drug retail markets have operated in physical spaces, with associated practical limitations and boundaries. Whether taking place in a city-centre open drug scene or in a dealer's flat on a suburban housing estate, low-level drug sales have typically been associated with tangible people, places and geographical spaces. New developments have enabled the growth of online commerce in virtual marketplaces with global reach. This has the potential to expand the boundaries of drug supply and provide more opportunities for those wishing to buy drugs to do so. Virtual drug markets also offer participants the opportunity to sell and shop from their own homes, avoiding the face-to-face encounters associated with offline markets. Participants report that this can provide a degree of anonymity and physical safety that would otherwise be difficult to attain.

Technology has always been linked with changes in drug markets. A recent example is the widespread use of mobile phones, which has allowed the buying and selling of drugs to move out of more openly accessible physical spaces and into closed networks of known contacts. The development of virtual markets changes the dynamics of the selling and buying process further, potentially opening the market up to a wider audience, with participants unlikely to be known to each other. Thus, such markets may represent to participants the best of both worlds: open markets operating in a covert manner.

In reality, not all aspects of drug markets can take place in a virtual world. Both the production and distribution phases remain firmly linked to tangible real-world processes. Physical transactions, often involving postal delivery, must still take place.

Recent evidence suggests that practically any type of drug can be bought on the internet. Drug markets operating on the surface, or clear, web appear to be primarily associated with the distribution of either non-controlled substances or substances for which legal controls differ between countries and jurisdictions (medicines, lifestyle products, new psychoactive substances, precursor chemicals). Online pharmacies have flourished, broadening their supplies from lifestyle products to performance enhancement products and prescription drugs. A rapid expansion of the online market for new psychoactive substances has been observed since 2008, with these substances sold as both 'research chemicals' and 'legal highs' in online shops. A market for the supply of precursor and pre-precursor chemicals has also been identified. Alongside these markets, the growth of social media has seen the emergence of forums and mobile applications where drugs are discussed, advertised and sometimes sold.

More recently, attention has shifted to the sale of drugs and other illicit products and services in what have become known as dark net markets or cryptomarkets, which exist in what is in effect a 'hidden' part of the internet that is not accessible through standard web browsers. Cryptomarkets represent a notable innovation in the online drug trade. Software enabling anonymisation (e.g. The Onion Router) or encryption (e.g. PGP) and cryptocurrencies (e.g. bitcoin) provides a high level of anonymity for buyers and sellers, and drugs are delivered through the post, avoiding direct contact between the parties involved.

Although some commentators suggest that this virtualisation of drug-related trading, with forums providing user advice and ratings on sellers and their products, may reduce criminality, violence and intimidation in drug markets (Barratt et al., 2013; Aldridge and Décary-Hétu, 2014; Van Hout and Bingham, 2014), the speed with which the internet is transforming drug markets poses a major challenge to law

enforcement, public health, and research and monitoring agencies.

The EMCDDA study on the internet and drug markets

With a view to shedding further light on this complex topic and fast-changing environment, in autumn 2014, the EMCDDA initiated a mixed method study on internet drug markets, aiming to map out the territory and better understand the potential impact of this phenomenon. The objectives of this study were to increase understanding of the online supply of drugs with a focus on the sale of new psychoactive substances, research chemicals and 'legal highs'; the use of social media and apps; online sales of medicinal products for illicit use; and the sale of drugs on the deep web. The study methodology incorporated a number of investigative approaches and used data from multiple sources, and the work culminated in a meeting attended by international experts. During the meeting, the experts shared their experiences and contributed to an analysis of the topic, providing insights from IT, research and monitoring, law enforcement and drug user perspectives. Given the importance of the topic and the quality of knowledge and expertise shared during the meeting, it was decided to initiate a joint publication in which many of the meeting participants would be given the opportunity to share their insights in a structured way.

The 13 chapters of this publication on the internet and drug markets are the result of this endeavour and incorporate contributions from over 20 authors. By design, this is a heterogeneous work, drawing on the different backgrounds and world views of the multiple authors. It is the unique combination of different perspectives, including from academia, journalism and frontline practice, that makes this work rich and informative, offering a global overview of the situation alongside more detailed technical insights into specific aspects of this complex area.

A note on terminology

Perhaps unsurprisingly, given the novelty of the discipline, there are both overlaps and some discrepancies in the way certain terms are used in the scientific and popular literature. Below, we define how a number of key terms are used in this publication when referring to online drug marketplaces. We note, however, that certain authors have preferred usage that may differ from these definitions, and have used editorial discretion to allow variation in some cases. An example here is that some authors use the term 'dark net markets' while others prefer 'cryptomarkets'. Readers should note that a more detailed glossary section can be found at the end of this publication, on page 135.

The surface or clear web is the part of the internet that can be found by the link-crawling techniques used by a typical search engine such as Google, Bing or Yahoo (http://www.brightplanet.com). On the other hand, the deep web is a part of the internet not accessible to these search engines. The only way to access the deep web is by conducting a search within a particular website. Government databases and libraries, for example, contain huge amounts of deep web data.

The dark web or dark net is defined as a small portion of the deep web that has been intentionally hidden and is inaccessible through standard web browsers. The dark net can be accessed only using additional software such as the Tor Browser (Bright Planet, 2013), and it is the portion of the internet most widely known for illicit activities, because of the anonymity it offers to users.

Tor is an acronym for The Onion Router; it is free browsing software that hides a computer's IP address, enabling online anonymity and protecting the personal privacy of the internet user. The relatively recent development of usable interfaces with anonymity networks such as Tor has made it easy for anybody to browse the internet anonymously, regardless of their technical ability. It allows, for example, military operations to avoid being tracked and enables any individual to browse the internet protected from 'traffic analysis'. However, this has also facilitated the emergence of anonymous online markets specialising in 'black market' goods, such as pornography, weapons and drugs (Christin, 2013; Aldridge and Décary-Hétu, 2014).

Cryptomarkets or dark net markets are located in the dark web and accessed via Tor. A cryptomarket can be defined as an online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities (Martin, 2014). To date, most studies on online drug markets have centred on cryptomarkets, and in particular on Silk Road, one of the earliest cryptomarkets to be established. Silk Road began operating in February 2011, and captured worldwide media and political attention following an expose in the New York-based blog Gawker (Chen, 2011; Martin, 2014). Although it was not the only drug

cryptomarket, it was certainly the largest and best known (Barratt et al., 2014). Others, such as Black Market Reloaded, The Armory, Evolution and Agora have offered similar services.

It is important to note that bitcoin and encryption, as well as Tor, serve the legitimate purpose of protecting one's privacy. Individuals might wish to opt out of having their internet browsing habits recorded and stored, or to spend their own finances without the intermediation of a bank; journalists can use such technology to protect their sources. Although these technologies are used for criminal purposes, criminals are by no means their only users.

In the following sections, we briefly introduce the main online market segments and the thematic areas covered in more detail by the individual chapters in this publication.

Online anonymous drug marketplaces

On the deep web, drug sales can take place within a marketplace (e.g. Silk Road), within a decentralised network or between individuals. However, it is the dark net drug markets, also referred to as cryptomarkets, that have received most attention. Silk Road is to date the best known and most researched cryptomarket, and within this publication it functions almost as a case study. Although the situation has changed and many other markets have opened and closed, the information gathered around the first and, at the time, largest cryptomarket provides unique and invaluable insights.

Although it differed in offering anonymity, Silk Road provided a similar infrastructure for sellers and buyers to conduct transactions to those provided by other online marketplaces such as eBay, with professional dispute resolution mechanisms, use of vendor and buyer ratings, hosting of member discussion forums, and so on. Although a wide variety of products was advertised on Silk Road, established recreational drugs such as cannabis, MDMA and LSD, and some prescribed medicines, were reported to be the most popular (Barratt et al., 2014), while the sale of new psychoactive substances on the dark net markets seems to be limited.

Silk Road maintained the secrecy of its operators and location by combining two technologies: Tor and bitcoin. Tor enables anonymous communication between buyer and seller, and bitcoin can be used to facilitate anonymous transactions. Silk Road used bitcoins as a trading currency. Instead of paying the seller directly, buyers placed the corresponding number of bitcoins in escrow with Silk Road, and payments were only released to vendors when the item reached its destination and the delivery was confirmed. In fact, cryptocurrencies such as bitcoin are not anonymous (as there is a central ledger) and they require laundering (e.g. using a website such as Bitcoin Fog) if they are to be used for illicit activity. An important feature of Silk Road was that both sellers and buyers received ratings, with trust built on reputation. This system, explained in more detail in Chapter 5, was weakened by various scams.

Drug markets on the surface web

Legal highs, research chemicals and trade sites

The use of the surface web for the sale of new psychoactive substances is a topic that has received increasing attention over the last decade. The online market for these substances has been categorised into four primary segments: shops selling new psychoactive substances as research chemicals, mostly under their chemical names; a commercial segment, with products sold under brand names; classified ads, often located within public websites; and a deep web segment (Lahaie et al., 2013). The EMCDDA has been involved in online monitoring for a number of years and identified 651 websites selling 'legal highs' to Europeans in 2013 (EMCDDA, 2015). New methods for automated monitoring of this area are being developed by the I-TREND (Internet Tools for Research in Europe on New Drugs) project and are reported on in Chapter 10. In addition to the methodologies used, the project team describe some recent developments in the online new psychoactive substances market including increased hybridisation between the commercial and research chemical segments and the development of a 'grey market', with some websites having both a surface web presence and a hidden element on the deep web.

Online pharmacies

Online sales of medicines increased substantially in the early 2000s (Forman, 2006), and, although various platforms have been used, online pharmacies have been a primary source of distribution for both the legitimate and the illicit supply of medicinal products. Legitimate websites are those that comply with national and international regulations and standards, thus guaranteeing the quality of the product; sell controlled medicines only with a valid medical prescription; and

ultimately ensure consumer safety. Reports suggest, however, that there are a sizeable number of illegitimate online pharmacies involved in the illicit supply of products. These sites are not registered with any recognised accreditation system and do not abide by regulations and professional standards; therefore, they are operating illegally. There is concern that illegitimate online pharmacies may have a role in the supply of drugs for misuse. This is an area explored in more detail in Chapter 11, drawing on the limited studies available in this area.

Social media and apps

Social media are Web 2.0 technologies, characterised by increased participation and multidirectional lines of communication. They largely operate on the surface web, although Facebook, for example, has recently allowed access to its services through Tor. Social media may have an active role in drug markets, with sites and apps being used for buying and selling drugs, or they may have a more indirect role, providing a platform for experience sharing, photo and video sharing, opinion forming, and so on.

As explained in Chapter 12, many forms of networking might best be described as taking place on virtual social networks (VSNs), rather than online social networks, as much communication takes place via smart phones and tablets. VSNs can be categorised into static networks, which are more permanent and may include user profiles and terms of use (e.g. Facebook), and dynamic networks (e.g. Skype or ooVoo video chat), which are temporary and often by invitation only. A feature of VSNs is the creative use of slang and argot to get around moderation. Static (and especially) dynamic VSNs that use webcams have been recently associated with 'chem sex' parties and/or 'slamming' among men who have sex with men.

Who uses the internet to obtain drugs?

There is limited information available on the customers or users of street and virtual drug markets, with limited survey data tending to focus on overall sources of drug supply. These data indicate that, for most people who use drugs, the internet plays only a limited role in supply. The 2014 Flash Eurobarometer, a telephone survey of 13 128 young adults aged 15–24 in the 28 EU Member States found that, of those who had used new substances or 'legal highs' in the last 12 months, only 3 % had purchased them from the internet. In contrast, 68 % had been given them or had bought them from a friend (European Commission, 2014).

Numbers may be higher, however, in certain drug- and internet-savvy groups. The results of the Global Drug Survey 2015, an online survey that attracted more than 100 000 responses from individuals around the world about their drug use, showed that just over 1 in 10 respondents reported buying drugs via conventional internet sites and dark net sites in the previous year.

There are a limited number of studies on those buying drugs from dark net marketplaces. Van Hout and Bingham (2013) described the motives and purchasing experiences of a small group of Silk Road users. These were predominantly male and in professional employment or tertiary education. Their patterns of drug use were described as typically recreational and confined to weekend consumption, and several participants referred to themselves as 'psychonauts'. The majority reported commencing internet drug sourcing on Silk Road with little prior experience of cyber drug retailing prior to 2011 and finding out about the site by chance, for example when Googling, watching TV or browsing Craigslist. Van Hout and Bingham concluded that the need for a conscious decision on the part of the user to access Silk Road, as well as for technical resources and expertise, combined with the time needed for delivery, appears to exclude more vulnerable consumers. One of the conclusions here is that internet supply assumes planned drug use — which may explain why drugs such as MDMA appear to be more popular online. This raises important questions about whether or not and how the online market changes purchasing behaviour and consumption. Have those buying drugs from the internet bought drugs (the same ones in the same quantity) elsewhere?

Given the relatively low levels of internet purchasing, an important area explored further in this publication is the extent to which bulk or wholesale purchases of drugs are occurring online. Evidence is presented in Chapter 2 to suggest that drug dealers may be the primary customers for some dark net markets.

Dark net markets and interventions

Both demand reduction and supply reduction interventions on the surface web have been gathering pace (EMCDDA, 2013; Interpol, 2015). The deep web, however, has provided new opportunities and challenges

for both health and law enforcement professionals. A number of studies cited by authors in this publication suggest that Silk Road may have helped users reduce the harm caused by illicit drug use, particularly compared with street-based drug marketplaces. Examples include the sale of high-quality products with low risk for contamination, vendor-tested products, sharing of trip reports and online discussion of harm reduction practices (Barratt et al., 2013; Van Hout and Bingham, 2013, 2014). There appears to be a growing interest in the provision of health-related interventions directly to users of the deep web, and 'DoctorX' (www.elsubmarinodeldoctorx.com; see Chapter 7) offers a range of services to dark net market users, including information, advice and drug-testing services.

For law enforcement agencies, online monitoring represents a new approach to tackling drug markets, and they continue to build experience in this area, as described in Chapter 8. Law enforcement strategies are primarily focused on market disruption, which includes reducing trust around anonymity, as well as the identification, arrest and prosecution of sellers in cryptomarkets. Undercover officers may engage in covert operations by infiltrating markets, becoming a trustworthy buyer and arranging a face-to-face meeting. More overt tactics involve making individuals aware of police presence and ensuring that the takedown of markets receives media attention. At the EU level, Project: ITOM (Illegal Trade on Online Marketplaces) has established an EU cybercrime network, with one of its tasks being to establish effective ways to combat the illegal trade within online marketplaces.

A note on the structure of this publication

This publication is divided into four sections. In the first, the reader will find a series of chapters introducing dark net markets and their role, function and interaction with traditional drug markets, as well as the infrastructure and technology that support their operation. Section 2 includes a group of chapters that build on this topic by providing perspectives from different dark net market actors: drug users, health professionals and law enforcement practitioners. Section 3 expands the focus to look at a range of surface web drug markets, some of which overlap and interact with dark net drug supply. The final section pulls together some insights into and implications for the future in this area.

References

Aldridge, J. and Décary-Hétu, D. (2014), 'Not an "eBay for Drugs": the cryptomarket "Silk Road" as a paradigm shifting criminal innovation'. Available at: http://ssrn.com/abstract=2436643 or http://dx.doi.org/10.2139/ssrn.2436643

Barratt, M. J., Lenton, S. and Allen, M. (2013), 'Internet content regulation, public drug websites and the growth in hidden internet services', *Drugs: Education, Prevention and Policy* 20, pp. 195–202.

Barratt, M. J., Ferris, J. A. and Winstock, A. R. (2014), 'Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States', *Addiction* 109, pp. 774–783.

Chen, A. (2011), 'The underground website where you can buy any drug imaginable'. Available at: http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160

Christin, N. (2013), 'Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace', *Proceedings of the 22nd International Conference on World Wide Web, International World Wide Web Conferences Steering Committee*, Rio de Janeiro.

EMCDDA (2013), *Perspectives on drugs: Internet-based drug treatment*, Perspectives on Drugs series, European Monitoring Centre for Drugs and Drug Addiction, Lisbon.

EMCDDA (2015), *European drug report 2015: trends and developments*, European Monitoring Centre for Drugs and Drug Addiction, Lisbon.

European Commission (2014), 'Young people and drugs: Flash Eurobarometer 401'.

Forman, R. F. (2006), 'Narcotics on the net: the availability of web sites selling controlled substances', *Psychiatric Services* 57, pp. 24–26.

Interpol (2015), Operation Pangea, 2015, http://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea

Lahaie, E., Martinez, M. and Cadet-Taïrou A. (2013), 'New psychoactive substances and the Internet: current situations and issues', *Tendances* 84, Observatoire Français des Drogues et des Toxicomanies (OFDT). Available at: http://en.ofdt.fr/publications/tendances/new-psychoactive-substances-and-internet-tendances-84-january-2013/

Martin, J. (2014), 'Lost on the Silk Road: online drug distribution and the "cryptomarket"', *Criminology and Criminal Justice* 14(3), pp. 351–367.

Van Hout, M. C. and Bingham, T. (2013), '"Surfing the Silk Road": a study of users' experiences', *International Journal of Drug Policy* 24, pp. 524–529.

Van Hout, M. C. and Bingham, T. (2014), 'Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading', *International Journal of Drug Policy* 25(2), pp. 183–189.

SECTION I

Dark net cryptomarkets

CHAPTER 2
Cryptomarkets and the future of illicit drug markets

CHAPTER 3
Tor and links with cryptomarkets

CHAPTER 4
Staying in the shadows: the use of bitcoin and encryption in cryptomarkets

CHAPTER 5
Reputation is everything: the role of ratings, feedback and reviews in cryptomarkets

Overview

In Chapter 2, Judith Aldridge and David Décary-Hétu provide a brief introduction and history of the development of cryptomarkets on the deep web. They explore the impact of cryptomarkets on local and global drug markets, present some results from their own investigations of Silk Road marketplace shortly before it was taken down, and finally they offer consideration how drug cryptomarkets may be likely to impact on the global drugs trade should they should they continue to grow.

In the deep web, cryptomarkets facilitating drug trafficking have flourished during recent years due to the combination of anonymising software such as Tor, cryptocurrencies such as Bitcoin, and encrypted messaging. The Tor Browser enables users to anonymously host and browse content (e.g. websites) and services within a vast address space. In Chapter 3, Andrew Lewman, former director of the Tor Project, explains how this technology works, how it is used to create cryptomarkets and how law enforcement agencies are trying to identify criminals using it. He provides insight into the technical infrastructure that supports cryptomarkets and gives the reader a glimpse of what the next generation of these marketplaces might look like.

In Chapter 4, Joseph Cox follows up on the previous chapter by introducing the two other essential technologies that have made cryptomarkets possible: cryptocurrencies and encryption, explaining the process of Bitcoin transactions from their purchase to their exchange for regulated currency. He explains the rationale for using encryption and the tools that make it possible, as well as the process cryptomarket users go through to keep their communications anonymised. In Chapter 5, Joseph Cox provides the reader with an introduction to the role of ratings, feedback and reviews in cryptomarkets, including a look at why vendor reputation matters and how these systems may be abused.

2

CHAPTER 2

Cryptomarkets and the future of illicit drug markets

Judith Aldridge and David Décary-Hétu

Introduction

A cryptomarket is an online marketplace platform bringing together multiple vendors and listing mostly illegal and illicit goods and services for sale. Cryptomarkets have the same look and feel as surface web, or 'clear web', marketplaces such as eBay and Amazon, and they allow their customers to search and compare products and vendors. What differentiates these markets from established clear web marketplaces, however, is that they offer anonymity. Cryptomarkets employ a range of strategies to hide the identities of their participants, make transactions anonymous and conceal the physical locations of servers. These include anonymisation services, such as Tor (The Onion Router), that hide a computer's IP address when accessing the site (see Chapter 3); decentralised and relatively untraceable cryptocurrencies, such as bitcoin and litecoin, for making payments; and encrypted communication between market participants. Like some others (e.g. Barratt, 2012; Martin, 2013) we employ the term 'cryptomarkets', following early use of this term in hacker forums, but we note that the term 'dark net markets' is also gaining currency (e.g. Buxton and Bingham, 2015).

Although the academic research literature on cryptomarkets is growing (e.g. Barratt, 2012; Barratt et al., 2013, 2014; Martin, 2013, 2014; Van Hout and Bingham, 2013a, 2013b, 2014; Aldridge and Décary-Hétu, 2014, in press; Phelps and Watt, 2014; Buxton and Bingham, 2015; Dolliver, 2015; Décary-Hétu et al., in press), our understanding of these marketplaces has been shaped in no small part by journalists (e.g. Bartlett, 2014) ([1]), bloggers (e.g. Ormsby, 2014) and other independent researchers (e.g. Branwen, 2015). Through a combination of these efforts, we are able here to piece together evidence about and conjecture on the implications of cryptomarkets ([2]) for global and local drug markets.

This chapter begins by sketching a brief history of these markets and the technologies that gave rise to them. We chart the growth of the first cryptomarket, Silk Road, its demise, and the proliferation since of such marketplaces in spite of law enforcement activities. We show that, despite the growth and popularity of these markets, they tend to be short-lived, and their success substantially hampered by the growth of mistrust amongst market participants due to scams and, to a more limited extent, law enforcement activities. At present, cryptomarkets represent only a tiny fraction of the global drug trade. Their effect on how illicit drugs change hands is therefore minimal in global terms. Their potential for expansion is hampered by the fact that, given the risks of making international shipments, vendors elect to ship domestically in the absence of strong 'push' factors to do otherwise, and by the fact that the postal system through which all shipments must ultimately reach their destination remains a weak link. Nevertheless, drug cryptomarkets have substantial advantages for both buyers and sellers, and should be considered, we argue, a significant drug market innovation. They allow vendors operating on these markets to sell to unknown customers (thus shifting drug markets back to 'open', as opposed to the 'closed' markets many have become as a result of mobile phone technology) and to do so on a global scale; their appeal to drug sellers and their customers cannot be ignored.

We then consider how drug cryptomarkets, or some decentralised version of these (see Buxton and Bingham, 2015), may be likely to impact on the global drug trade should they overcome existing obstacles, continue to grow and ultimately flourish. Cryptomarkets allow for the possibility of a direct link between drug-using buyers and producers, growers or synthesisers of illicit drugs, and may eventually serve to cut out some of the middle level of the market. On the other hand, we know that a substantial proportion of cryptomarket

([1]) Also 'Wired,' http://www.wired.com/author/andygreenberg

([2]) It is important to note that our understanding of cryptomarkets is limited by the fact that these markets are, by their very nature, hidden. The ones that have come to the attention of researchers and others interested in documenting their activities tend to be English language and dominated by drug sales.

customers are drug dealers themselves, sourcing stock to sell offline, thereby allowing cryptomarkets to function in a middle market location. We conclude that both of these characterisations are likely to be true, depending on the drug in question. Finally, we consider the possibility that drug cryptomarkets may have some capacity to reduce the harm caused by drug markets by reducing the violence sometimes associated with these markets by virtue of their virtual location.

A brief history of drug cryptomarkets

Silk Road was the first cryptomarket devoted predominantly to the sale of illicit drugs, including cannabis, a wide range of psychedelic drugs, stimulant drugs such as cocaine, and prescription medications (Christin, 2013). Drugs were purchased online from vendors displaying eBay-style shopfronts and delivered through postal services. Buyers were protected by a system of escrow: they 'paid' for their purchases in the anonymous and difficult to trace cryptocurrency bitcoin (so no need for identity-carrying credit card payments), but payments were not released to vendors until buyers were satisfied with their deliveries (Aldridge and Décary-Hétu, 2014). This market functioned successfully because it was part of the hidden or 'dark' web, where all communications are anonymised by the Tor service. The site was launched in February 2011 and ran successfully for over two and a half years until the US FBI seized it on 2 October 2013.

Within weeks of Silk Road's closure, Silk Road 2.0 was launched, although by this time rival marketplaces were vying for dominance. One of these, Sheep, quickly grew to a size comparable to that of Silk Road, but a few weeks later its administrators shut down the site, claiming that a user had exploited a security loophole and stolen 5 400 bitcoins of their users' money (at the time worth around USD 6 million) (Pangburn, 2013), although many believed this was an 'exit scam' by the marketplace administrators, designed to enable them to abscond with the funds themselves. Throughout 2014, marketplaces grew in size, with Pandora, Agora, Hydra, Evolution and Silk Road 2.0 competing to win back the trust of vendors and buyers once the possibility of scams by marketplace administrators became apparent. Another exit scam by market administrators occurred on 18 March 2015, when the Evolution marketplace closed, with administrators reportedly having stolen USD 12 million from buyer and seller accounts (Woolf, 2015), with others since this time.

In November 2014, a little over a year after the original operation against Silk Road, cryptomarkets were hit once again by law enforcement agencies in Europe and the United States, in Operation Onymous. This time, multiple marketplaces were targeted, including Silk Road 2.0, Cloud 9 and Hydra (Department of Justice, 2014). Although many smaller marketplaces were also shut down, only the administrator of Silk Road 2.0 was arrested, alongside a small number of vendors. What was reportedly unique to this particular operation, however, was the undercover agent who had been involved from the start of the market working as an administrator (Afilipoaie and Shortis, 2015). As a result, the very aspect of cryptomarkets that provided their users with confidence in the platform — anonymity — may simultaneously have undermined that confidence; anonymity obscures the identities of criminals and law enforcement actors alike.

In spite of scams and law enforcement efforts, however, cryptomarkets continue to proliferate. Independent researcher Gwern Branwen, who has been systematically documenting and archiving these markets, found that 43 new markets opened in 2014 and 46 markets closed. Most of these closures, he estimates, were due to scams by marketplace administrators (or outside hacks), with only six closures attributable to law enforcement. Of the markets remaining in operation, nine opened during 2014 (Branwen, 2015). Soska and Christin (2015) found that these marketplaces are extraordinarily resilient, with law enforcement 'take-downs' resulting primarily in vendor displacement to other marketplaces. In summary, cryptomarkets tend to have a fairly short life, and their longevity is reduced more by scams than by law enforcement crackdowns. Our own data collection efforts tell us that, at the time of writing, four marketplaces are open, each with over 1 000 active listings.

The emergence of online sales of illicit drugs has been detailed by Buxton and Bingham (2015). They, and Martin (2014), refer to Markov's description of marijuana transactions as far back as 1971 between students at Stanford University and MIT using technology at the artificial intelligence laboratories that became the foundation of the internet. As we and others have discussed elsewhere (Aldridge and Décary-Hétu, 2014; Buxton and Bingham, 2015; Décary-Hétu and Aldridge, 2015), however, cryptomarkets are the direct descendants of markets for a range of illegal goods and services that emerged in the late 1990s and early 2000s. These markets were hosted in Internet Relay Chat (IRC) chat rooms and online discussion forums, providing participants with virtual locations where they could meet to arrange transactions. These 'first-

generation' online criminal markets were popular but not engineered for security; indeed, they did little to obfuscate the location of their servers. This led to a series of highly publicised arrests and shutdowns (Poulsen, 2012), and enabled law enforcement officials to access public and private messages as well as logs of connections, leading them directly to market participants. These markets, furthermore, were not terribly efficient; it was difficult to assess before purchase the trustworthiness of vendors or the quality of the goods and services they sold. Because of the rudimentary security features of these online platforms, therefore, criminal operators could face a considerable degree of victimisation both from vendors and platform administrators (Décary-Hétu and Aldridge, 2015).

Cryptomarkets, the 'second-generation' online criminal markets, represent a step change in criminal innovation (Aldridge and Décary-Hétu, 2014). Visually, they look just like any other legitimate online marketplace (eBay, for example): they bring together a range of vendors in one location, each listing products for sale, and allow customers to comparison-shop. They offer the same opportunities for networking and carrying out business transactions as the first-generation criminal markets, but in a much more secure environment. Cryptomarkets did not invent any technology per se, but they brought together four security measures never used in conjunction before. First, cryptomarkets require that participants make their payments in virtual currencies such as bitcoin. Transactions made in virtual currencies are exceptionally difficult to trace and their use does not entail checks by regulatory agencies, for example in relation to anti-money laundering legislation. Second, cryptomarkets require that their participants use an anonymising protocol, such as Tor or the Invisible Internet Project (I2P), to hide their identities when connecting to them. Cryptomarkets also take advantage of these protocols to hide their IP addresses, thereby hindering the ability of law enforcement to seize their servers. The remaining two measures are aimed at providing buyers with security and confidence in relation to their transactions. Cryptomarkets use escrow systems, and finally, they employ feedback or purchase review systems similar to those found on large online merchant sites such as Amazon and eBay. Buyers can check the feedback scores for vendors and their products to help them evaluate the likelihood that they will be buying the product they want from a trusted vendor (Van Hout and Bingham, 2013).

The impact of cryptomarkets on global and local drug markets

A number of estimates — by Christin (2013) and by Aldridge and Décary-Hétu (2014) — of revenue generation ([3]) on Silk Road before it was first shut down suggest that the marketplace generated around USD 16.7 million in 2012 and USD 89.7 million in 2013 ([4]). Estimating the value of the global trade in illicit drugs, by comparison, is notoriously difficult (Reuter and Greenfield, 2001). Estimates regularly quoted in the media that ostensibly derive from the United Nations Office on Drugs and Crime (UNODC) estimates range from USD 300 billion to USD 1.3 trillion annually, but the methodologies employed, it has been argued, generate little more than wild guesses (Thoumi, 2005). Even in the absence of a sensibly derived estimate of the global drug trade, however, we can be sure that sales on cryptomarkets are likely to represent only a tiny fraction of the global drug trade.

This should be unsurprising, since the bulk of supply and trafficking activities in the worldwide drug trade rely on conventional interpersonal networks of drug manufacturers, wholesalers and brokers (Martin, 2014). At first glance, then, it seems unlikely that cryptomarkets will have had much of an impact on traditional drug markets.

However, as Martin goes on to argue persuasively:

> Cryptomarkets transform conventional drug sales by facilitating the creation of global networks of offenders. These networks comprise both vendors and purchasers of illicit drugs who, once online, are able to conduct a range of illicit activities not only on an unprecedented scale, but also with a degree of freedom that significantly exceeds what is possible through conventional, interpersonal criminal networks. ... This suggests that cryptomarkets facilitate a form of illicit drug sales that is qualitatively different from the conventional, offline variety. (Martin, 2014, p. 10)

([3]) These estimates were made possible by the automated feedback system that strongly encouraged buyers to leave feedback on vendors, so that feedback could be used as a proxy measure for a transaction with reasonable confidence. Our research indicated that about 88 % of buyers posted publicly available feedback after a purchase (Aldridge and Décary-Hétu, in press). By multiplying the number of transactions received by the price of a listing, it was possible to estimate the sales generated on cryptomarkets with a high level of certainty.

([4]) By the time of its closure, the first Silk Road was a well-functioning, confident, successful and growing market; no cryptomarket since has operated with the same success or in an environment with the same confidence, and, even if some of these second-generation markets generate high revenues, their instability and short lifespans suggest that our best source of data about a well-functioning cryptomarket remains the first Silk Road.

In other words, it seems likely that the kind of trade facilitated by drug cryptomarkets may not simply replace conventional trade but supplement it, for example by catering to a different kind of buyer, able to purchase a range of substances not previously available to them. Christin (2014) has recently underlined the importance of this question for future research: do cryptomarkets primarily displace drug purchases from traditional markets or instead provide access to drugs for those without previous access?

We have already discussed the loss of confidence in cryptomarket platforms on the part of both buyers and vendors following scams and law enforcement activities, creating a potential limiting factor for the future growth of drug cryptomarkets, but there are additional factors that may impose limitations on the growth of these markets. Access to them requires a degree of technological knowledge; for example, a buyer needs to understand how to use Tor or another anonymising service and how to purchase and use a cryptocurrency. Some of those who are willing and able to learn to use these services may simply mistrust the security they afford, particularly in light of media coverage of arrests associated with cryptomarkets. Furthermore, cryptomarket drug purchases require advance planning: some drug users may be unwilling to plan their drug use sufficiently in advance, preferring instead to make purchases from known dealers, in person, who can supply their requirements as and when the desire for consumption arises. Another limitation on the growth of cryptomarkets arises from the fact that drugs must be sent using postal systems, with the accompanying risks that result from monitoring and seizure, which can take place both within and at borders. It seems likely that some drug users may be unwilling to purchase from cryptomarkets because of a reluctance to have illicit drugs sent to them through the post, perceiving that doing so carries risks and preferring their existing access to drugs through known and trusted retail dealers.

This concern about the risks of sending/being sent illicit drugs through the post may be heightened where drugs are shipped across international borders. Shipping across borders carries greater risks for both vendors and their buyers because of the increased chance that a package will be searched and confiscated. From the vendor's point of view, this increases the risk of customer dissatisfaction if a package is not received, potentially affecting the vendor's ever-important feedback rating. From the customer's point of view, having illegal goods shipped to an address formally connected to them might be a risk they are especially unwilling to take if those packages risk being confiscated or held at borders. Shipments across international borders also simply take more time and cost more than purchases made within local jurisdictions. For all these reasons, both customers and vendors may prefer illegal goods to be shipped only within their own country's borders.

The authors' own research, based on data collected from Silk Road in September 2013, just before closure, confirmed this: vendors generally chose only to ship domestically (71 % of US vendors, for example) unless there were substantial 'push' factors to do otherwise. Our multivariate analysis found six such push factors: (i) insufficient domestic demand for illicit drugs; (ii) a perceived lower effectiveness of law enforcement, making it safer for vendors to operate internationally with impunity; (iii) a lower GDP per capita that limits the purchasing power of local customers; (iv) a lower vendor rating which makes it more difficult to compete on the national level against vendors who have a perfect rating score; (v) the scope of the products offered by vendors measured by the number of listings offered and; (vi) the sale of smaller packages (as measured in weight) given that it should be easier for these packages to pass through the inspections at the borders undetected (Décary-Hétu et al., in press). These results suggest that, although cryptomarket vendors can theoretically sell in a global marketplace, many elect not to in the absence of substantial factors pushing them to do so.

Even though cryptomarkets still have a minor market share in the overall illicit drug trade, evidence suggests that they may be expanding. Research by Barratt et al. (2014) using Global Drugs Survey data suggests that, among survey respondents who usually buy their own (primarily recreational) drugs, access to drugs via the first Silk Road was not insubstantial. In Australia, the United Kingdom and the United States, 7 %, 10 % and 18 % of the sample (respectively) had consumed drugs purchased via the first Silk Road, and just over half of these had self-purchased (between 5 and 10 %). Customers appreciate the ease of access and the quality and range of products that cryptomarkets offer, as well as perceiving these markets as providing them with a higher level of security than street drug markets (Barratt et al., 2014). Drug sellers perceive the likelihood of arrest to be substantially reduced and appreciate access to a much larger potential market of buyers (Van Hout and Bingham, 2014).

This last point — cryptomarket vendors having access to a larger market of buyers — has important implications for the potential effects of drug cryptomarkets on local and global drug markets. Cryptomarket dealers can effectively transcend the physical restrictions of a local drug market — the limited number of people they could physically reach to transact with — to supply, through postal

delivery, a (potentially) worldwide market. In recent years, many drug markets have moved from 'open' to 'closed', in which drug dealers sell only to those customers with whom they have trusted relationships (see May and Hough, 2004). However, cryptomarkets reverse this arrangement, with vendors able to transact with unknown customers, whom they encounter only in the virtual sphere (Aldridge, 2012; Aldridge and Décary-Hétu, 2014).

There is some debate about the extent to which drug cryptomarkets, if they continue to proliferate and grow, will change the structure of drug markets. To the extent that these markets allow a direct link between drug-using customers and producers, cryptomarkets may serve to cut out some of the middle or wholesale level in the drug market chain (Martin, 2013) and/or may reduce the links in the chain between producer and end-user. We have argued, in contrast, that cryptomarkets may instead in part function at the middle level of the drug market.

Our evidence is derived from an analysis of the nearly 12 000 listings on Silk Road downloaded in September 2013, only weeks before it was shut down by the FBI (Aldridge and Décary-Hétu, in press). Wholesale-level revenue generation (sales for listings priced over USD 1 000) accounted for about a quarter of the revenue generation on the first Silk Road overall. Ecstasy-type drugs dominated wholesale activity on this marketplace, but we also identified substantial wholesale activity for benzodiazepines and prescription stimulants. Less important, but still generating wholesale revenue, were cocaine, methamphetamine and heroin. Although vendors on the marketplace were located in 41 countries, wholesale activity was confined to only a quarter of these, with China, the Netherlands, Canada and Belgium prominent. The terminology employed by vendors in some instances made this explicitly clear; for example, one cannabis seller stated: 'This is a mid-grade commercial hash perfect for resale due to the low price.' The fact that vendors gave substantial discounts for bulk purchase seems likely to have further facilitated the likelihood that purchases made there by drug dealers could have made for profitable offline resale (Aldridge and Décary-Hétu, 2014). These large-sized purchases could have been made by customers for a number of reasons, such as for personal use over a long period or 'social supply' (with the purchases made by one individual on behalf of a group of friends) (Aldridge et al., 2011; Coomber and Moyle, 2013). However, the sometimes very large prices/sizes of the purchases provide compelling evidence that a substantial proportion of customers on Silk Road were drug dealers sourcing stock.

Therefore, Silk Road functioned as a virtual broker, connecting upper-, mid- and retail-level sellers. So although it is possible, as Martin (2013) argued, that drug cryptomarkets may directly connect producers/synthesisers with drug users buying for their own use, thereby cutting out the middle level of the market, our findings suggest that cryptomarkets may also perform a middle market function. It seems likely that both of these characterisations may be true simultaneously, depending on the drug in question. We suspect, for example, that direct producer–user transactions are more likely for the kinds of drugs where small-scale producers can operate without large-scale international networks (cannabis, for example, and easy-to-produce psychedelic drugs such as mushrooms, varieties of NBOMe and DMT). These direct producer–user transactions seem much less likely for drugs such as cocaine or heroin, both of which require large-scale international networks for distribution. We have not yet disentangled the potential effects that the online drug trade has on global and local markets in this regard, and this remains a fruitful avenue for future research.

Finally, we consider the possibility that cryptomarkets may have the capacity to reduce the harm caused by drug markets in some important ways. Others (e.g. Ormsby, 2014; Van Hout and Bingham, 2014; Caudevilla, see Chapter 7) refer to the online culture of harm reduction that was evident in the first Silk Road, and many have referred to the high level of purchase satisfaction amongst its customers, suggesting that drug quality may be superior to that in traditional retail drug markets. Recent research by Caudevilla (see Chapter 7) shows positive results on the quality of cryptomarket purchases for 129 samples submitted by cryptomarket customers to Energy Control's testing service. In 120 (93 %) of the samples submitted, the drug that customers thought they had purchased was the only psychoactive substance detected. The purity of cocaine samples submitted (n = 54) was high (mean 70.4 % purity) compared with that we see reported for street seizures in the United Kingdom, for example, which averaged 38 % in 2013 (Burton et al., 2014). In addition to the possibility of these markets being 'good' in this sense for drug users, these markets may also be 'good' for drug dealers and for the environments in which they operate. Before the advent of online availability of bulk-quantity illicit drugs, dealers had to have on-the-ground connections and relationships of trust built with middle-level drug dealers and/or importers in order to be able to acquire product (McCarthy and Hagan, 2001; Morselli, 2001), as well as a tough reputation (Topalli et al., 2002). With the advent of the cryptomarket, almost anyone with sufficient technological skills can access stock. In other words, the type of 'subcultural capital' (Thornton, 1995) required to be a drug dealer is likely to be different for those who operate on a cryptomarket.

This new type of drug dealer is also likely to be relatively free from the violence typically associated with traditional drug markets (Caulkins and Reuter, 2009). Traditional illicit markets do not have the state (police, trading standards) to adjudicate disputes; in virtual markets, the marketplaces have regulatory mechanisms that function in this way (escrow, seller and buyer trust metrics, marketplace adjudication of disputes), removing some of the unstable factors in illegal markets. Because of the virtual location of online drug markets, in addition to the presence of conflict-reducing features such as escrow and bitcoin, violence and theft are likely to be reduced. It is probable that these changes will have a deep impact on the skills needed to succeed in criminal markets. In the drug cryptomarket era, having good customer service and writing skills, and a good reputation, via feedback, as a vendor or buyer may be more important than muscles and face-to-face connections.

Although it may seem self-evident that the virtual location of online drug markets should reduce violence because interactions there occur in virtual rather than in physical space, this potential capacity of cryptomarkets to reduce harm may have limitations. Our research (Aldridge and Décary-Hétu, 2014, in press) showed that cryptomarket customers are likely to include drug dealers sourcing stock to sell offline. For this reason, cryptomarkets remain 'anchored' in offline drug markets, with vendors there also purchasing offline to sell online. The requirement, therefore, to operate either wholesale purchase or retail sales in offline drug markets means that cryptomarket users may still be victims and perpetrators of violence connected with these face-to-face transactions. In addition, harm can manifest itself in forms other than real-world violence: threats; damage to reputation; 'doxing' (hacking and then threatening to expose the victim's identity) and other forms of blackmail; theft and fraud; and cyber-bullying. Finally, the violence associated with drug markets may be culturally, politically and socially conditioned (Bourgois, 2003; Johnson et al., 2006), rather than arising as a function of the illegal market itself. To the extent that these external conditions remain unchanged, the ability of cryptomarkets to reduce violence and conflict may be limited. All these questions need to be addressed empirically.

Conclusion

Cryptomarkets are still very much in their infancy. Market administrators are learning how best to protect their activities and their participants from law enforcement, while law enforcement actors are learning how to investigate and clamp down on this drug market innovation. One important question must therefore be asked: given the potential we've discussed here for harm reduction to arise from the online drug trade — for drug dealers, for users and within the markets themselves — should drug cryptomarkets be a high priority for law enforcement? We might consider reframing the problem: instead of deeming cryptomarkets problematic because the criminals operating there are harder for law enforcement to reach, perhaps we should consider the possibility that cryptomarkets reduce the problems associated with this kind of criminality. The extent to which harm might actually be reduced by cryptomarkets, however, remains an open question that requires systematic empirical research.

The impact that cryptomarkets have will depend largely on the shifting balance between the success of those seeking to set up and run effective cryptomarkets with longevity, on the one hand, and the investigative success of law enforcement, on the other. Law enforcement may seem to have the upper hand, having successfully closed large cryptomarkets two years in a row. However, the limited number of arrests made and quantity of drugs seized, and the proliferation of markets that has followed each law enforcement effort, suggest that these police operations are having only a limited impact. For now, it seems inevitable that the internet will continue to be a source of drug market innovation.

References

Afilipoaie, A. and Shortis, P. (2015), *Operation Onymous: international law enforcement agencies target the dark net in November 2014*, GDPO Situation Analysis, Global Drug Policy Observatory, Swansea.

Aldridge, J. (2012), 'Dealers in disguise: the virtualisation of retail level drugs markets', http://www.youtube.com/watch?v=q4ZsNuC2kqg

Aldridge, J. and Décary-Hétu, D. (2014), 'Not an "eBay for drugs": the cryptomarket "Silk Road" as a paradigm shifting criminal innovation'. Available at: http://ssrn.com/abstract=2436643 or http://dx.doi.org/10.2139/ssrn.2436643

Aldridge, J. and Décary-Hétu, D. (in press), 'Hidden Wholesale: How drug cryptomarkets may transform traditional "offline" drug markets', *International Journal of Drug Policy*.

Aldridge, J., Measham, F. and Williams, L. (2011), *Illegal leisure revisited: changing patterns of alcohol and drug use in adolescents and young adults*, Routledge, Sussex and New York.

Barratt, M. J. (2012), 'Silk Road: eBay for drugs', *Addiction* 107, pp. 683–684.

Barratt, M. J., Ferris, J. A. and Winstock, A. R. (2014), 'Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States', *Addiction* 109(5), pp. 774–783.

Barratt, M. J., Lenton, S. and Allen, M. (2013), 'Internet content regulation, public drug websites and the growth in hidden Internet services', *Drugs: Education, Prevention and Policy* 20, pp. 195–202.

Bartlett, J. (2014), *The dark net*, Random House, London.

Bourgois, P. I. (2003), *In search of respect: selling crack in El Barrio*, Cambridge University Press, Cambridge.

Branwen, G. (2015), '2014 in DNMs: by the numbers', http://www.reddit.com/r/DarkNetMarkets/comments/2r58vs/2014_in_dnms_by_the_numbers/

Burton, R., Thomson, F., Visintin, C. and Wright, C. (2014), *United Kingdom drug situation: Annual report to the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) 2014*, United Kingdom Focal Point at Public Health England, London.

Buxton, J. and Bingham, T. (2015), *The rise and challenge of dark net drug markets*, Global Drug Policy Observatory, Swansea.

Caulkins, J. and Reuter, P. (2009), 'Towards a harm-reduction approach to enforcement', *Safer Communities* 8, pp. 9–23.

Christin, N. (2013), 'Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace', WWW 2013, International World Wide Web Conference Committee (IW3C2), Rio de Janeiro, Brazil, preliminary version revised in November 2012. Available at: https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf

Christin, N. (2014), 'Commentary on Barratt et al. (2014): steps towards characterizing online anonymous drug marketplace customers', *Addiction* 109, pp. 784–785.

Coomber, R. and Moyle, L. (2013), 'Beyond drug dealing: developing and extending the concept of "social supply" of illicit drugs to "minimally commercial supply" ', *Drugs: Education, Prevention and Policy* 21, pp. 157–164.

Décary-Hétu, D. and Aldridge, J. (2015), 'Sifting through the Net: Monitoring of online offenders by researchers', *European Review of Organised Crime* 2(2), pp. 122–141.

Décary-Hétu, D., Paquet-Clouston, M.-C. and Aldridge, J. (in press), 'Drug cryptomarkets facilitating drug sales on a global scale: An analysis of the factors that encourage or prevent sales across international borders', *International Journal of Drug Policy*.

Department of Justice (2014), 'Dozens of online "dark markets" seized pursant to the forfeiture complaint filed in Manhattan Federal Court in conjunction with the arrest of the operator of Silk Road 2.0', http://www.justice.gov/usao/nys/pressreleases/November14/DarkMarketTakedown.php

Dolliver, D. S. (2015), 'Evaluating drug trafficking on the Tor Network: Silk Road 2.0, the sequel', *International Journal of Drug Policy*. Available at: http://www.sciencedirect.com/science/article/pii/S0955395915000110

Johnson, B., Golub A. and Dunlap, E. (2006), 'The rise and decline of hard drugs, drug markets, and violence in inner-city New York', in Blumstein, A. and Wallman, J. (eds), *The Crime Drop in America*, Cambridge University Press, Cambridge, pp. 164–206.

McCarthy, B. and Hagan, J. (2001), 'When crime pays: capital, competence, and criminal success', *Social Forces* 79(3), pp. 1035–1060.

Martin, J. (2013), 'Lost on the Silk Road: Online drug distribution and the "cryptomarket"', *Criminology and Criminal Justice*, published online 7/10/2013, doi: 10.1177/1748895813505234.

Martin, J. (2014), *Drugs on the dark net: how cryptomarkets are transforming the global trade in illicit drugs*, Palgrave Macmillan, Basingstoke.

May, T. and Hough, M. (2004), 'Drug markets and distribution systems', *Addiction Research and Theory* 12(6), pp. 549–563.

Morselli, C. (2001), 'Structuring Mr. Nice: entrepreneurial opportunities and brokerage positioning in the cannabis trade', *Crime, Law and Social Change* 35(3), pp. 203–244.

Ormsby, E. (2014), *Silk Road*, Macmillan, Sydney.

Pangburn, D. (2013), 'Did one of the Silk Road's successors just commit the perfect Bitcoin scam?', http://motherboard.vice.com/blog/did-one-of-the-silk-roads-successors-just-commit-the-perfect-bitcoin-scam

Phelps, A. and Watt, A. (2014), 'I shop online — recreationally! Internet anonymity and Silk Road enabling drug use in Australia', *Digital Investigation* 11(4), pp. 261–272.

Poulsen, K. (2012), *Kingpin: how one hacker took over the billion-dollar cybercrime underground*, Random House, New York.

Reuter, P. and Greenfield, V. (2001), 'Measuring global drug markets', *World Economics* 2(4), pp. 159–173.

Soska, K. and Christin, N. (2015), 'Measuring the longitudinal evolution of the online anonymous marketplace ecosystem', SEC'15 *Proceedings of the 24th USENIX Conference on Security*, Washington, DC.

Thornton, S. (1995), *Club cultures: music, media and subcultural capital*, Polity Press, Cambridge.

Thoumi, F. E. (2005), 'The Colombian competitive advantage in illegal drugs: the role of policies and institutional changes', *Journal of Drug Issues* 35(1), pp. 7–26.

Topalli, V., Wright, R. and Fornango, R. (2002), 'Drug dealers, robbery and retaliation: vulnerability, deterrence and the contagion of violence', *British Journal of Criminology* 42(2), pp. 337–351.

Van Hout, M. C. and Bingham, T. (2013a), ' "Silk Road", the virtual drug marketplace: a single case study of user experiences', *International Journal of Drug Policy* 24(5), pp. 385–391.

Van Hout, M. C. and Bingham, T. (2013b), ' "Surfing the Silk Road": a study of users' experiences', *International Journal of Drug Policy* 24(6), pp. 524–529.

Van Hout, M. C. and Bingham, T. (2014), 'Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading', *International Journal of Drug Policy* 25(2), pp. 183–189.

Woolf, N. (2015), 'Bitcoin "exit scam": deep-web market operators disappear with $12m', http://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars

3

CHAPTER 3
Tor and links with cryptomarkets

Andrew Lewman

Introduction

Recent years have seen the development of software that allows individuals to browse the internet anonymously and which supports the anonymous hosting of content and services on the internet. This chapter provides an introduction to Tor: how it works, its 'hidden services' feature and how cryptomarkets, particularly those selling drugs, use its features. It also gives an overview of the development of cryptomarkets and the potential future of such markets.

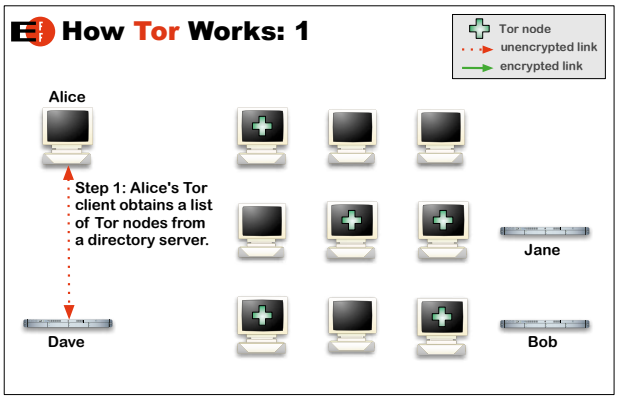
The Tor Project

The Tor Project ([1]) researches and develops software to enable people to maintain their privacy and anonymity while on the internet. The most popular product is the Tor Browser ([2]), which has been downloaded hundreds of millions of times over the past few years. The Tor Browser is a web browser, much like a normal browser such as Internet Explorer, Safari, Chrome or Firefox. However, it has the Tor Network built in and enabled by default. The Tor Network provides around 7 000 relays ([3]) (as of February 2015) for global usage. The Tor Network, and the underlying Tor Browser software, both rely upon a protocol known as 'onion routing'. Onion routing was originally a project of the US Naval Research Laboratory ([4]) in the 1990s. The core of onion routing is separating where you are in the world and on the network from where you are connecting in the world and on the network. Onion routing, and therefore the Tor Browser, provides a 'flexible communications infrastructure that is resistant to both eavesdropping and traffic analysis'. Eavesdropping is the ability of one or many secret parties to see, record or otherwise listen in to your communications with or without your knowledge. Traffic analysis is the ability to infer who is talking to who, how much they talk and how frequent their communications are.

As an analogy, think of your post office: the postal system can learn how often you send letters or packages, how large the letters or packages are, and who the sender and recipient of each letter or package is. This provides a simple example of how easy it is to map your contacts and easily sort them into most frequently contacted, most content sent/received, and so on. On the internet, anyone eavesdropping on your internet connection will be able to collect vast amounts of data about you just by watching your connection to the network. This is true regardless of the type of internet connection, whether it's from a mobile phone, or a fixed line to your residence or office, or the Wi-Fi available at your favourite coffee shop.

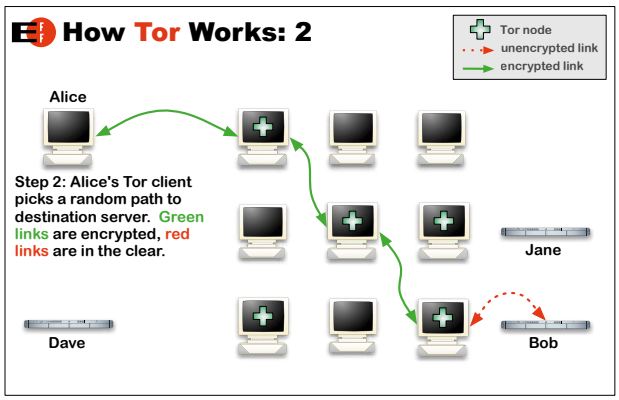
Onion routing works by wrapping your communications in layers of encryption and routing them around the world. The Tor Browser uses the Tor Network to accomplish this encryption and global routing. The following figures will help you to visualise how this happens behind the scenes. Alice wishes to privately browse the websites of Bob and then Jane. Perhaps Bob is her favourite news website, and Jane is her favourite social networking website.

FIGURE 3.1
The first stage of the Tor Browser as started on your computer



([1]) http://www.theonionrouter.com/
([2]) http://www.theonionrouter.com/projects/torbrowser
([3]) http://metrics.torproyect.org/networksize.html
([4]) http://www.onion-router.net/

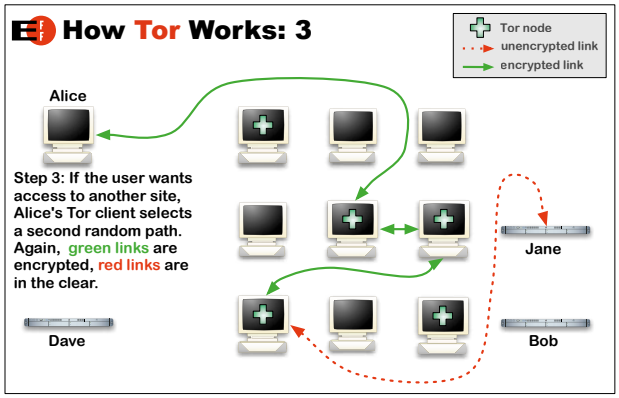
FIGURE 3.2
The Tor Browser makes a connection through the Tor Network



What happens behind the scenes is that the Tor Browser contacts special relays, known as directory authorities, in the Tor Network; directory authorities maintain a list of all possible relays at any given moment. The Tor Browser downloads this information and builds a list of plausible relays for selection. Figure 3.1 shows the basic setup. The Tor Browser software then chooses three relays and builds a series of circuits directly from your machine to each relay. Figure 3.2 shows how this works. If, after browsing Bob's website, Alice then wants to browse Jane's website, her Tor Browser easily accommodates this request. It simply builds a new set of circuits through the Tor Network and, following the same logic as the first request, allows access to the new destination, in this case Jane's website. Figure 3.3 shows how this occurs.

Relays are merely computers that switch traffic from one computer to another. The computers can be your own computer, one of the 7 000 computers comprising the Tor Network, or the destination you're trying to reach through the Tor Browser. A virtual circuit is a means of transporting data over a computer network in such a way that it appears as though there is a dedicated physical layer link between the source and destination end systems of these data. Relays run the Tor software, which enables them to talk to you, other relays or destinations on the Internet. Circuits are connections through the relays on which your traffic flows from start to finish. Circuits in Tor are typically active for 10 minutes before being pulled down and created with a different set of relays.

FIGURE 3.3
The Tor Browser then browses another website using the same circuit as before



Let's extend the postal service analogy to how Tor works. Alice wants to send a letter to Bob, but because of the sensitivity of the materials, she wants to keep it private. Alice writes out three envelopes: one to Alfred, one to Barbara and one to Charles. She puts her materials for Bob into the envelope for Charles. She then puts the envelope for Charles into the envelope for Barbara. Finally, she puts the Barbara envelope into the Alfred envelope. Alice takes this stuffed envelope to the post office. It's then sent to Alfred. Upon receiving the envelope, Alfred opens it up and drops the envelope for Barbara in the post to her. The post office then delivers this envelope to Barbara. When it arrives, she opens the envelope and sees a letter for Charles. Barbara hands this letter to the postal service, which then delivers it to Charles. Charles receives the letter and sends it off to Bob. Finally, after having the materials delivered through Alfred, Barbara and Charles, Bob opens his envelope and views the materials from Alice. Imagine Alfred, Barbara and Charles are in different countries. Someone watching each individual postal system could learn about each individual point, but not that the original message went from Alice to Bob.

Hidden services with Tor

The Tor Browser also provides a feature known as hidden services ([5]). This is the ability to anonymously host and browse content and services within a vast address space. A hidden service needs to advertise its existence in the Tor Network before clients will be able to contact it. Therefore, the service randomly picks some relays, builds circuits to them and asks them to act as *introduction points* by telling them its public key. Note that in Figures 3.1–3.3 the green links are circuits rather than direct connections. By using a full Tor circuit, it is hard for anyone to associate an introduction point with the onion server's IP address. Although the introduction points and others are told the hidden service's identity (public key), they do not discover the onion server's location (IP address).

([5]) http://www.theonionrouter.com/docs/hidden-services.html.en

The hidden service then assembles a descriptor, containing its public key and a summary of each introduction point, and signs this descriptor with its private key. It uploads that descriptor to a distributed hash table ([6]). The descriptor will be found by clients requesting XYZ.onion, where XYZ is a 16-character name derived from the service's public key. After this step, the hidden service is set up.

A client that wants to contact a hidden service needs to learn its onion address first. After that, the client can initiate connection establishment by downloading the descriptor from the distributed hash table. If there is a descriptor for XYZ.onion (the hidden service could be offline or have left long ago, or there could be a typo in the onion address), the client now knows the set of introduction points and the right public key to use. At this point, the client also creates a circuit to another randomly picked relay and asks it to act as rendezvous point by telling it a one-time secret.

When the descriptor is present and the rendezvous point is ready, the client assembles an introduce message (encrypted to the hidden service's public key) including the address of the rendezvous point and the one-time secret. The client sends this message to one of the introduction points, requesting that it be delivered to the hidden service. Again, communication takes place via a Tor circuit: nobody can relate the introduce message to the client's IP address, so the client remains anonymous.

The hidden service decrypts the client's introduce message and finds the address of the rendezvous point and the one-time secret in it. The service creates a circuit to the rendezvous point and sends the one-time secret to it in a rendezvous message.

In the last step, the rendezvous point notifies the client about successful connection establishment. After that, both client and hidden service can use their circuits to the rendezvous point for communicating with each other. The rendezvous point simply relays (end-to-end encrypted) messages from client to service and vice versa.

In general, the complete connection between client and hidden service consists of six relays, three of them picked by the client (the third being the rendezvous point) and the other three picked by the hidden service. The details of these messages and hidden service protocols are further described in the rendezvous specification (Lewman, 2015).

([6]) http://en.wikipedia.org/wiki/Distributed_hash_table

The current state of hidden services

Hidden services have attracted the attention of the research community. The research community has tried to both challenge (Murdoch, 2006; Øverlier and Syverson, 2006a) and enhance (Øverlier and Syverson, 2006b) the anonymity provided by hidden services. Further research aims to gather basic data on the content hosted in a set of published hidden services (Biryukov et al., 2013). The Memex project by the US Defense Advanced Research Projects Agency has been working to identify all available hidden services published over time ([7]). The goal is to develop a search engine-like interface to the automatically indexed data set. This will allow for easier demographic determination of content and services available in 'onion land'.

A recent blog post by the Tor Project ([8]) looks at the volume of hidden services traffic. It estimates that there are around 30 000 active hidden services serving around 5 terabytes of information daily. Compared with the 268 million available domains ([9]), this is a small number.

Independently of Tor, there is a general-purpose search engine for hidden services at Ahmia ([10]). Its 'mission is to create a working search engine for indexing, searching and cataloguing content' in the Tor onion space. The website provides some data suggesting that, as of 12 February 2015, around 2 274 hidden services existed ([11]). Much like Google, Yahoo and Bing all have different counts of how many websites exist on the clear internet, so do Tor and Ahmia for the hidden internet. One difference that accounts for Tor Project's and Ahmia's differing numbers is that Ahmia only counts websites that are available to be indexed. Tor Project counts total hidden services available, which includes non-website addresses.

Cryptomarkets

The first iteration

A certain type of hidden service website has gained notoriety through the attention of the global media. The most written about and well-known website is the Silk

([7]) C. White on http://www.darpa.mil/Our_Work/I2O/Programs/Memex.aspx
([8]) https://blog.torproject.org/blog/somo-statistics-about-onions
([9]) http://www.domaintools.com/statistics/tld-counts/ (retrieved 12/2/2015)
([10]) https://ahmia.fi/search/
([11]) https://ahmia.fi/stats/viewer

Road marketplace. Silk Road was a unique black market created as a hidden service with a custom-generated domain name, now defunct, silkroad6ownowfk.onion. What helped Silk Road, and the now many clones of it, work and survive for years was a combination of Tor hidden services and the digital currency bitcoin ([12]). The heavy use of cryptography in both products, which were the basic building blocks of the market, spawned the term 'cryptomarket'. In essence, a cryptomarket is similar to Amazon, eBay and many other internet-based commerce websites. For example, eBay is run by a company in the United States, hosted at the domain name www.ebay.com, and works with known vendors and suppliers around the world to provide a large variety of products for global consumers to purchase. What makes eBay work is the software and financial management processes behind the scenes, allowing both consumers and vendors to purchase and sell goods through their site. EBay receives a small percentage of every sale resulting from a listing or advertisement on its websites, as well as charging some other fees. The first iteration of cryptomarkets are nothing more than similar software and financial logistics hosted on an onion domain using the bitcoin cryptocurrency. The largest difference is that the customers and vendors are knowingly participating in a global black market. Cryptomarkets also differ in that they allow the purchase and sale of both digital and non-digital goods to a global customer base with the goal of providing private transactions through the use of a hidden service and digital currency. Deep Dot Web maintains a directory of cryptomarkets ([13]).

Architecture of a cryptomarket

The technology involved in running this type of cryptomarket is pretty basic. Tor's hidden services allow anyone with a running Tor client to configure and host a service on any device, from a laptop, desktop computer or mobile phone to a large and powerful dedicated computer, commonly called a server, located in a dedicated, well-connected and reliable data centre. The commoditisation of software and hardware lets anyone build such a cryptomarket infrastructure for very little money. It requires only hardware (such as a laptop), an operating system, e-commerce software, integration with a bitcoin payment processor, and installation and configuration of Tor to provide a hidden service address at the web server. If a market grows and the hardware starts to fail, all the software and the hidden service can be migrated to a dedicated hosting service ([14]).

([12]) https://bitcoin.org/en/
([13]) http://www.deepdotweb.com/marketplace-directory/listing/
([14]) https://en.wikipedia.org/wiki/Dedicated_hosting_service

The Invisible Internet Project (I2P) ([15]) is an alternative to Tor hidden services. It is an overlay network based on passing messages between routers using 'garlic routing' with a distributed hash table for a global directory of available routers. All users of I2P are also running routers to pass encrypted traffic between other routers. A few cryptomarkets have recently started to use I2P as an alternative to Tor hidden services (O'Neill, 2013). Websites hosted via I2P are referred to as 'eepsites'.

Organised crime and cryptomarkets

As cryptomarkets become easier to set up and use, it's natural for them to attract more customers and sellers of a less technically inclined mindset. As sellers realise the potential to generate profits with less risk of physical violence and no need for face-to-face contact with their buyers, more organised groups move in. Groups already accustomed to trafficking illegal materials can adapt to the internet and cryptomarkets very easily. Local street dealers can attract more clients and increase their sales to move up the hierarchy in criminal organisations. The 'Dread Pirate Roberts' of Silk Road allegedly interacted with the Hells Angels organisation while running the site (Paul, 2015). Through his trial, it came to light that a Canadian chapter of the Hells Angels organisation was the supplier to a seller on Silk Road. This provides a concrete example of how organised crime can be involved with cryptomarkets.

It is likely that the Canadian Hells Angels were part of a larger transnational organised crime (TOC) network (Albanese and Reichel, 2014). A TOC network may be engaged in sourcing illegal narcotics, transporting them across national borders and ultimately selling them to local clients or expanding to international clients through the internet and cryptomarkets. The 'surface web' is still far more commonly used to sell drugs than esoteric 'dark web' marketplaces (EMCDDA, 2015). However, the increasing ease of use of cryptomarket websites and the Tor Browser is attracting a larger user base for these markets, in terms of both buyers and sellers. As an example, a former IT professional became one of Silk Road's largest heroin dealers within a year (O'Neill, 2014).

TOC networks exist in several operational models, or typologies, as defined by the United Nations Office on Drugs and Crime (UNODC) (2002). The five models are rigid hierarchy, devolved hierarchy, hierarchical conglomerate, core criminal group and organised criminal network. The box on p.37 defines each model in

([15]) https://geti2p.net/en/

United Nations Office on Drugs and Crime transnational organised crime typologies

Rigid hierarchy: single boss. Organisation or division into several cells reporting to the centre. Strong internal systems of discipline.

Devolved hierarchy: hierarchical structure and line of command. However, regional structures, with their own leadership hierarchy, have a degree of autonomy over day-to-day functioning.

Hierarchical conglomerate: an association of organised crime groups with a single governing body. The latter can range from an organised umbrella type body to more flexible and loose oversight arrangements.

Core criminal group: ranging from relatively loose to a cohesive group of core individuals who generally regard themselves as working for the same organisation. Horizontal rather than vertical structure.

Organised criminal network: defined by the activities of key individuals who engage in illicit activity together in often shifting alliances. They do not necessary regard themselves as an organised criminal entity. Individuals are active in the network through the skills and capital that they may bring.

Source: UNODC (2010).

more detail. In each organisational type, there is a common series of seven steps (Lavorgna, 2014): (1) preparatory activities, (2) cultivation/production, (3) intermediate passage, (4) trafficking, (5) intermediate passage, (6) distribution, and (7) consequential activities.

The internet is currently involved in aspects of each step. Cryptomarkets have generally only been involved in the sixth step: distribution of the product ([16]). The individuals involved in such cryptomarket operations have generally been opportunistic entrepreneurs at the distribution level of any of the TOC typologies. The technical sophistication of cryptomarkets and the complexity of setting up and running one, or a shop in one, has, to date, limited the population of available candidates to those with more advanced technology skills.

([16]) Personal communications, (2014, 2015), Netherlands National Police, Europol and Team Cymru staff.

The next generation of cryptomarkets

The basic design for establishing a cryptomarket is still a single computer somewhere on the internet. This model cannot sustain much more than a small business. It also opens up the single machine to a variety of investigative and technical approaches to de-anonymising the traffic and the patrons, and exposing the entire operation. As a result of this reality and the success of the bitcoin block chain, a new generation of cryptomarkets are beginning to appear. The leading candidate for identification as such a next-generation cryptomarket is OpenBazaar ([17]). OpenBazaar works by distributing the transactions of the e-commerce software among all participants of the market. The market itself is based not on a single instance of e-commerce software running on a single server somewhere on the internet, but rather on the software running on all the computers participating in the market. This is accomplished using the basics of the bitcoin block chain. The bitcoin block chain is a distributed audit log of all transactions ([18]). OpenBazaar applies this block chain logic to all transactions in the marketplace. Therefore, when someone runs the OpenBazaar software on their computer, it immediately becomes part of the marketplace itself. This creates the potential for a fully distributed marketplace spread across millions of computers around the globe. Each computer handles only a part of the marketplace, rather than everything being handled on one single computer. Tor hidden services or I2P eepsites could be used with this model to further protect the identity and privacy of users involved in the marketplace.

Positive consequences of cryptomarkets

The coverage of Silk Road in the mainstream media and the moderated and open format of the forums attracted people from all walks of life. Silk Road was the most popular cryptomarket to offer discussion forums. There were forums dedicated to testing the purity of the product, to safe shipping methods, to safe bitcoin practices and, most interestingly, to harm reduction strategies and ending addiction to illicit drugs. It's easy to understand why someone involved in an illegal trade might want to share best practices and tips on many topics. However, what wasn't expected was that users would use the forums to discuss ending their dependencies on illicit drugs or reducing the harm caused

([17]) https://openbazaar.org/
([18]) https://en.wikipedia.org/wiki/Bitcoin#The_block_chain

to themselves and others by their use of them. Dr Fernando Caudevilla, aka 'DoctorX', was the first to realise the potential of the privacy and anonymity these hidden services and cryptomarkets can provide (Cox, 2014).

Law enforcement approaches to cryptomarkets

As criminals and criminal activity move to cryptomarkets, so do the law enforcement agencies. Law enforcement agencies have the added challenge of learning about the entire range of technologies that may be used by a criminal. Criminals have the advantage of having to learn only one technology at a time, and use it well, to be successful in both profit generation and avoiding legal consequences. Law enforcement agencies also have to consider a diversity of products, some digital and some physical. Laws on digital products are, by the nature of these products, more difficult to enforce. They can be easily copied, distributed, bought and sold, both online and offline. Physical products are easier to investigate and control, as they have to be delivered somewhere and to someone.

Essers (2014) provides an example: the National Police of the Netherlands (Politie) ran a sting operation where they posed as buyers in a cryptomarket. They targeted vendors selling to restricted markets, such as within the Netherlands or to Dutch speakers only. They purchased the drugs from the cryptomarket and arranged a rendezvous with the seller or the seller's delivery person. The Politie then arrested the person who arrived at the rendezvous point and subsequently used this person as an informant. The Politie further infiltrated the sellers and the cryptomarket until they were able to take down the cryptomarket itself (Essers, 2014).

Another approach to locating and taking down cryptomarkets is attacking the software itself. There are many layers of software involved in the operation: the operating system, the web server software, the Tor software and the e-commerce software. Any one of these parts of the cryptomarket can have vulnerabilities that may be exploited. In the case of a cryptomarket selling child pornography, the Politie was reportedly able to execute a warrant by breaking the software behind the cryptomarket (Dingledine, 2011). It has been suggested that Europol was able to break into Tor, watching the distributed hash table of hidden services in order to take down 414 hidden service addresses pointing to 28 individual cryptomarkets (Deutsch and Raymond, 2014).

The operational security of the criminals is another area for law enforcement agencies to target, as was the case with the takedowns of Silk Road (Greenberg, 2013) and Silk Road 2.0 (Rushe, 2014). In both cases, law enforcement agencies were able to follow financial trails to put together a list of suspects. The suspects were then easily placed under surveillance and further information leaks and patterns were discovered as a result of weak operational security practices. These information leaks were then used to further target the suspects, and eventually enough data were gathered for a conviction (Mullin, 2015a, 2015b).

The future of cryptomarkets

The first iteration of cryptomarkets still has a long life ahead of it. At the time of writing, there are a number of cryptomarkets still running after years of operations against them. They prove that strict operational security and operational focus can enable markets to continue despite many law enforcement investigations. The current weakness in all of these markets is the single-server model. Whether running Tor or I2P, essentially there is marketplace/e-commerce software located on a single computer in an encrypted address space. Having a single computer running the marketplace software opens the market up to computer attacks, which can start to place the server within various network locations. A fully distributed cryptomarket increases the difficulty and economic costs of removing such markets from the internet. This is expensive from a law enforcement perspective, but possibly desirable from a user perspective.

The next generation of cryptomarkets provides a glimpse into the future. The actual exchange of currency, especially from virtual (such as bitcoin) to fiat (such as euros), will always be a vulnerable boundary. This boundary, virtual world to real world, can be used by law enforcement to watch for transactions that may be traceable from the marketplace through to conversion to fiat currency. This boundary can also be a point of security for users looking to participate in forums or transactions not tied to their real-world identity.

As both citizens and law enforcement learn about, exploit and use cryptomarkets, they may usher in a new age of e-commerce. As with any new technology, criminals and opportunistic businesses will be early adopters of cryptomarket technology. These early adopters, and their customers, will work out the issues in the systems while simultaneously helping to improve the systems for future users.

References

Albanese, J. and Reichel, P. (2014), *Transnational organized crime: an overview from six continents*, Sage Publications, Thousand Oaks, CA.

Biryukov, A., Pustogarov, I. and Weinmann, R. (2013), 'Trawling for Tor hidden services: detection, measurement, deanonymization', *Proceedings of the 2013 IEEE Symposium on Security and Privacy*. Available at: http://www.ieee-security.org/TC/SP2013/papers/4977a080.pdf

Cox, J. (2014), 'Buying your drugs online is good for you', *Vice*, 24/1/2014, http://www.vice.com/read/silk-road-is-good-for-you

Dingledine, R. (2011), 'Dutch police break into webservers over hidden services', *Tor-talk mailing list*, https://lists.torproject.org/pipermail/tor-talk/2011-September/021198.html

Deutsch, A. and Raymond, N. (2014), 'Europol seizes 400 "dark market" sites in coordinated raid', *Reuters*, 7/11/2014, http://www.reuters.com/article/2014/11/07/us-europol-cybersecurity-arrests-idUSKBN0IR0Z120141107

EMCDDA (2015), *The Internet and drug markets: summary of results from an EMCDDA Trendspotter study*, European Monitoring Centre for Drugs and Drug Addiction, Lisbon. Available at: http://www.emcdda.europa.eu/attachements.cfm/att_234684_EN_Internet %20and %20drug %20markets %20study.pdf

Essers, L. (2014), 'Dutch police seize hidden online marketplace Utopia', *PC World*, 11/2/2014, http://www.pcworld.com/article/2096740/dutch-police-seize-hidden-online-marketplace-utopia.html

Greenberg, A. (2013), 'End of the Silk Road: FBI says it's busted the web's biggest anonymous drug black market', *Forbes*, 2/10/2013, http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/

Lavorgna, A. (2014), 'Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics', *Trends in Organized Crime*, 17(4). Available at: http://link.springer.com/article/10.1007/s12117-014-9226-8

Lewman, A. (2015), 'The Tor Project', retrieved from https://gitweb.torproject.org/torspec.git/tree/rend-spect.txt

Mullin, J. (2015a), 'At Silk Road trial, federal agent explains how he trapped Ulbricht', *Ars Technica*, 14/1/2015, http://arstechnica.com/tech-policy/2015/01/silk-road-trial-federal-agent-explains-how-he-trapped-ulbricht/

Mullin, J. (2015b), 'Ulbricht guilty in Silk Road online drug-trafficking trial', *Ars Technica*, 4/2/2015, http://arstechnica.com/tech-policy/2015/02/ulbricht-guilty-in-silk-road-online-drug-trafficking-trial/

Murdoch, S. (2006), Hot or not: revealing hidden services by their clock skew', *Proceedings of ACM CCS 2006*, Alexandria, Virginia. Available at: http://freehaven.net/anonbib/cache/HotOrNot.pdf

O'Neill, P. (2013), 'As Silk Road 2.0 struggles, new black markets look beyond Tor', *The Daily Dot*, 26/12/2013, http://www.dailydot.com/crime/deep-web-black-markets-beyond-tor-i2p/

O'Neill, P. (2014), 'The final confessions of a Silk Road kingpin', *The Daily Dot*, 22/1/2014, http://www.dailydot.com/crime/silk-road-confession-steven-sadler-nod/

Øverlier, L. and Syverson, P. (2006a), 'Locating hidden services', *Proceedings of the 2006 IEEE Symposium on Security and Privacy*. Available at: http://www.onion-router.net/Publications/locating-hidden-servers.pdf

Øverlier, L. and Syverson, P. (2006b), 'Valet services: improving hidden servers with a personal touch', *Proceedings of the Sixth Workshop on Privacy Enhancing Technologies*, Cambridge, pp. 223–244. Available at: http://www.onion-router.net/Publications/valet-services.pdf

Paul, K. (2015), 'The Silk Road boss allegedly encouraged the Hells Angels to kill a blackmailer', *Motherboard*, 29/1/2015, http://motherboard.vice.com/read/the-silk-road-boss-allegedly-encouraged-the-hells-angels-to-kill-a-blackmailer

Rushe, D. (2014), 'Silk Road 2.0's alleged owner arrested as drugs website shuttered by FBI', *The Guardian*, 6/11/2014, http://www.theguardian.com/technology/2014/nov/06/silk-road-20-owner-arrested-drugs-website-fbi

UNODC (2010), *The globalization of crime: a transnational organized crime threat assessment*, UNODC, Vienna. Available at: https://www.unodc.org/unodc/en/data-and-analysis/tocta-2010.html

UNODC, (2002), *Results of a pilot study of forty selected organized criminal groups in sixteen countries*, UNODC, Vienna. Available at: http://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf

4

CHAPTER 4

Staying in the shadows: the use of bitcoin and encryption in cryptomarkets

Joseph Cox

Introduction

There are two essential technologies that have given birth to cryptomarkets. The first is anonymity networks, which allow users to browse the web without revealing their location, and which also disguise where a site's servers are located. This allows cryptomarkets to sell illegal products in an open fashion while remaining relatively safe from law enforcement. Most commonly, cryptomarkets use Tor's hidden service model, as explained in the previous chapter, although there are markets on other networks, such as the Invisible Internet Project (I2P). The second technology deals with the financial side, and ensures that online transactions can be carried out with a substantial level of anonymity. Bitcoin, and other currencies that have been inspired by it, are used to purchase items rather than using a PayPal account or credit card, both of which can be easily linked to a user's identity.

Other technologies have been adopted by the users, vendors and administrators of cryptomarkets, but they aren't strictly necessary for a site to function. These include message encryption, which hides the contents of a message so that only the intended recipient can read it, and hard-drive encryption, which protects the files on a user's computer from access by an unauthorised party.

This chapter explains the fundamentals of bitcoin, the commonly used forms of encryption and how they are used within cryptomarkets.

Bitcoin

The problem for digital currencies

When someone sends a digital item across the internet, they haven't lost the original: when a user sends an email attachment, the file is still on their computer; when they upload a picture to Facebook, the photo doesn't disappear from their hard drive, and it's still there for them to view, delete or share over and over again. This is a problem for digital currency. When Alice sends Bob a digital coin, how can anyone be sure that Alice didn't simply send a copy? Usually, with financial transactions, a bank or other body makes sure that this doesn't happen, by keeping a record of their transactions, but this isn't the case for files sent between computers. This is commonly known as the 'double-spending problem' (Bonadonna, 2013).

Bitcoin's answer comes in the form of the 'block chain': a public ledger that records all successful transactions made with the currency, meaning that no one can spend their coins twice. It's similar to a bank statement, except it keeps track of the whole currency, rather than just an individual's account. With the block chain, it is easy to see which addresses, analogous to a bank account, hold what amount of bitcoins.

A 'block' is a series of updates of the transfers between addresses, and can be thought of as a fresh page in the ledger. As well as these transactions, a block also includes information that refers directly to the block that preceded it. This ongoing connection, from each block to the next, is why the collection of blocks is called the block chain.

Mining bitcoins

Each block also contains a very difficult mathematical problem that needs to be solved before the block can permanently join the block chain. There are multiple solutions to any of the block's mathematical problems, but only one needs to be discovered, although these problems intentionally become more difficult over time and require more computing power to solve. The computer that finds the solution for a block first is given additional bitcoins as a reward for helping to maintain the block chain. This process is known as 'mining'. Importantly, this updating of the ledger is not controlled by a third party, be that a bank, a formal financial institution or a government, who might, for whatever reason, tamper with it or let records go astray. Instead, the bitcoin network regulates itself.

Using bitcoins on cryptomarkets

If a user wishes to start storing bitcoins, they will first need a bitcoin 'wallet'. One of these can either be downloaded locally onto the user's computer or smartphone, or be hosted by an online service. The former is a piece of software, opened like any other computer programme. The latter functions in very much the same style as internet banking: a user logs in via their internet browser, and can view their balance and send bitcoins to other people. Included with the wallet will be a user's bitcoin address. This string of 25–36 characters is what somebody else needs to send bitcoins to the user, for example: 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy.

Cryptomarket user accounts usually include a bitcoin wallet address too, and it is possible to send purchased coins to it straight away. However, since cryptomarkets are under constant threat of being shut down by law enforcement and having all of their coins seized, users tend to avoid storing a significant number of bitcoins in a market address.

When trading on a cryptomarket, a buyer and a seller will both use addresses that are built into the market. This is to take advantage of any escrow system that the market might use. Escrow gives the buyer financial security when purchasing an item on the cryptomarket. In a basic system, a buyer will order an item, and the fee will be provided to the seller only once the buyer has confirmed that they have received their order. More advanced escrow systems, such as that on the now-defunct market Evolution, use multi-signature transactions. This means that, instead of just the buyer confirming their successful order and releasing the funds, two out of the three parties involved — the buyer, the seller and the market — need to sign off the transaction.

Buying bitcoins

The vast majority of those using bitcoin to buy products on cryptomarkets will not have mined the bitcoins themselves. Instead, they are likely to have purchased them with fiat currency. One option for this is buying the coins in person or through cash deposits. Although this may take slightly longer than other methods, buying coins in this way allows for a high degree of anonymity. A user will find a suitable bitcoin trader on a site such as localbitcoins.com, be given the vendor's bank details and then make a cash deposit at a local bank branch. This can usually be done without the buyer presenting any form of identification. So when the purchased bitcoins arrive in their wallet, and as long as the wallet itself does not give away their name or personal information, the buyer will have bitcoins that are in no way linked to their identity, and they can therefore spend their bitcoins anonymously.

However, many users buy their bitcoins via means that link their bitcoin wallet to their real-world identity. For example, many of the most popular websites for buying bitcoins require a form of identification, such as a passport or driver's licence, to be presented. Even if the exchange doesn't require identification, the coins may still be bought with a credit or debit card, which is in turn linked to a user's personal information. Once the link has been made, a persistent and resourceful observer can trace bitcoin transactions back to a wallet, a pseudonym and possibly a user's real identity.

Reasons for bitcoin anonymity

There are a number of reasons why someone might want to buy their bitcoins anonymously and not have their identity linked to any transactions. The most obvious reason when it comes to cryptomarkets is because many of the items available are illegal to possess. A user may be worried that their purchase of drugs or weapons, for example, may be traced back to them, and that they could face criminal charges.

Theoretically, a law enforcement agent could track a buyer's transactions back to the point when the bitcoins were purchased online, a practice known as 'block chain analysis' (Simonite, 2013). Thus, the buyer's identity has been revealed, or the law enforcement agency at least has enough information to issue the bitcoin exchange with a subpoena, forcing them to hand over the identity

of their customer. By way of illustration, *Forbes* magazine asked Sarah Meiklejohn, a computer science researcher at the University of California, San Diego, to attempt to map what transactions *Forbes* had made, with knowledge only of its bitcoin address. Meiklejohn managed to 'identify every transaction we had made, including deposits to Silk Road, [and] to competitor sites Atlantis and Black Market Reloaded' (Greenberg, 2013). In fact, anybody with an internet connection can examine the block chain: it is available through a number of web services.

Another reason for wanting to use bitcoin anonymously is less obvious. Once a bitcoin wallet has been linked to a real-world identity, and personal details such as name, email address and other information have been discovered, it is possible for a hacker to attempt to steal the user's coins. Armed with that kind of information, an attacker can write a 'phishing email'. These are emails that coerce the user into replying with sensitive information, such as their banking details, or trick the user into entering their login details or password into a spoofed web page (Cluley, 2014).

Unlinking bitcoins

To conceal their identity, to avoid either prosecution or hacking attacks, a bitcoin user may wish to separate any transactions from their identity. Some cryptomarkets have obfuscation systems built into their infrastructure. For example, the original Silk Road would disguise the path of its users' coins to make it difficult to identify by whom each transaction was made. 'Silk Road also used a so-called "tumbler" which, as the site explained, "sen[t] all payments through a complex, semi-random series of dummy transactions … making it nearly impossible to link your payment with any coins leaving the site,"' according to an FBI press release posted after the site's closure (New York Field Office, 2013). However, users may wish to unlink their identity from any transactions they make themselves, either because the cryptomarket they are using doesn't provide such a service or to build in an added layer of security.

One popular site for doing this is Bitcoin Fog, which obfuscates the destination of a user's coins to the point where block chain analysis becomes exceptionally difficult. Users sign up for a free account on Bitcoin Fog, accessible only via Tor, and then deposit an amount of bitcoins at an address randomly generated by the service. 'Since it is just a bitcoin address like any other, there is no way to even see that you have deposited money to Bitcoin Fog, and not to a random account you have generated yourself,' according to the Bitcoin Fog support site ([1]). From here, a user can schedule a series of withdrawals, all of which will have variables of them randomised: the size of each payout, the time at which they occur and also the destination address, of which there can be several. 'This way there is no practically reliable way to do statistical analysis on the block chain and link your deposits to your withdrawals,' states the support site.

Bitcoin Fog does require the user to be thoughtful: the amount withdrawn should be different from that originally deposited. The reason for this is given by an example on the support site: 'If you transfer 1.382 to us, and the next day you withdraw ~1.38 bitcoins to another account, those amounts will be visible in the block chain, and unless there were 10 other people that day that also withdrew just 1.38 bitcoins, the link between your deposit and your withdrawal will be obvious.'

Another method for obfuscating bitcoin transactions is the use of CoinJoin. For instance, Alice wants to transfer 1 bitcoin from address A to address B, and Bob wants to transfer 1 bitcoin from address C to address D ([2]). In essence, CoinJoin allows Alice and Bob to combine their trades into a single transaction, with two inputs (A and C) and two outputs (B and D). Anyone observing the block chain will not be able to determine which of the outputs is Alice's and which is Bob's. This can be done with more than two people, and although it doesn't disguise that a transaction took place (as all transactions are recorded in the block chain), it does obscure who is behind each transaction. In addition, because a user's coins aren't being stored by a third party, as in the case of Bitcoin Fog, there isn't the possibility of a user having their coins stolen by the service. The CoinJoin method has been adopted by popular bitcoin wallet services, including Blockchain.info, which has incorporated it into its online wallet service, under the name 'SharedCoin' ([3]).

A third method for ensuring bitcoin privacy is the use of a dedicated wallet that incorporates many different technologies together. One of those is DarkWallet, a project led by the computer programmer Amir Taaki. DarkWallet can be used without providing any identifying information, and it includes the technology behind CoinJoin. It also uses 'stealth addresses', which are generated on demand by the user, 'without anyone watching the block chain knowing the receiver is the owner of the original stealth address,' according to the DarkWallet Wiki ([4]). DarkWallet is currently available as a

([1]) The support site can be found at http://www.bitcoinfog.com/
([2]) This example was taken from a post on Stack Exchange (Rami, 2013).
([3]) The company's explanation of this service can be found at https://sharedcoin.com/
([4]) https://wiki.unsystem.net/en/index.php/DarkWallet/Alpha#Stealth

browser plugin for Chrome; it will also be released for use with Firefox.

Recently, DarkWallet released a feature allowing its users to anonymously convert and withdraw funds from their wallet through an ATM. At the moment, this feature extends across thousands of ATMs in Europe, and requires a user to enter a code sent to their mobile phone, rather than using a bank card (Rogers, 2015). DarkWallet also hosts an independent bitcoin exchange, where users can purchase bitcoins anonymously.

The research community investigating bitcoin anonymity is a vibrant one, and the subject is likely to become more relevant as it becomes harder to purchase bitcoins anonymously in the first place. For example, localbitcoins.com, the previously mentioned platform used to meet bitcoin merchants in person or obtain their bank deposit details, had to cease operations in Germany after being approached by the country's Federal Financial Supervisory Authority (Rizzo, 2014).

Anonymity-focused cryptocurrencies

Some programmers and bitcoin enthusiasts have developed other cryptocurrencies. The method of acquiring these coins is essentially the same as bitcoin — computers solve increasingly complex equations with their processing power — and the way they are spent is indistinguishable from bitcoin. But many of these newer coins have different features. Naturally, those of most interest to cryptomarkets are the coins that push for greater anonymity: those that mitigate the problems of bitcoin trading being linked to a real-world identity, and which bypass the need to be cleaned using another service. Very few of these cryptocurrencies have gained any sort of wider use, and even those that have been given more attention make up a tiny part of the overall trade of cryptocurrencies. Nevertheless, use of anonymity-focused cryptocurrencies is an important development, because it indicates that people are keen to make the trade in illegal substances and other items even more secure. Furthermore, the purpose of these privacy-focused coins isn't necessarily to gain value when traded for a fiat currency, but to allow more anonymous trade.

One of those cryptocurrencies is the aptly named 'Dark Coin'. Described by *Wired* as 'Bitcoin's stealthier cousin', Dark Coin became an acceptable form of payment on the Nucleus and Diabolus markets in November 2014 (Greenberg, 2014). It is also used for buying web hosting and virtual private network services. Dark Coin's appeal is that it incorporates technologies that obfuscate who is sending coins to whom. So rather than having to buy an amount of currency and then process the coins through a separate service, the currency itself has these anonymity features built in.

Other privacy-focused cryptocurrencies do exist, but their uptake has been limited, even by the cryptomarkets. At the moment, it is likely that bitcoin will remain the primary cryptocurrency used by the markets.

Encryption

Due to the illicit nature of the business conducted on cryptomarkets, or just to ensure their own privacy, many users decide to encrypt their communications. This behaviour isn't required for the use of cryptomarkets, but is generally recommended by staff, with sections of forums dedicated to teaching new users how to use encryption. The most common message encryption programme is PGP, used by cryptomarket administration, vendors and buyers. PGP stands for 'Pretty Good Privacy'. Created in 1991 by Phil Zimmermann, it is a computer programme that allows a user to encrypt text and files so that only the intended recipient is able to decrypt it. PGP also allows a user to digitally 'sign' messages, in order for the interlocutor to feel reasonably confident that the messages are coming from who they say they are. In his essay, 'Why I Wrote PGP', Zimmermann summed up the various possible uses of the programme (Zimmermann, 1999):

> It's personal. It's private. And it's no one's business but yours. You may be planning a political campaign, discussing your taxes, or having a secret romance. Or you may be communicating with a political dissident in a repressive country. Whatever it is, you don't want your private electronic mail (email) or confidential documents read by anyone else. There's nothing wrong with asserting your privacy. Privacy is as apple-pie as the Constitution.

Zimmermann distributed this software as 'shareware', meaning that it could be spread freely as long as it wasn't used for commercial purposes (Spectacle, 1995). However, when PGP ended up in the hands of non-US citizens, Zimmerman faced a government investigation for exporting munitions without a licence, because, at the time, cryptography of a certain strength was considered a weapon (Zimmermann, 1995). This investigation was eventually dropped with no charges being brought, but it spurred Zimmerman to release the source code for PGP in the novel form of a book published by The MIT Press, as 'it would be politically

difficult for the Government to prohibit the export of a book that anyone may find in a public library or a bookstore,' Zimmermann wrote in its preface.

Since its launch, PGP has seen many updates and improvements to ease of use, and the company PGP Incorporated was formed and subsequently acquired by a number of different corporations. The software PGP is now maintained by Symantec, but many alternatives of the software have sprung up, with one of the most popular being GnuPG (GPG). However, when talking about message encryption generally, the acronyms GPG and PGP are typically used interchangeably, as the two pieces of software serve essentially the same purpose. Today, PGP is still considered the standard for message encryption; Edward Snowden, the former NSA contractor who blew the whistle on the agency's mass surveillance programmes, used it to communicate with journalists (Lee, 2014).

How PGP works

PGP works through the use of pairs of 'keys', with each pair of keys comprising a 'public' key and a 'private' or 'secret' key. These keys are simply files stored on a user's computer or USB stick. The 'public' key, as the name suggests, is one that should be used in the public domain for others to see. This may be on a user's personal website, in his or her forum profile or on a site or server that hosts the public keys of other people. It is what people use to encrypt a message to a user. The 'private' key is one that, ideally, should never be shared with anyone else. This key is used to decrypt any messages or files encrypted for a user, as well as signing any messages the user sends, to assure the recipient that they are indeed communicating with the correct person. If a third party is in possession of a user's secret key, they may be able to read encrypted messages sent to the user, or the third party could impersonate the user and sign messages with their key. It is worth mentioning that some users do share their secret keys. For example, the secret key of 'Heroin Vendor' may be accessible by more than one person, if 'Heroin Vendor' is actually a team of people working to sell product on a cryptomarket. However, in the majority of cases each individual using a cryptomarket is likely to have their own secret key.

PGP is the protocol used to encrypt messages, but the actual process of applying these protocols to messages is done either by the user via the command line of their computer — a process that requires some technical knowledge — or by another programme that makes the process easier for the user. This programme is what the user will typically interact with, with simple buttons for 'Encrypt', 'Save' and other common functions. For example, a commonly used version for Windows machines is GPG4Win, which uses GPG as its basis. Below is a message before it has been encrypted with the PGP protocol.

> *Hello,*
>
> *This is a message that I would like to have encrypted.*
>
> *Thanks,*
>
> *A user*

The user will then select which public keys they wish to encrypt the message for. After being encrypted, the result is either a new file or a body of text, depending on the programme. Either way, its contents will be unintelligible: a mixture of seemingly random digits, symbols, and upper- and lower-case letters. Below is the earlier message after being encrypted.

> -----BEGIN PGP MESSAGE-----
>
> hQIMA3mulckJMVeCARAAoliWbrv6tYyXcA2tMs16Avp
> Ng37bt/eLsX3EdYS5YWMCI3Cictc8y93lMhOJNWRDL
> mt1Zrj9kDcEThysCFePrRLUzxQQdFqsWh29VTa7vfKT
> pYCSXhsgUft0bPu62ISI+sYR51CWaE/bAtSwF7fqtKI4
> AYUG3jeedHF8QScTtcCM15eNmp7TWZvURZT3kq6rW
> AVoSt938XN3JZhHd2SvX1qhOwqjoHGaQE+KI2ejaZ8jr
> u7Javwq3ix3/NF+b7EXBdM7eBbI0Z1/sLEcgkyp1vEO8
> RJ8HtXEf1g/TE+u+JHI1IfcUxxafPZFNKp8AJhAvEe/r/
> x5qABKEPBYxDOxBT84i+aWgGSN5X1nx0Z2j8VyqWh
> xdmkugok/XNL0KbuH2sHIBAWsAByNTfbzm612WihhN
> akEbyP5V719VvFBRIvr1bOP4RTj35xCi/V838V8cUku0
> +U1YuWd+24avMHivRlLodZqLhe5K9C/JyP22E/m4Ww
> sa0ZPemm4g7vCKQWUDWRaa/OaBu4N1q37hVp83dj
> ED5dqSDmt15DU/eC65a7Mb3aKxajqQqwk7ivq0cBme
> YfbWlekREZU2QTe6Vq6P5Tz94MfwJGNxOiDooEMGv
> 82AqPBjyYArF50znAcqU9raqUMpH4EY1x+mUlJWir+a
> 6adimIEg1wXhje5LG0Ic63SqwFxoXD8m+Swdo2jbGLll
> HaSnNJH0VQE15KS5JkbHm9M3qtd27vGxqKGlnnrWf
> eeuc2ljsqmdtjwatCL7CQNRqSOC+g8OPowfd6unDF3
> mIMOW9CjIGik89FTJPeyy6XCPd7vBezAstsdpIQ43W
> THucHtIy4ezScEy36hqKtSe28P40ZBVplw6MXH65ZG
> hLKiffc4MlJTS3qXVrGZL4THn5dRF1osIjGMoELIA==
>
> =iJXY
>
> -----END PGP MESSAGE-----

This message can then be pasted into the body of an email or sent using the messaging service of a cryptomarket. This way, even if the message is

intercepted through a government's mass surveillance system, is inspected by those providing the messaging service (either the email company, such as Google, or the administrators of the cryptomarket) or is viewed by law enforcement agents who have acquired copies of a cryptomarket's private messages, the actual content of the message will be unreadable to those without the correct key. To decrypt a message sent via a cryptomarket's messaging system, the user will need to paste it into their PGP programme. After this, they are prompted to type in a password, and then they can read the original message.

It is important to note that the use of PGP does not encrypt a user's metadata. Metadata comprise all of the information related to a communication that isn't the content of the communication itself. Metadata include, for example, the date an email was sent; which address it was sent from; the recipient's email address; and the services that the email travelled through to its destination. In practical terms, this means that, if an administrator of a cryptomarket was snooping on who was talking to whom via the site's messaging system, they would still be able to see a buyer talking to a vendor, although they wouldn't be able to read the content of the message if the users had been using PGP.

As mentioned, PGP is important for all types of users of cryptomarkets, but it is especially useful for buyers sending a vendor their name and delivery address. This way, even if law enforcement manages to seize a cryptomarket's servers and, in turn, all private messages written through the site, they will not be able to see the real names of any customers who have encrypted their details.

Other forms of encryption

PGP is certainly the most widely used form of message encryption on cryptomarkets, but a couple of others are used as well. Off-the-Record (OTR) is a method for encrypting instant messaging services, such as Google Talk, Facebook or Jabber. The software typically comes as a plugin that is installed alongside another chat programme. This method of communication doesn't use the messaging system of a cryptomarket, but vendors may advertise their OTR contact details on a site. For example, on one site, 'Map Dealers legalize world', many vendors advertise OTR chat in their contact details (Cox, 2014).

As well as encrypting their communications, some users take the step of making access to the files on their computer more difficult. Hard-drive encryption prevents someone with physical access to a computer, such as a law enforcement officer once an arrest has been made, accessing certain files or the entire contents of the computer. In order to decrypt the hard drive, a password needs to be entered, and some encryption software allows users to set up two different passwords: one to be entered if they are under duress, which reveals one set of files, and another, genuine, password that protects the sensitive information in another set of files.

Conclusion

Cryptomarkets use several different pieces of technology: as well as Tor, covered in the previous chapter, they also use bitcoin for fairly anonymous financial transactions; message encryption for communicating securely; and other forms of security for keeping sensitive information hidden. As law enforcement agencies continue to crack down on these markets, it seems that advances in these technologies are likely to be adopted by cryptomarkets and their users.

References

Bonadonna, E. (2013), 'Bitcoin and the double-spending problem', http://blogs.cornell.edu/info4220/2013/03/29/bitcoin-and-the-double-spending-problem/

Chen, A. (2013), 'Redditor claims to have been arrested for buying drugs on Silk Road', http://gawker.com/redditor-claims-to-have-been-arrested-for-buying-drugs-1444086695

Cluley, G. (2014), 'Bitcoin phishing attack targets Blockchain users', http://grahamcluley.com/2014/03/bitcoin-phishing/

Cox, J. (2014), 'This deep web site maps the world's drug dealers', http://motherboard.vice.com/read/this-deep-web-site-maps-the-worlds-drug-dealers

Greenberg, A. (2013), 'Follow the bitcoins: how we got busted buying drugs on Silk Road's black market', http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/

Greenberg, A. (2014), 'Online drug dealers are now accepting darkcoin, bitcoin's stealthier cousin', http://www.wired.com/2014/11/darkcoin-and-online-drug-dealers/

Lee, M. (2014), 'Ed Snowden taught me to smuggle secrets past incredible danger. Now I teach you', https://firstlook.org/theintercept/2014/10/28/smuggling-snowden-secrets/

New York Field Office (2013), 'Manhattan U.S. Attorney announces seizure of additional $28 million worth of bitcoins belonging to Ross William Ulbricht, alleged owner and operator of "Silk Road" website', https://www.fbi.gov/

newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website

Rami (2013), 'Can someone explain to me how coinjoin works for anonymity in plain English without all the tech jargon?', https://bitcoin.stackexchange.com/questions/16649/can-someone-explain-to-me-how-coinjoin-works-for-anonymity-in-plain-english-with

Rizzo, P. (2014), 'LocalBitcoins "exploring options" after service halt in Germany', http://www.coindesk.com/localbitcoins-exploring-options-service-halt-germany/

Rogers, K. (2015), 'Dark wallet, now with cash', http://motherboard.vice.com/read/dark-wallet-now-with-cash

Simonite, T. (2013), 'Mapping the bitcoin economy could reveal users' identities', http://www.technologyreview.com/news/518816/mapping-the-bitcoin-economy-could-reveal-users-identities/

Spectacle (1995), 'The Zimmermann case', http://www.spectacle.org/795/zimm.html

Zimmermann, P. (1995), 'Author's preface to the book: "PGP Source Code and Internals" ', https://www.philzimmermann.com/EN/essays/BookPreface.html

Zimmermann, P. (1999), 'Why I wrote PGP', https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

5

CHAPTER 5

Reputation is everything: the role of ratings, feedback and reviews in cryptomarkets

Joseph Cox

Introduction

Cryptomarkets rely heavily on trust. Because a drug vendor in any cryptomarket transaction is pseudonymous, and does not have to deal with the buyer in any sort of close proximity, it is theoretically easy for them to deliver a product that is of a lesser quality than advertised — or not to deliver the item at all — and not be held to account.

Within cryptomarkets, this problem has been mitigated by the use of various reputation systems, such as ratings, feedback and reviews of products and vendors, which are posted on the cryptomarkets themselves, in their forums or on social media. These reputation systems provide buyers with a fairly reliable account of a vendor's previous transactions and track record, as well as of the quality of individual products, and can help them to build up an overall picture of whether a drug vendor is trustworthy or not. These systems ensure that dealers who do provide a low-quality service are shunned by the cryptomarket community. In turn, this insight allows buyers to make informed decisions on what to purchase and from whom, and to avoid more dangerous batches of drugs, so that these reputation systems potentially offer, in this respect, certain harm reduction benefits.

This chapter describes the main features of reputation systems and their role in cryptomarkets.

Ratings and feedback

One type of reputation system is the use of ratings for individual products. After a buyer has ordered and paid for an item, they are prompted to leave a rating. These ratings are typically a number between one and five, in the same style as traditional 'five star' ratings. Naturally, these ratings have often been compared to those used on eBay, Amazon and Yelp. Indeed, cryptomarkets in general are often described as being similar to these sites, which also allow users to rate products and services (Harris, 2013; Kopstein, 2013).

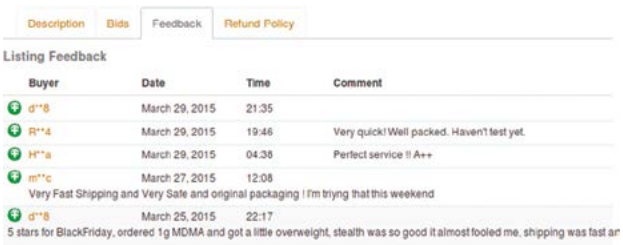
Along with the numbered rating, customers are also encouraged to leave a short piece of feedback about their particular order. These snippets of feedback focus on a variety of different aspects of the customer's drug purchase. Some talk about the quality of the product: 'half gram weight out to 0.3, gear was decent, expected better,' was one piece of feedback left on a listing for Afghan heroin on Silk Road 2.0.

Other users report on the packaging used and how effectively shipped the item was. 'Very safe and original packaging!' one piece of feedback left on an MDMA listing on the AlphaBay market reads. 'stealth was good it almost fooled me,' was another left on the same listing, with 'stealth' here referring to how likely a drug is to remain undetected owing to the way it has been packaged.

Others focus on the speed of delivery. 'I ordered 11:30 AM yesterday and my package was in my mail box in literally 25 hours. Quality is up there with the best tar I've ever had. I'll definitely be back for more in the future,' was one comment left on Silk Road 2.0.

FIGURE 5.1

A screenshot of feedback list on a listing for MDMA on the cryptomarket AlphaBay



The feedback isn't always positive, however. 'This seller is a f***ing scammer, i payed for hashish and now i have 40 grams of f***ing paraffin. DON'T BUY FROM THIS **** 1/5,' is one example from Silk Road 2.0 (Bartlett, 2015).

These negative pieces of feedback are often based on the same aspects discussed above with respect to positive feedback: the stealth, the quality of the product and its delivery time. If the item doesn't arrive at all, a buyer can also leave feedback saying so.

Overall, however, the ratings left by buyers seem to be positive, or at least that was the case on Silk Road 2.0. Over three months, 120 000 pieces of feedback were left on the site, with the average rating attached to the corresponding listings being 4.85 out of 5 and 'great' 'fast' and 'good' being the most common words left on the written feedback section (Bartlett, 2015).

On top of these individual product ratings, some markets employ vendor ratings. On the now-defunct Evolution market, vendors were given a 'level', ranging from one to five (one being the lowest and five being the highest). As for how this helps buyers, it is reasonable to assume that a Level 5 heroin dealer, for example, is experienced and perhaps also offers a good-quality product, because presumably the vendor's items have been popular in the past.

The rating and feedback system is not infallible, however, and it can be abused, as has also been the case with legitimate marketplaces.

Abuse of ratings and feedback

One scam involves the drug vendor generating only the appearance that they are trustworthy and have served customers in the past. 'Padding' feedback, as the practice is known, is when a vendor purchases drugs from themselves using a series of buyer accounts that they have created. To anyone else using the cryptomarket and looking at the ratings and feedback, it appears that the customers are legitimate, when in fact they are simply aliases of the vendor.

Another way the rating system can be abused is by vendors building up a reputation for being reliable, and then deliberately making an unexpected switch in behaviour and scamming users out of their bitcoins.

Over time, a vendor with consistently high ratings is likely to be deemed generally trustworthy by users of the cryptomarket. This in turn may mean that users feel comfortable enough to 'finalise early'; that is, send their full payment for the product to the vendor before it has been shipped (vendors sometimes ask for this payment method when the value of bitcoin is fluctuating wildly). However, a vendor can abuse this trust to accept as many payments as possible without shipping any drugs until users start to notice the discrepancy. The vendor will then close their account and disappear with the stockpiled bitcoins. This is commonly known as an 'exit scam' (Christian, 2014).

One example is the vendor 'Tony76' from the original Silk Road, who used his reputation, built up through the rating system, to lull users into a false sense of security. During a sale to celebrate 4/20 (20 April, a date popular in the United States for recreational drug use), Tony76 offered large discounts on his products, as well as allowing orders from outside the United States for the first time (O'Neill, 2014). Tony76 even went so far as to offer prizes to random customers as part of the sale.

Some buyers started to complain that their packages weren't arriving. In response, Tony76 started issuing partial refunds to unsatisfied customers. However, vendors cannot comprehensively check these claims of failed deliveries, so Tony76 instead switched to the 'finalise early' system, meaning that customers had to pay the full product price in advance. Because users believed him to be trustworthy, they agreed to send their bitcoins to Tony76 before the product had been shipped. Tony76 then reportedly failed to deliver the items and disappeared with the funds. This is a case of the rating system working disproportionately in the vendor's favour (Ormsby, 2012).

Another, more recent, case involved '9THWonder', a cannabis vendor from the now closed Evolution cryptomarket (Christian, 2015). However, these scams, and abuse of the rating and feedback systems in general, are reportedly relatively rare.

Reviews

As well as ratings and their accompanying short pieces of feedback, some users write much longer, in-depth reviews of a particular product or batch of drugs. These can appear on the forums of cryptomarkets or on other social media.

FIGURE 5.2
Example of a template from Reddit

Information	Details
_Vendor:	[EmeraldTriangle]
_Market:	[Abraxas]
_Product:	[1/2oz Blue Dream]
_Shipped from:	[USA]
_Shipped to:	[USA]
_Required FE:	[NO]
_Vacuum Sealed:	[Yes]
_Decoy:	[No]
_Handwriting:	[No]
	Rating
_Communication:	[10]/10
_Stealth:	[10]/10
_Shipping time:	[10]/10
_Price value:	[10]/10
_Aesthetics:	[10]/10
_Weight:	[10]/10
_Quality:	[10]/10
_Transaction:	[10]/10
_Vendor:	[10]/10
_Drug:	[10]/10
Total score:	**[100]/100**

Extremely potent when turned into butter. A quarter oz was turned into a stick of butter, which made 16 1x1" brownies. One brownie sent a 200lb muscly man into a wild trip. Be careful. (Gosh-Damit, 2015).

One of the popular hubs for this activity is the DarkNetMarkets sub-Reddit. Reddit is a social media site that allows users to create sections of the site dedicated to certain topics, or 'sub-Reddits'. Naturally, the DarkNetMarkets sub-Reddit deals in cryptomarket news, as well as being a space where users can post reviews of vendors and their products.

Many of these reviews follow a template that has been uploaded by a user. It includes a wide array of information, including where the drug was shipped from, the quality of the product, its value for money, the communication between the buyer and seller, and the level of the seller's security (whether or not they used their own handwriting for the packaging labels, or whether or not the package containing the drugs was vacuum-sealed, for example). These are presented in a clear, easy to digest format, along with any additional comments from the reviewer. Below is an example of a completed template uploaded to Reddit.

Guides on how to write more helpful reviews have also been posted on the DarkNetMarkets sub-Reddit (entactoBob, 2015). Advice includes covering the main areas of interest to users ('communication, product and price, and market'), as well as including images and making sure that the review is clearly formatted.

Other reviews are much more personal, and detail the user's experience with the drug rather than strictly the quality of the product itself. One dark web forum, The Majestic Garden, provides a section for users to submit their own 'trip reports'. These vary in length, from a few short sentences to pages' worth of content, but they often pay great attention to detail, describing the dosage consumed, which vendor the drugs were brought from and the user's subjective experience of the drug.

The report continues, detailing what music the user listened to, how the trip progressed into the comedown and how it ended.

At the time of writing, there have been over 45 replies to this forum thread, although not all of those are trip reports, as some are supportive messages or thanks from other users.

One particular group stands out when it comes to providing reviews of drugs sourced from cryptomarkets. The 'LSD Avengers', as the name suggests, focused on the use of psychedelic drugs, although they also provided reviews for MDMA. When they started, they were based on the original Silk Road. According to Jeffries (2014), 'the Avengers began ordering from different vendors on the site, subjecting their wares to a chemical reagent test and a gas chromatography mass-spectrometry machine. If the drug was in fact

FIGURE 5.3
A screenshot of a trip report from 'The Majestic Garden', a dark web forum

Transcript of above: Trip report for Blueviking House Xtal 100ug tab one such report starts. I took 2 of the 100ug tabs at 4:00 pm at the 30 min mark I felt a very strong electrical feeling in the back of my head and butterfly's in my stomach,I then start laughing like a MadWomen for 10 min,when that was over I started to get some crazy leg tremors, Kinda freaked me out for a bit, after about 30 min of tremors it subsided into pure bliss, like an old friend come home to see you.

LSD, the Avengers consumed it and posted Yelp-like reviews.'

These reviews were similar to those carried out by individual users of cryptomarkets, but, thanks to the tests performed by the LSD Avengers, were generally considered more detailed. They also primarily reviewed vendors rather than individual products. Some examples provided by Jeffries (2014) include:

> 3JANE — Canada to International. Known fondly as the Queen of SR. Quality LSD with appropriate dosages advertised. Extreme Ninja-Spy stealth shipping with friendly communication.
>
> HAIZENBERG — Czech to International. Extremely friendly and personable customer service with consistent product and regular stock. Currently selling: Hofmann, Dancing Bears and Strawberrys (advertising 110ug) Trip Test Hofmann: ~100ug.
>
> MARIJUANAISMYMUSE/GOINGPOSTAL — Canada to International. Vials and some other shit. Last time we tried to test them they packaged the acid so badly that it was seized in transit. A few past selective scamming claims from trusted members, so be absolutely sure to read their FE [finalise early] and refund policies. We still don't know the quality/consistency of the acid because it was taken by LE [law enforcement] and will not be able to test them for safety reasons.

In all, the LSD Avengers reviewed 60 vendors, and ranked 14 'star' sellers, 19 vendors who were 'OK' and 27 'bad' sellers (Jeffries, 2014). The group entered retirement in October 2014, but a few months later they re-emerged on their own forum, the previously mentioned The Majestic Garden.

Why reputation matters

Reputation systems appear to instil buyers with greater confidence in using cryptomarkets. Surveys have indicated that vendor ratings are one of the main reasons that users are attracted to cryptomarkets, with 60–65 % of respondents saying that the existence of ratings was a motivation for using the original Silk Road, and that they were more comfortable purchasing drugs from vendors with a higher rating (Barratt et al., 2014).

So when reputation systems are in place, it creates an environment where the best dealers, or at least those with the highest ratings, may be rewarded with more customers. 'The seller-rating system built into the site, along with efforts by unofficial groups like the Avengers, created a system that rewarded dealers who sold good stuff' (Jeffries, 2014). Indeed, to be successful as a vendor on the cryptomarkets, 'it turns out the key to their success is not clever encryption, or bitcoin, or even Tor. It's good old-fashioned customer service' (Bartlett, 2015).

In a way, thanks to reputation systems, the cryptomarkets have developed an organic method of self-regulation: vendors who sell low-quality products or who provide poor customer service will simply not receive good ratings, feedback or reviews, so arguably only those providing high-quality products will survive.

Reputation systems can also provide information to users about product quality and potential risks. According to 'Harry', a pseudonymous heroin and crack cocaine addict who purchased drugs from the first and second Silk Road sites, the rating systems were especially useful for ensuring that he received a consistent quality of product (Cox, 2014). When purchasing drugs from a street dealer, there is 'no way of knowing how strong any given batch is, [making] it near impossible to manage dosage properly,' according to Harry. On cryptomarkets, however, a consistent product is likely to be labelled as such thanks to the reviews and ratings left by other users. If there is a sudden dip or increase in drug quality, this will probably be highlighted by the community.

The cryptomarket community can also use these reputation systems to flag vendors who sell one substance under the pretence that it is something else entirely. In one post on the DarkNetMarkets sub-Reddit, a user accused a vendor of selling PMA, or paramethoxyamphetamine, as MDMA (SilentRaider3, 2015). Although the drugs have similar effects, it takes longer for the user to feel PMA's effects, meaning that, thinking that they haven't take enough, they may ingest more and overdose. 'If we had taken MDMA dosages, we would all be [f******] dead now,' the complaining user wrote.

This harm reduction element is reflected in the motivation of those who encourage reviewing or write reviews themselves. According to the Reddit user who constructed one of the commonly used templates for reviews, 'I do this to encourage vendor reviews, because it helps keep our markets safer than they would be otherwise and adds some degree of accountability' (entactoBob, 2015).

The primary motivation of the LSD Avengers was reportedly to expose dealers who were selling research chemicals as traditional hallucinogens, as well as to

discover the best-quality LSD available on the deep web. Specifically, they were searching for 'needlepoint acid', a particularly potent variation of LSD (Jeffries, 2014).

Recent developments

More recently, some cryptomarkets have experimented with 'contracts', in various forms. AlphaBay, a market that launched in December 2014, and was still up and running at the time of writing, implemented a feature the administrators of the site dubbed 'digital contracts'. Each contract costs USD 5, which is payable to the administrators, and can contain anything that two contracting parties desire. This is as long as it relates to products already traded on the market: the owners of AlphaBay made it explicit that they would not tolerate contracts being used to hire hit men, for example.

Vendors can already create custom listings for buyers if they desire, if they wish to purchase a bulk amount that isn't already listed, for example. But these new contracts 'are for more long term business,' according to the owner of AlphaBay (Cox, 2015). The terms of the contract are then signed by the AlphaBay administrators with a PGP key. If one of the parties involved feels they've been cheated, they can raise a dispute with the site's administrators; in this way, the market is similar to PayPal or other e-commerce services. A decision will be made about whether or not one of the parties should be stated to have 'failed' the contract. This failure will then be added to the offending user's profile, for everybody to see, and if a user is deemed to be particularly untrustworthy, they may be banned from the site all together. If the contract is successful, and both parties are satisfied with the result, then a 'completed' note will be added to the users' profiles.

These contracts, however, will not stop people scamming other users outright. It is perfectly possible for a user to repeatedly fail their contracts, or to make multiple accounts with the sole purpose of scamming while avoiding detection. There is also the problem of possible bias in a site administrator: the person enforcing the contract may have made another deal with one of the involved parties, perhaps to take their side in any dispute.

There have been other developments in the area of digital contracts, notably from OpenBazaar, a decentralised platform for trading goods (drwasho, 2014).

Conclusion

Reputation systems, rather than being a tacked-on feature, are essential for the functioning of cryptomarkets. They are important in enabling buyers to make informed decisions, they are used by vendors to build up trust over time and they also regulate vendors on cryptomarkets. Scams and abuse still exist, but it appears that they are carried out by a minority of vendors.

As well as supporting the smooth functioning of cryptomarkets, reputation systems may also have a protective role in contributing to stamping out vendors who sell dangerous batches of drugs or those who sell something other than what they advertise.

References

Barratt, M., Ferris A. and Winstock, A. (2014), 'Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States', *Addiction* 109(5), pp. 774–783.

Bartlett, J. (2015), 'What "dark net" drug buyers say about their dealers', http://www.telegraph.co.uk/technology/internet/11466413/What-dark-net-drug-buyers-say-about-their-dealers.html. Last accessed 29/5/2015.

Christian, J. (2015), 'The "exit scam" is the darknet's perfect crime', http://motherboard.vice.com/read/darknet-slang-watch-exit-scam

Cox, J. (2014), 'Buying your drugs online is good for you', https://www.vice.com/read/silk-road-is-good-for-you

Cox, J. (2015), 'This dark web market just started offering contracts for anything', http://motherboard.vice.com/read/alphabay-contracts

Drwasho (2014), 'Ricardian contracts in OpenBazaar', https://gist.github.com/drwasho/a5380544c170bdbbbad8

EntactoBob (2015), 'Useful templates for reviewing DNM vendors and their products', https://www.reddit.com/r/DarkNetMarkets/comments/2uyrs7/psaarticle_useful_templates_for_reviewing_dnm/

Gosh-Damit (2015), 'Emerald Triangle — 1/2oz Blue Dream', https://www.reddit.com/r/DarkNetMarkets/comments/35xn6c/vendor_review_emerald_triangle_12oz_blue_dream/

Harris, S. (2013), 'Feds bust the Amazon of drugs, seize its untraceable loot', http://foreignpolicy.com/2013/10/02/feds-bust-the-amazon-of-drugs-seize-its-untraceable-loot/

Jeffries, A. (2014), 'The LSD Avengers, Silk Road's self-appointed drug inspectors, announce retirement', https://www.theverge.com/2013/10/14/4828448/silk-road-lsd-avengers-drug-inspectors

Kopstein, J. (2013), 'How the eBay of illegal drugs came undone', http://www.newyorker.com/tech/elements/how-the-ebay-of-illegal-drugs-came-undone

O'Neill, P. (2014), 'How the Deep Web's biggest 4/20 sale helped bring down the Silk Road', http://www.dailydot.com/crime/tony76-420-sale-silk-road/

Ormsby, E. (2012), 'The great 420 scam', http://allthingsvice.com/2012/05/30/the-great-420-scam/

SilentRaider3 (2015), 'Frosties2014 selling PMA as MDMA', https://www.reddit.com/r/AgMarketplace/comments/342odf/frosties2014_selling_pma_as_mdma/

SECTION II

Dark net markets — key actor perspectives

CHAPTER 6
Silk Road: insights from interviews with users and vendors

CHAPTER 7
The emergence of deep web marketplaces: a health perspective

CHAPTER 8
The drug trade on the deep web: a law enforcement perspective

CHAPTER 9
How the use of the internet is affecting drug trafficking practices

Overview

This section explores internet drug markets from the perspectives of a number of central protagonists in dark net markets, the experiences of Silk Road users, a 'frontline' health professional working in cryptomarkets and a law enforcement representative are presented.

In Chapter 6, Eileen Ormsby, who has been following Silk Road and blogging on the topic from its inception, presents findings from her interviews with a variety of Silk Road users, including sellers, buyers and administrators. She provides insight into the social profiles of Silk Road users and their motives for engaging in this cryptomarket. She also explores the ideology and sense of community central to the early Silk Road marketplace and forums. She concludes her chapter with user feedback on the closure of Silk Road marketplace and the consequences of its disappearance.

For Fernando Caudevilla, dark net marketplaces offer opportunities and a setting for targeted actions aimed at reducing risks associated with drug use. As he explains in Chapter 7, cryptomarkets can be a virtual setting for harm reduction interventions. As a physician, Fernando has been providing information and advice from a risk reduction perspective to drug users in dark net marketplaces since 2013 through his own forum thread ('Ask a Drug Expert Physician about Drugs and Health'). In this chapter, Dr Caudevilla shares his experiences of providing health advice in these forums and presents results from drug testing of samples purchased online.

In Chapter 8, Joost van Slobbe introduces the law enforcement approach to combatting online drug supply via dark net markets. He explores the similarities and differences between actual and digital market places, the key market players, law enforcement strategies, as well as intended and actual effects.

In Chapter 9, Anita Lavorgna presents a criminological analysis of drug supply and trafficking covering both the deep and the surface web. She explores the different levels at which the internet is used for drug supply and distribution purposes, the new criminal opportunities offered through online markets and the need for proactive online policing.

6

CHAPTER 6

Silk Road: insights from interviews with users and vendors

Eileen Ormsby

Introduction

Between January 2011 and October 2013, Silk Road, dubbed the 'eBay' or 'Amazon' of illicit drugs, grew from an underground black market known by few, to a slick commercial enterprise that had been accessed by over a million people. It is estimated that, in a little under three years, the site's users spent around USD 200 million (Flitter, 2015) on a range of drugs: cannabis, prescription drugs, MDMA, LSD, heroin, crystal meth; in fact, every illicit drug.

Silk Road was the first of the contemporary dark net markets to provide a mainstream clientele with an anonymous, accessible method of purchasing drugs. This chapter presents the findings from interviews with hundreds of users of Silk Road carried out over three years. It gives an overview of the types of people using Silk Road, what they purchased and their reasons for preferring the online model over traditional methods of procuring drugs.

Interviews and the collection of individual stories were carried out by an investigative journalist over a number of years. Participants included Australian-based buyers, who provided their stories in person or by telephone, and active members of the Silk Road marketplace and forums from around the world, who provided their stories by email, private forum messages or encrypted chat. Those participants usually remained anonymous. Any who claimed to be prominent members of Silk Road (staff or vendors) could verify their pseudonyms in a variety of ways, most often using PGP encryption and signatures. Some participants responded to requests for interviews and case studies for mainstream and independent news stories and blog posts or for inclusion in a book. Others contacted the journalist independently to tell their stories.

It is accepted that there is a self-reporting bias in the stories, as certain people may be more inclined to agree to an interview. In particular, those who proactively sought out the opportunity to tell their stories were keen to dispel common notions of drug users as junkies and thieves and may have presented an incomplete or one-sided version of their drug habits.

The Silk Road user

> *Believe it or not I am pretty much as technically unsavvy as they come but I had heard someone talking about getting drugs online from a little place called Silk Road. Did a little searching, a little researching, and next thing I know I find myself amongst a very different community.* — 'Dan' ([1])

Drug users come from all backgrounds and demographics. Computer use is no longer the domain of the young and technologically advanced. Thus, there is no truly 'typical' Silk Road user. However, several key themes came up repeatedly among the users who provided interviews.

Who?

> *I work hard, I pay my taxes. I'd never hurt anyone on purpose. If I choose to wind down with something I enjoy more than alcohol, why does that bother anyone else?* — 'Malcolm'

According to the prosecution case against Ross Ulbricht (who has been convicted of being the founder and owner-operator of Silk Road), Silk Road users were almost exclusively based in the United States, the United Kingdom, other parts of Europe, and Australia and New

([1]) All names have been changed or online pseudonyms used.

Zealand (United States District Court Southern District of New York, 2013).

Although coming from a broad demographic, the majority of those Silk Road users who agreed to be interviewed were employed with disposable income, technologically literate and aged in their 20s to 40s. However, the site's users ranged from teens to one member who claimed to be in his 70s. Some used Silk Road to purchase medicinal cannabis, others to feed addictions, but most were recreational users.

Every buyer interviewed had used drugs prior to finding Silk Road. None reported deciding to try drugs only because they had discovered the marketplace. Most heard about Silk Road through friends; many found it after reading a media story. A few discovered it through the early online equivalent of word of mouth, niche internet discussion forums, where news of the site first spread in January 2011.

'Stacey' was in her late 30s when first interviewed in 2011, professionally employed and a heavy recreational drug user. Her drug use began in her mid-teens and she never considered herself a problem user, occasionally abstaining for several months with no ill effects.

The drugs she used changed over time. In her teens, it was cannabis and speed (amphetamine), but as she got older she settled on MDMA and psychedelics as her drugs of choice, with cocaine a special treat when she could afford it. Before Silk Road, her pattern of purchasing was typical of many recreational users. She bought from friends of friends, or from small-time dealers to whom she was introduced by acquaintances. 'Most of them didn't last long,' she said. She would find a trustworthy and reliable dealer and they would stop dealing, or become less reliable, for a variety of reasons, most often a dearth of product.

A number of Stacey's friendship circle also agreed to be interviewed. All were within a similar demographic: late 30s to early 40s, employed and with disposable income. More than half had children. They ranged from occasional to regular recreational drug users. None considered themselves criminals. All felt that Silk Road provided a more sophisticated and convenient method for purchasing drugs that was more congruent with their lifestyles than sourcing from the street.

It was like being a kid in a candy store. — 'John'

There were those who 'rediscovered' drugs through Silk Road: people in their 50s and 60s who had used cannabis and LSD in their youth but who no longer had or wanted contact with drug scenes. Some of these users also discovered new drugs as a result of participating in Silk Road.

I came for the drugs. I stayed for the revolution. — anonymous Silk Road member

Although the majority of Silk Road users were interested solely in buying quality drugs in a safe and convenient setting, some were attracted by the ideals and philosophies espoused by the site's owner, Dread Pirate Roberts.

Silk Road was built on a platform of agorism ([2]) and anarcho-capitalism, with the stated intention of building a free-market system that would eradicate coercive force by the state. Few users interviewed subscribed wholly to the hardline free-market position of the site's leader, but all had libertarian views when it came to the right to choose what to put in one's own body.

Those interviewed had both left- and right-wing political views. Many did not believe an unregulated illicit drug market was an ideal manner of acquiring drugs; it just happened to be the best way available while their drugs of choice were illegal. Most of those interviewed would have preferred to see an end to prohibition and the 'War on Drugs', something that would put markets such as Silk Road out of business altogether.

I saw the relative ease that came with it. There was a personal level of safety [from law enforcement], as well as anonymity. — heroin dealer Michael Duch, aka 'Deezletime' (United States District Court Southern District of New York, 2015)

The dealers interviewed invariably shared characteristics with many of their street-dealing counterparts. They were males in their 20s to 40s (or at least that was what they claimed; most dealers were reluctant to meet face to face and interviews were conducted via encrypted message). Many of them were former small-time street dealers who had found a new, lucrative market.

([2]) Founded by Samuel Edward Konkin III, agorism is a libertarian philosophy based on market anarchism with the ultimate goal of bringing about a society in which all relations between people are voluntary exchanges. Konkin believed in a totally free market devoid of violence or coercion by either market participants or the state.

However, interviews with vendors also suggested that a new breed of drug dealer was emerging. While most had experience of procuring and supplying drugs to their friends, some had never dreamed of dealing on a more professional level. They were ill equipped to become part of the drug trade that included contact with hardened criminals. Dark net markets provided them with an opportunity to sell drugs anonymously and safely.

Although many Silk Road dealers were one-man operations, the more popular vendors required a team of staff to keep up with demand. They would split tasks across the team, so that those who ran the computer side of the business were never in possession of drugs.

What?

Silk Road was a marketplace from which any illicit drug could be purchased. The majority of users who granted interviews were recreational users of MDMA, psychedelics and cannabis. Few of those interviewed were purchasers of heroin or methamphetamine, although whether or not this was a result of self-selection bias is difficult to determine. However, reading through the forums and viewing the most popular listings on the marketplace seemed to confirm that the most popular purchases were 'soft' or 'party' drugs.

Such anecdotal evidence was bolstered by the results of a global drug survey conducted by dance and clubbing magazine *Mixmag* in conjunction with *The Guardian* in 2012. Over 15 000 people from around the world filled in the online survey, which posed a wide range of questions about drug use. It included questions about Silk Road (Winstock et al., 2012–2014).

The findings from this survey relating to Silk Road were published in the academic journal *Addiction* (Barratt et al., 2014). MDMA was the most popular drug purchased by Silk Road users in the three countries that made up the bulk of Silk Road's customers (the United States, the United Kingdom and Australia). This was followed by cannabis, LSD and cocaine. Heroin and methamphetamine did not feature in the top 10.

These statistics, which were self-reporting by survey respondents, were empirically backed up some time later by researchers Judith Aldridge and David Décary-Hétu in a 2014 academic study. They collected data by crawling the visible listings on the Silk Road website. They estimated that 'in annual revenue terms, the vast majority of sales were for cannabis (USD 24.8 million), MDMA (USD 19.9 million) and psychedelics (USD 8.6 million)'. 'Drugs associated with drug dependence, harmful use and chaotic lifestyles (heroin, methamphetamine and crack cocaine) do not appear much on Silk Road, and generate very little revenue' (Aldridge and Décary-Hétu, 2014).

This is not to say that there were no problem users on Silk Road. One heroin user claimed Silk Road had been 'a godsend'. He credited it with providing him with a regular, affordable supply of consistent quality that allowed him to function and hold down his job while maintaining his addiction. However, he also said that the necessary delay between ordering and receiving the heroin was helping him get off the drug: 'learning to have to wait till next day, made me finally realise that I could wait ... delay, delay ... it's given me a last chance at life' ('Paul', October 2013).

> *The group I am in charge of wholesales MDMA here in the UK and I had originally considered vending that on the road, but at the time, nobody bought more than a few hundred dollars' worth of products.*
> — 'StExo'

Silk Road was designed to bring together buyers and sellers of small personal quantities of drugs. The creator of the site, when first advertising it, described it as 'kind of like an anonymous amazon.com' (Bitcointalk.org, 2011), suggesting that, as with Amazon, the purchaser would be the end-user of the product. Interviews with Silk Road purchasers supported this. All who agreed to be interviewed bought drugs from the website for their personal use.

Aldridge and Décary-Hétu (2014) challenged this notion, stating that their research led them to believe that 'Silk Road was an online marketplace catering primarily to those making purchases for resale; that is, to street drug dealers buying stock to sell offline'.

They recognised that some of their data included people who 'may have been buying for personal use over a longer term, or perhaps making "social supply" purchases on behalf of a group of friends', but stated that they thought these accounted for only a small number of the larger purchases.

Interviews with users suggested stockpiling and social supply to be the norm, rather than the exception. Most buyers were more concerned about having a high quantity of envelopes delivered than about receiving a high volume of drugs in one delivery. 'The charge is the same whether I buy one gram or ten [grams of MDMA],' said 'Joel', 'so why risk a bunch of deliveries where one

might get picked up and tip off my address to customs?'

Ten grams of MDMA — a quantity that is considered by law enforcement to be for supply rather than personal use — was a typical order for a regular user or festival-goer. Stacey claimed that 10 g would last 'maybe four weeks', although she did admit that having such quantities easily available made her more likely to 'top up' as soon as the effects started diminishing, and also made her more generous in sharing the drugs with friends than she otherwise might have been.

> *In the old days, when you'd buy five pills for around the same amount as you can buy five grams of MDMA on Silk Road [equivalent to around 30–40 capsules, depending on strength], you'd be more likely to keep them all to yourself.*

As with recreational users in real life, social supply was also common. A group of friends would pool resources and the one member of the group who had access to Silk Road would place the order. Risk was shared by rotating the address to which the order would be mailed. This would enable the group to receive discounts for larger orders and to build up strong buyer statistics. Because they gave vendors access to quantity and volume of purchases, accounts with good buyer stats were given certain advantages. They might receive promotional freebies or overweight orders and were more likely to be offered a no-questions-asked re-ship if they claimed that items had gone missing, rather than having to go to Silk Road to resolve a dispute.

> *Many people here purchase in bulk as well as retail quantities.* — Dread Pirate Roberts

Although information gathered from interviews suggested that it was only end-users who purchased from Silk Road, it is likely that those who bought to make offline sales locally were less inclined to be interviewed. StExo, who found that there was not enough demand for bulk MDMA in early 2012, went on to run a money laundering business instead. However, Aldridge and Décary-Hétu's findings that the quantities sold indicated that dealers were purchasing to sell offline resulted from analysis after Silk Road had been operational for a couple of years. By then, it had enough of a customer and vendor base to attract bulk purchases.

Australian purchasers of bulk quantities often bought in order to re-sell to Australian Silk Road customers. They would buy large amounts of (most often) MDMA from the United States or Europe, which would then be divided into capsules and sold to Australian users who did not want to risk a customs seizure or wanted overnight delivery. The dealer's profit in this situation would be around 400 %.

Why?

Several key themes emerged consistently from the interviews when exploring why drug users chose to buy from Silk Road rather than using traditional methods. These were price (in some regions), availability and convenience, quality, eradication of violence and libertarian ideals. Vendors cited similar reasons for choosing to sell online, although profitability was paramount.

Price and availability

The number one reason users gave for buying online was the price and availability of their drug of choice. For the geographically isolated Australians and New Zealanders, recreational drugs — particularly the most popular, MDMA and LSD — cost a quarter of the normal price when ordered overseas on Silk Road. Users in most parts of the United States and Europe were also happy with the prices, although these were not as dramatically different as in Australia and New Zealand.

The range of products on offer was also a factor. Different strains of cannabis, designer psychedelics that were otherwise hard to come by and prescription drugs were easily available. Those interviewed who had tried new drugs as a result of participating in Silk Road invariably stuck to similar types of substances to those they already favoured. Thus, someone who enjoyed LSD and mushrooms might try psychedelics in the 2C family, the most popular of which was 2C-B.

Some users found that Silk Road meant they could order their preferred drugs for use on holiday. Users would arrange a delivery to their overseas hotel from a vendor near their destination. They felt that this involved less risk than smuggling drugs on an airplane, arguing that good hotels are protective of their customers' privacy and would not question the arrival of a package'.

For vendors, the overwhelming motivation for selling on Silk Road was profitability. One vendor interviewed in

early 2012 claimed a turnover of more than USD 4 000 per day, 75 % of which was profit. Another, who sold a variety of drugs, said that his profit on cocaine alone was USD 20 000 per month. All of the vendors agreed that the commission structure charged by Silk Road (6–12 % per transaction) was fair and reasonable.

A seller who had built up a solid reputation could expect hundreds of orders a day. 'I made it into the Top Ten, and let me just say, the money is GOOD!' said one vendor. '[Silk Road] could take 50 % tax and I'd still be making a killing.'

Some markets were particularly lucrative. 'Personally I am completely financially motivated in what I do … I went through the local Australian listings, did a bit of maths and thought "Wow, these guys are paying ridiculous prices for their drugs, there's definitely profit to be made here!" ' said AussieDomesticDrugs, who sold exclusively to Australian and New Zealand buyers.

Quality and harm reduction

> *Samples of these purchases have been laboratory tested and have typically shown high purity levels of the drug the item was advertised to be on Silk Road.* — FBI (United States District Court Southern District of New York, 2013)

More importantly, users felt they were getting value for money. The user feedback model that works so well on sites such as eBay was just as effective on the black market. Sellers had the incentive of repeat business to ensure their product was as described. Regular online black market users were sophisticated when it came to spotting padded or faked feedback.

Occasional drug users invariably find that the quality of their purchases is variable. Even those with 'reliable' small-time dealers have to rely on a long supply chain, along which drugs may be cut or substituted. In addition to the system of feedback, Silk Road spawned groups such as the 'LSD Avengers', who tested and provided detailed analyses of various vendors' products. Like restaurant reviewers, the LSD Avengers made purchases anonymously and reported their findings, although they soon found that vendors began to send them free samples for review.

The tested quality of Silk Road's drugs assisted in harm reduction. Many users had previously purchased 'ecstasy' and discovered that, instead of MDMA, the main ingredient in their pills was inferior piperazines or PMA. Similarly, purchasers of LSD had found themselves imbibing 25i, which has a toxicity not found in LSD. Users reported few, if any, substitutions when purchasing from Silk Road.

Eradication of violence

> *It's cheaper, it's higher quality and I don't have to meet some guy in an alley or a dodgy apartment — it comes to me. What's not to like?* — 'Stacey'

Buyers and sellers alike expressed the desire to be able to make drug transactions without the fear of violence or other problems often associated with traditional drug deals. An online model, where both parties remained anonymous and were probably geographically separated, removed any possibility of an aggressive resolution to a dispute between buyer and seller.

Female interviewees in particular perceived Silk Road as providing them with a safe alternative to purchasing drugs in person. Many had faced requests for sexual favours in lieu of payment for drugs. Even when there had been no repercussions to a refusal, female users often felt frightened and intimidated by male sellers in person.

> *The best thing about selling online is not having to deal with people knocking on my door or ringing me at all hours.* — AussieDomesticDrugs

Vendors were equally enthusiastic about not having to deal with their customers face-to-face. Not only did dealers have to be wary of customers, who might use violence to rob them of their wares, many found that habitual drug users could become irritating when looking for drugs at short notice. They knew their dealers' addresses and their phone numbers and demanded that they be available day and night. Silk Road provided them with the opportunity to deal with orders at times convenient to them, and to ensure their best customers' orders were prioritised.

Low-end street dealers might find that they need to compete with other sellers nearby for local trade. Prolific vendor JesusOfRave said that, rather than compete for turf, the vendors of Silk Road collaborated and assisted

each other: 'There are more buyers than sellers can stock. There was no sense of competition for us during our time on Silk Road.'

Despite the fear of violence being an oft-quoted reason for purchasing online rather than by traditional means, the majority of interviewees admitted that they had never faced any violent behaviour in their real-life dealings. However, they were all acutely aware of the potential for a deal to go sour, and the fear itself created high levels of anxiety.

Community and ideals

> *It really is more than a place to buy drugs. It's a place to hang out, make friends and just talk shit.* — 'Zach'

For many, Silk Road was more than just a marketplace. For them, the website had become a close-knit community of people from all around the world with one thing in common: illicit drugs. Although less than half of those interviewed actively engaged in the Silk Road discussion forums, many of those who did cited their value as a source of advice, information and friendship.

In 1.2 million posts on over 70 000 topics, discussions on the site's forums covered everything from sophisticated methods of evading law enforcement to favourite movies to watch when stoned. But they covered much more than that. Dread Pirate Roberts fostered a community that was active and highly engaged. He encouraged philosophical discussions and sharing of knowledge. The online community was particularly important to those whose drug-taking was a solitary pursuit.

Professionals shared their knowledge of chemistry, the law in various jurisdictions and harm reduction. The drug safety forum was one of the most popular; there, members could receive useful, realistic advice on harm reduction and the dangers of drugs, and assistance with giving up highly addictive drugs. Silk Road member 'DoctorX' (see Chapter 7) was a family physician who provided a service, dispensing advice aimed at minimising potential harm from drug use.

'The SR [Silk Road] community has probably been the best support and advice I've got actually,' said former methamphetamine user Ben. 'The mental health system really isn't recognising, as best as I try to explain it to them, what I am actually going through.'

> *There is a great deal of cooperation and skill sharing amongst vendors.* — JesusOfRave

JesusOfRave claimed that their team did not start selling on Silk Road only because it was a new means of doing what they were already doing — selling drugs at a profit — but also because the team fully subscribed to the philosophy of the site. 'This has a large part to do with DPR's [Dread Pirate Roberts'] writings. We feel we share complementary ethics,' said a representative. JesusOfRave regularly engaged with customers and other members in the forums.

Silk Road seizure and law enforcement efforts

> *Now I've got to go back to associating with criminals and the dregs of society to get my drug of choice. And if that's not bad enough the quality of the H [heroin] that I get in real life is sub-par to the stuff I was getting on Silk Road.* — 'Paul'

On 2 October 2013, Silk Road was seized; the site was shut down and its owner arrested. The shutdown apparently did nothing to stop drug users purchasing their wares online, with a clone site appearing five weeks later and several new, more technically robust, markets opening and vying for market share.

Interviews conducted with users immediately after the shutdown revealed that, for some, the seizure of Silk Road was a catastrophe, but, for most, it was little more than a temporary inconvenience. By the time Silk Road was closed, many vendors were already active on two other active black markets, Sheep and Black Market Reloaded. Able to verify that they were dealing with the same seller by use of encrypted signatures, users simply migrated to the alternative websites.

Other users had by that time formed relationships with their favourite suppliers, enabling them to make private transactions via secured email, bypassing the black markets altogether.

However, some were unnerved by the shutdown, particularly in the weeks afterwards, when it was unclear

if the technology that enabled anonymous buying and selling had been compromised. Those users said they would return to traditional methods of buying for the time being, but expressed frustration that they would have to go back to a system that had more inherent dangers and flaws than the online model. No one indicated that closure of the site would stop them using drugs.

> *The damage was going to be considerable, I had a lot in escrow on all of my buying and selling accounts. Once I had calculated the damage it was over $60,000 worth of BTC [bitcoins]. A lot less than I had made in the time I'd been selling there but a considerable loss regardless.* — AussieDomesticDrugs

Vendors complained of losses of bitcoins held in escrow that had yet to be released from orders dispatched in the weeks before the shutdown, but most had already signed on with the alternative markets. Their customers soon followed them.

Overall, for vendors and buyers alike, the shutdown of Silk Road was inconvenient but appeared to have little effect in the medium term.

Conclusion

Users of Silk Road and other dark net markets are a varied group, but several themes came through repeatedly: the beliefs that drug use was not morally wrong and that people had the right to take drugs without interference from government or law enforcement; relief at the opportunity to purchase drugs in a safer environment (i.e. dealing with criminals virtually rather than in person); a belief that the market supported harm reduction by providing information on the quality and contents of purchases; and a feeling that Silk Road offered a sense of community.

The shutdown of Silk Road and the arrest of its owner has seen the emergence of over 20 similar markets. Some are single-item markets. Most are small. Two — Evolution and Agora — grew to be bigger than the original Silk Road. New markets seek to combat rogue operators by offering multi-signature escrow, which means the marketplace cannot access funds in escrow without a second 'key', that of either buyer or seller. Emerging markets plan to fight law enforcement infiltration by becoming decentralised, using peer-to-peer technology that is similar to that used to pirate music, movies and software.

Notably absent in the current markets is the strong community feeling fostered by Silk Road. The trial of Ross Ulbricht in January and February 2015 was not a major topic of conversation in the forums of Agora or Evolution, the leading dark net markets at the time of writing ([3]). Discussions concentrated on the quality of the drugs, the best suppliers, avoiding scams and evading law enforcement efforts.

Although some dark net market users lament the loss of Silk Road, many have found it a relief. 'Silk Road courted publicity at the end, putting a major target on their back,' said Sam. 'All these noobs stumbling their way in without any sense of self-preservation became really annoying. We're back to where we were supposed to be — flying under the radar.'

References

- Aldridge, J. and Décary-Hétu, D. (2014), 'Not an "eBay for drugs": the cryptomarket "Silk Road" as a paradigm shifting criminal innovation'. Available at: http://ssrn.com/abstract=2436643 or http://dx.doi.org/10.2139/ssrn.2436643
- Barratt, M. J., Ferris, J. A. and Winstock, A. R. (2014), 'Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States', *Addiction* 109(5), pp. 774–783.
- Bitcointalk.org (http://bitcointalk.org) (2011), thread 'A Heroin Store', post by Altoid, 29/1/2011.
- Flitter, E. (2015), 'U.S. sharply reduces Silk Road's estimated sales volume,' *Reuters*, 16/1/2015.
- Konkin, S. E. III (2008), *An Agorist Primer*, KoPubCo, California.
- United States District Court Southern District of New York (2013), *United States of America vs Ross William Ulbricht, a/k/a 'Dread Pirate Roberts'*, Criminal Complaint, 27 September 2013.
- United States District Court Southern District of New York (2015), *United States of America vs Ross William Ulbricht*, trial transcripts, January–February 2015.
- Winstock et al. (2012–2014), *Global Drug Survey*, findings reported at www.globaldrugsurvey.com

([3]) After just over a year of operation, the owners of Evolution carried out an 'exit scam', closing the market without notice and absconding with the bitcoin balances held in users' accounts and in escrow.

7

CHAPTER 7

The emergence of deep web marketplaces: a health perspective

Fernando Caudevilla

Introduction

Deep web marketplaces (DWMs) represent a major change in online drug trading. Although they are currently a limited phenomenon, their operational characteristics offer significant advantages for both buyers and sellers, and it is likely that their importance will grow. The structure of DWMs facilitates communication, exchange and dissemination of information. This provides opportunities for health professionals to engage with users. This chapter discusses some aspects of DWMs from a health perspective and describes harm reduction strategies developed specifically for DWMs.

The internet, drugs and health

The internet has changed many aspects of healthcare. Health professionals have traditionally been considered an undisputed and unique source of knowledge, and the role of patients has been to passively accept medical advice. However, this relationship has been transformed by the democratic access to information and the interactivity provided by the internet. Virtual communities, chats, discussion forums, online social networking services and virtual libraries are tools that change the balance of knowledge between health professionals and the public, empowering patients to become more involved in decisions related to their health. The internet is also a powerful tool for professionals, and clinicians and researchers have increased access to scientific publications, guidelines and professional tools that facilitate research and improve knowledge and abilities. On the other hand, dissemination of inaccurate or inadequate messages can have negative health consequences and is a growing concern, given that it is sometimes difficult to evaluate the quality of information online.

In relation to illegal or recreational drugs, these changes have been even more dramatic. Drug information provided through traditional media has tended to focus on universal prevention, encouraging people to reject any use of illegal psychoactive substances, not differentiating between use, abuse and dependence, and often exaggerating the negative aspects and consequences of drug use. In the age of the internet, however, resources focused on harm reduction, including more information about risks and harms, have gained popularity.

Alexa Internet ([1]) is a company that provides web traffic data analysis, classifies websites according to their global popularity and generates a score (Alexa ranking (AR)) that is considered the 'gold standard' for estimating the importance of websites on the internet, with lower AR scores denoting greater popularity. Websites aimed at providing harm reduction information, such as Bluelight ([2]), Drugs Forum ([3]) and Erowid ([4]), have higher Alexa rankings (Bluelight, 16 356; Drugs-forum, 19.965; Erowid, 20.670) than official prevention web pages such as the US National Institute of Drug Abuse ([5]) (28 686) or the United Nations Office on Drugs and Crime (UNODC) ([6]) (50 942). It is also important to note that harm reduction websites are generally run by volunteers or small non-governmental organisations with limited technical and economic resources compared with official government prevention websites. It is likely that these virtual communities of individuals using the internet all over the world are having an impact on social perceptions about illicit drugs.

([1]) http://www.alexa.com
([2]) http://www.bluelight.org
([3]) http://www.drugs-forum.com
([4]) http://www.erowid.org
([5]) http://www.drugabuse.gov/
([6]) http://www.unodc.org/

Online drug trading: from research chemicals to deep web marketplaces

As with any other consumer goods, illicit drugs have been offered online since the internet began. However, until recently, their illegal status has made this business extremely difficult in practice. Purchasing illicit drugs through an internet website or forum on the surface web gives no guarantee about the quality of the product or that the product will actually arrive. Payment and shipping allows the purchaser to be physically identified and there is no possibility of lodging a complaint. Nevertheless, small closed-access websites and forums have always existed where select individuals can purchase illicit drugs by invitation; their impact, however, has been limited.

From the mid-90s to 2003, a limited selection of psychoactive substances were offered online as 'research chemicals'. In general, they were phenethylamine and tryptamine derivatives, coming from discreet websites offering high-purity products. Consumers were, in general, individuals with an interest in psychoactive substances (so-called psychonauts); the phenomenon didn't attract the attention of the media and was of very limited significance. The US Drug Enforcement Administration closed most of these websites in July 2004.

The phenomenon re-emerged around 2007 in the form of 'legal highs', with visually attractive websites employing well-known marketing strategies such as special offers and discounts ('product of the week', 'buy 3 pay for 2', etc.) and offering a wide variety of drugs (synthetic cannabinoids, cathinone derivatives, pyrovalerones, NBOMe series, methoxetamine, etc.) marketed as herbal blends, incense, fertilisers, and so on. The main purpose of this market was to sell non-controlled substances. Most of the substances had not been studied in animals and there was a lack of data about human toxicology or psychoactivity from basic science studies. In many cases, product samples contained a mixture of different substances and, sometimes, products with identical labels contained different active substances (Caudevilla et al., 2013). There was high availability of these substances, some of which have much potential for harm (Johnson et al., 2013).

DWMs represent a significant change in the online drug trade. Relations between vendors and consumers are largely based on trust and professionalism, and are supported by user feedback and resolution models (Van Hout and Bingham, 2013). Forums linked to these markets provide user advice, 'trip reports', and product and transaction reviews. Some of these markets sell only psychoactive substances and support or integrate a harm reduction philosophy. In other cases, DWMs offer not only drugs but also counterfeit goods, stolen credit cards or weapons. However, offering child pornography, services of 'murder for hire', traffic of persons or human organs are strictly forbidden activities in these kinds of markets.

DWMs can also provide a virtual setting for harm reduction. The structure of DWMs allows the creation of virtual communities that share information, knowledge and experiences. For many individuals, it is not a matter simply of 'buying drugs', but a question of belonging to a community that shares similar interests. The implications of these aspects for prevention deserve further and more detailed research. Feedback from other users, posts in forums and control by site administrators allow users to be relatively well informed about the quality of products. Many vendors state that their products have been 'lab-tested' and offer information about purity. Users can leave their opinions about the quality of products and experiences with vendors. Many vendors communicate directly with users in forums, announce when a new batch of a substance is available, provide and share advice about safer use and openly discuss quality, purity, adulterants and advertisements. This system is imperfect, but it offers users more reliable information than that provided in the traditional street drug dealing system. So, in general, DWMs provide some advantages for both buyers and sellers compared with street-level distribution.

Technical difficulties in accessing and operating DWMs and the fact that a real postal address must be provided to receive the product are currently the main drawbacks for many users. There is no clear estimate about the market share of DWMs in relation to the whole global trade in illicit drugs, but it is likely to be very limited at present. Nevertheless, there are signs that suggest there may be increased interest in the future.

'Ask a Drug Expert Physician about Drugs and Health'

Internet forums are online discussion sites where people can hold conversations in the form of posted messages. Their structure is hierarchical: a forum can contain different sub-forums dedicated to different themes covering several topics or threads. In forums, administrators manage the technical running of the site and can give privileges to some users. Moderators are

users or employees of the forum who have been granted access to the posts and threads of all members for the purpose of moderating discussions and managing day-to-day affairs in the forum. The characteristics of organisation, structure, classification of information, democratic participation and simplicity of use make these online forums very popular, and they are often used as sources of information and sites where discussion can take place.

Online drugs forums have been used for scientific, medical and prevention research in different ways. Analysing information contained in them is a simple way to obtain some data (patterns of use of emerging drugs, motivations, harm, etc.) that would be very difficult to collect using other methods (Lefèvre and Simioni, 1999; Kjellgren et al., 2013; Månsson, 2014). The use of internet forums to recruit participants for studies can be very helpful when the subject of the study has a low prevalence or when it involves hard-to-reach populations (González et al., 2013; Caudevilla-Gálligo et al., 2014). The role of internet-based treatments using forums, chats or mobile phone applications has also recently been studied in fields such as smoking cessation (Civljak et al., 2013), social anxiety disorder (Schulz et al., 2014) and anxiety and depressive disorders (Schulz et al., 2014). Online drug forums can also be an environment where strategies for risk and harm reduction can be provided to drug users.

Most DWMs have associated forums, usually administrated or moderated by the same staff who run the marketplace. Nine of the eleven popular DWMs operating in February 2015 had an associated forum. At this time, the forums in Evolution ([7]) and Agora ([8]) were the most popular, with thousands of registered users and hundreds of new posts and messages every day. Forums in DWMs have a similar structure to those in the surface web: there is a general section for discussion about the market, and also sub-sections where users can discuss the quality of products, reviews of vendors, security, packaging, legal aspects, bitcoin, and so on. In most forums, there is also a sub-section dedicated to 'drug safety' where users discuss topics directly related to drugs and health (patterns of use, intoxication, adulterants, dosage, etc.).

The author of this chapter has been running threads (entitled 'Ask a Drug Expert Physician about Drugs and Health') in DWM forums providing information and advice to drug users from a risk reduction perspective. This service started in April 2013 in the original Silk Road forum ([9]) and moved to the Silk Road 2.0 forum ([10]) when Silk Road was closed by the FBI. Silk Road 2.0 was shut down in November 2014 and, since then, its forum has not been accessible. For this reason, the service was moved to Evolution ([11]).

TABLE 7.1
Summary of activity in an online health service for deep web drug users

Market	Dates	Number of questions (public)	Number of questions (private)	Total visits
Silk Road	Apr. to Oct. 2013	321	67	36 438
Silk Road 2.0	Dec. 2013 to Nov. 2014	352	103	52 725
Evolution	Dec. 2014 to Feb. 2015	258	45	47 244 ([1])

([1]) Thread active; data up to 2/2/15.

Most DWM users remain anonymous and do not give any clues about their identity in the real world. The author uses the nickname 'DoctorX' in the deep web, but, in order to gain credibility, DoctorX's real identity has been revealed, with a link in the forum profile to a professional web page with complete information about his profession and skills. The service is free of charge, but supported by anonymous and volunteer donations in bitcoins.

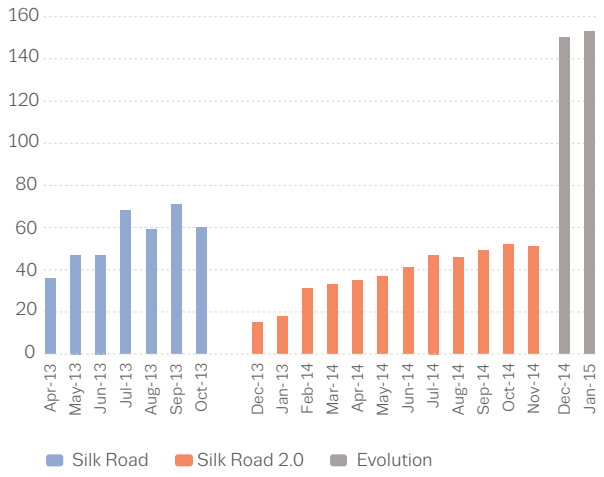
'Ask a Drug Expert Physician about Drugs and Health' (threads in Silk Road, Silk Road 2.0 and Evolution during a 22-month period) had received 136 407 visits on 3 February 2015 and 1 146 questions had been answered, 931 in the public forum, accessible to any visitor, and 215 as private messages from people who, for whatever reason, wanted to ask their questions privately. Data are summarised in Table 7.1.

Although a structured qualitative analysis has not been performed, the general impression is that the reception of this service in the community has been very positive. All the threads received many messages from users expressing support, appreciation and gratitude. Some users have offered collaboration, for example editing in English, gathering similar answers to create a 'Frequently Asked Questions' section or referring users to DoctorX's thread when questions about health are asked in different posts or forums. Some vendors have also asked questions aimed at improving safety of the products

([7]) http://i25c62nvu4cgeqyz.onion
([8]) http://lacbzxobeprssrfx.onion

([9]) The original forum was closed by the FBI in October 2013. A complete backup can be downloaded from http://antilop.cc/sr/download/stexo_sr_forum.zip
([10]) The forum was closed by the FBI/Europol in November 2014. No copies have been found.
([11]) 'Ask a Drug Expert Physician about Drugs and Health', Evolution forum, http://i25c62nvu4cgeqyz.onion/viewtopic.php?id=35190 (available only through Tor).

FIGURE 7.1
Number of questions answered by month



they are selling. The attitude of DWM administrators and moderators has also been very collaborative: the thread has always been highlighted, and technical or general support has been offered in all cases. The popularity of the thread has increased, as shown in Figure 7.1, where the number of questions answered each month in the three markets during a 22-month period is presented.

Questions in the thread have been categorised using a qualitative analysis technique that involves coding the posts and collating them into meaningful and distinct themes. The main themes that emerged are summarised in the box below.

Themes of frequently asked questions in an online health service for deep web drug users

- Drug effects, patterns of use, dosage
- Adverse effects
- Medical contraindications
- Pharmacological interactions with prescription drugs
- Pharmacological interactions with other illicit drugs
- Patterns for detoxification
- Therapeutic use of cannabis
- Neurotoxicity
- Long-term effects of drugs
- Urine detection of drugs
- Use of drugs during pregnancy and lactation

In order to better understand the nature and characteristics of questions asked in the 'Ask a Drug Expert Physician about Drugs and Health', some examples are shown in the box on p.73. Case 1 is particularly notable. The questioner asked about long-lasting symptoms that he attributed to opiate abstinence. However, fever, profuse sweating, enlargement of the lymph nodes and pain during the night suggested the need for a complete medical evaluation. A week later, the user posted in the forum that he had this done after reading the answer and that blood test results had revealed that he was suffering from leukaemia (Ormsby, 2014).

A drug information and counselling service in a DWM forum provided by a professional physician who specialises in drugs and harm reduction is an opportunity to reach drug users where they are. This 'virtual outreach' technique is perceived as reliable, effective and able to provide useful information and skills to drug users, although many aspects deserve further and deeper evaluation. It also has its own limitations and disadvantages, as messages in an internet forum provide very limited information compared with a real, face-to-face interview and intervention. It is important to remember that many drug users are reluctant to ask their questions of traditional health services because they feel they will be judged, or are afraid of professionals' moral prejudices. In many parts of the world, services aimed at drug users are simply non-existent.

Testing drugs purchased through deep web marketplaces: the International Drug Testing Service (IDTS)

Drug checking services are useful tools for reducing numbers of drug-related incidents, monitoring new substances or patterns of use, and providing information and assessment to drug users. In Spain, the non-governmental organisation Energy Control has been offering its drug-checking service since 1999 as part of an integrated harm reduction service for recreational drug users. Recreational users, who do not usually seek help or advice from substance abuse organisations, can test their drugs at checking points (in clubs, raves, etc.) or in Energy Control's offices in Spain. This service is supported and financed by the Spanish Government Delegation to the National Plan on Drugs and the regional authorities. It is part of the EU Early Warning System operated by the EMCDDA and Europol. Between 2010 and 2013, a total of 8 348 samples were analysed.

Some sample questions from an online health service for deep web drug users

CASE 1: Silk Road original forum, private message, 15 September 2013

After several years of using injected and smoked daily heroin I decided to quit this spring. I live in an Eastern Europe country where detoxification programs are unavailable. Doctors do not pay attention to heroin users and see them as scum, vicious people and not as ill persons. So I bought some methadone on Silk Road and read in some online books how to do this.

After several weeks I managed to detox completely methadone. I had read that it is normal to have abstinence symptoms during weeks, but it is two months since I finished and I have pain in all my body, changes of mood, sometimes diarrhea. This has not been improving and it is getting worse. In the last two weeks pain is extreme in the night and fever and sweating are extreme. Even I have some swollen nodes down my armpits and neck.

I have gone to the hospital but they discharged me even without doing tests and saying that this was abstinence from heroin (they didn't know that I had used methadone and I didn't say, but in fact I did not have the time to explain ...). I don't like to take more opiates but I can't continue with this pain. I am thinking about taking methadone again, maybe 5–10 mg/daily. Will this be enough to quit these symptoms? Maybe oxycodone or codeine are better options? Thank you in advance.

CASE 2: Silk Road original forum, 14 April 2013

Hey doctor thanks so much for offering your advice! I have type 1 diabetes and I am wondering if there is any information connected to MDMA and its effect on blood sugar? I have never done MDMA but am interested in exploring it. Would I have enough control over myself to realize 'I need to test' or should a trip sitter be there to remind me? Secondly, I have tripped in the past on LSD and mushrooms but that was before my diagnosis ... now that I know I have to monitor my sugar levels to avoid issues I'm afraid I might become afraid or paranoid of my glucometer or my insulin injections under the influence ... any recommendations on how to deal with this?

CASE 3: Silk Road 2.0 forum, 3 January 2014

I have a question about amphetamine usage.

I am in the age bracket of 20–40 and in good health. I use pure amphetamine between 15–70mg, depending on what I am using it for.

Is 70mg of pure amphetamine safe to use in one go? I have low tolerance and I do not go on 'binges.' Sometimes I may have a small top up, but I never go for more than 12–16 hours at a time.

Also, how frequently can I use it without causing harm to myself? I don't normally use it more than once a fortnight, but sometimes I do and I was wondering if it is damaging to use it weekly, or even more than that? Thanks for your time and effort.

CASE 4: Evolution forum, 12 December 2014

When taking NBomes my girlfriend gets red splotches on her face, legs, neck, back, an stomach (vasoconstriction.) It usually happens toward the end of the trip and gets worse when we stay up and trip all night. Usually redosing once. The tabs are no more than 1200ug each. Is there a reason this happens to her and not me? Is there any way to help with this? I know it is not life threatening unless it gets really bad and she gets stuck in her pants or something. (...) But for real. She is also anemic, does this have anything to do with it? Now that I think about it, it has happened with MDMA, and it happened on M1 as well I think (which was sent to me as MDMA.)

At the end of 2012 and during 2013, the Energy Control team was aware of the growing popularity of DWMs through information provided by recreational drug users. An exploratory search of the available markets at that time (Silk Road, Black Market Reloaded and Sheep) prompted the development of the IDTS provided by Energy Control and focusing on DWMs.

During the first quarter of 2014, a specific protocol with objectives, procedures, methods and techniques was elaborated using TEDI (Transnational European Drug Information: TEDI, 2014) guidelines as a reference. All samples were analysed by gas chromatography–mass spectrometry. The fee for a simple analysis was EUR 50 (to be paid in bitcoins). All funds raised were put back into running the project.

A one-year pilot project started in April 2014; drug users who purchase drugs in DWMs were the target population. Several threads in the main DWM forums

were opened offering general information about the IDTS with links to a specific IDTS page on Energy Control's website ([12]). An email address for users to contact the service for detailed information about the process was made available. After submitting samples for analysis, users receive a detailed report with drug test results and specific and individualised harm reduction information. Users were encouraged to engage with Energy Control experts by emails or in DWM forums in order to resolve their questions.

It is worth mentioning that this service is aimed at end-users and that IDTS does not accept samples from vendors. During the whole process, the service emphasises that a test result is representative of the analysed sample only and cannot be considered a quality control for any product or vendor. The use of the test results in DWMs as a 'guarantee of quality' for products or vendors is forbidden. Both DWMs and DWM forums are periodically monitored to check that test results have not been used in this way, but so far no instances of this have been found.

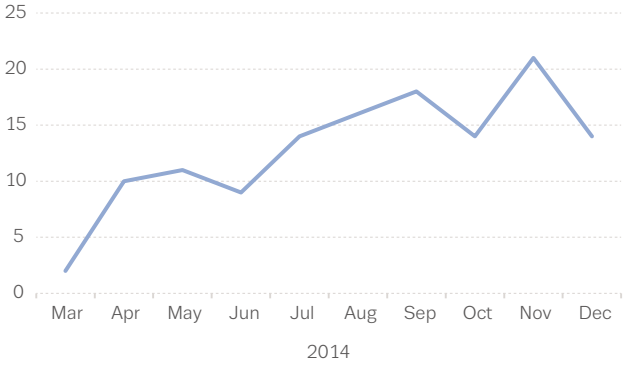
Between April and December 2014, a total of 342 users contacted IDTS asking for information about submitting samples for analysis. A total of 129 samples were analysed over this period, as shown in Figure 7.2.

Users are asked about the type of substance they believe they have purchased. In 120 of 129 samples (93 %), the main result of the analysis was consistent with the information provided by the user. In the remaining 9, the sample contained another drug, a mixture of substances was detected or it was not possible to determine the composition of the sample with the analytical techniques employed. The main results of the drug testing are shown in Table 7.2.

Cocaine was the substance most frequently submitted for analysis. Purity levels were high, although more than

FIGURE 7.2

Samples submitted for analysis by the Energy Control International Drug Testing Service (March–December 2014)



50 % of samples were adulterated. Levamisole was the adulterant most frequently detected, in 43 % (23 out of 54) of samples. Other adulterants detected in cocaine samples were phenacetin in 9 % (5 out of 54), caffeine (1 sample) and lidocaine (1 sample). MDMA samples (in both pill and crystallised forms) showed high levels of purity, and no adulterants or other active ingredients were detected.

Other samples analysed were MDA and methamphetamine (n = 3), 2C-E, alprazolam, mephedrone, 2C-B, butyrfentanyl, synthetic cannabinoids (n = 2), clonazepam, DOB, DOET, DOM, DON, DXM, kratom, mescaline, methylone, midazolam, modafinil and pentobarbital (n = 1).

Results for MDMA pills, showing very high dosages of MDMA that can lead to significant adverse or toxic effects, are similar to those reported by other harm reduction groups offering drug testing programmes (TEDI, 2014). The high frequency of non-adulterated cocaine samples is also notable, although levamisole contamination seems to be a widespread problem, as reported in the rest of the global drug market.

TABLE 7.2

Test results for samples analysed by the Energy Control International Drug Testing Service ([1])

Sample	*n*	Only main compound detected	Purity (m ± SD)	Range
Cocaine	54	48.1 % (26/54)	70.3 ± 19.9 %	5–99 %
MDMA (crystal)	9	100 % (9/9)	91.1 ± 8.0 %	78–99 %
MDMA (pills)	8	100 % (8/8)	142.1 ± 40.2 mg	94–188 mg
Amphetamine (speed)	8	37.5 % (3/8)	51.6 ± 34.6 %	10–98 %
LSD	8	100 % (8/8)	129.7 ± 12.1 µg	107–140 µg
Cannabis resin	5	100 % (5/5)	THC: 16.5 ± 7.5 % CBD: 3.4 ± 1.5 %	THC: 9.1–16.4 % CBD: 1.6–5.3 %
Ketamine	5	40 % (2/5)	71.3 ± 38.4%	27–95 %

([1]) Samples analysed between April and December 2014. Categories with $n < 5$ samples not included.

([12]) http://energycontrol.org/noticias/528-international.html

Another interesting aspect is the low frequency of 'legal highs' in samples submitted for analysis. Although these substances are widely offered in DWMs, demand for and sales of these drugs are limited (Caudevilla, 2014). It is possible that users of 'legal highs' choose to buy them outside DWMs, owing to their easy availability via the surface web. An alternative explanation is that, in the free-market conditions provided by DWMs, users prefer 'established' drugs to substitutes.

The data from IDTS support the hypothesis that substance purity is much higher in DWMs than in the global illicit drug markets. However, results from IDTS are not necessarily representative of the market as a whole and there are methodological biases derived from sample selection.

Conclusion

It seems likely that DWMs will continue to exist in the future and that their importance will probably increase. At the time of writing, there are at least 10 fully operative active markets with similar characteristics to Silk Road. DWMs are developing, and are now available using software other than Tor, such as I2P, or as open decentralised markets, such as OpenBazaar. DWMs seem to be a rapidly evolving, complex phenomenon with the potential to bring about major changes in drug markets. This new reality requires harm reduction strategies to be adapted if they are to successfully meet their objectives.

References

Aldridge, J. and Décary-Hétu, D. (2014), 'Not an "eBay for drugs": the cryptomarket "Silk Road" as a paradigm shifting criminal innovation'. Available at: http://ssrn.com/abstract=2436643 or http://dx.doi.org/10.2139/ssrn.2436643

Andrews, G., Cuijpers, P., Craske, M. G., McEvoy, P. and Titov, N. (2010), 'Computer therapy for the anxiety and depressive disorders is effective, acceptable and practical health care: a meta-analysis,' *PLoS One*, doi: 10.1371/journal.pone.0013196

Caudevilla, F. (2014), 'The importance of NPS in online drug markets: data from Silk Road 2.0', *III International Conference on Novel Psychoactive Substances (NPS)*, Rome, 16/5/2014. Available at: http://es.slideshare.net/fernandocaudevilla/the-importance-of-new-psychoactive-34803762 (accessed on 3/12/2015).

Caudevilla, F., Ventura, M., Indave Ruiz, B. I. and Fornís, I. (2013), 'Presence and composition of cathinone derivatives in drug taken from a drug test service in Spain (2010–2012)', *Human Psychopharmacology: Clinical and Experimental*, pp. 341–344.

Caudevilla-Gálligo, F., Riba, J., Ventura, M., et al. (2014), '4-Bromo-2,5-dimethoxyphenethylamine (2C-B): presence in the recreational drug market in Spain, pattern of use and subjective effects', *Journal of Psychopharmacology* 26, pp. 1026–1035. Published online before print 9/1/2012, doi: 10.1177/0269881111431752

Civljak, M., Stead, L. F., Hartmann-Boyce, J., Sheikh, A. and Car, J. (2013), 'Internet-based interventions for smoking cessation', *Cochrane Database of Systematic Reviews*, doi: 10.1002/14651858.CD007078.pub4

Fornís Espinosa, I., Vidal Giné, C., Caudevilla Gálligo, F. and Ventura Vilamala, M. (2013), 'Nuevas drogas de síntesis en España: *legal highs* (2010–2012)', *Medicina Clínica,* 140, pp. 189–190.

González, D., Ventura, M., Caudevilla, F., Torrens, M. and Farre, M. (2013), 'Consumption of new psychoactive substances in a Spanish sample of research chemical users', *Human Psychopharmacology* 28, pp. 332–340.

Johnson, L. A., Johnson, R. L. and Portier, R. B. (2013), 'Current "legal highs" ', *Journal of Emergency Medicine* 44, pp. 1108–1115.

Kjellgren, A.I., Henningsson, H. and Soussan, C. (2013), 'Fascination and social togetherness: discussions about spice smoking on a Swedish Internet forum', *Substance Abuse* 1, pp. 191–198.

Lefèvre, F. and Simioni, A. M. (1999), 'Marijuana, health, disease, and freedom: analysis of an Internet forum', *Cadernos de Saúde Pública* 2, pp. 161–168.

Månsson, J. (2014), 'A dawning demand for a new cannabis policy: a study of Swedish online drug discussions', *International Journal of Drug Policy* 25, pp. 673–681.

Ormsby, E. (2014), 'The Doctor', in *Silk Road*, Macmillan Australia, pp. 183–191.

Schulz, A., Stolz, T. and Berger, T. (2014), 'Internet-based individually versus group guided self-help treatment for social anxiety disorder: protocol of a randomized controlled trial', *BMC Psychiatry* 14, p. 115.

TEDI (Transnational European Drug Information) (2014), *Fourth TEDI trend report*, http://www.tediproject.org/uploads/trend_reports_file_1388103418.pdf

Van Hout, M. C. and Bingham, T. (2013), '"Silk Road", the virtual drug marketplace: a single case study of user experiences', *International Journal of Drug Policy* 24, pp. 385–391.

8

CHAPTER 8

The drug trade on the deep web: a law enforcement perspective

Joost van Slobbe

Introduction

Cybercrime has been an issue for law enforcement services in Europe since the early 1970s. Traditionally, a distinction has been made between cybercrime in a broad sense (computer-assisted crime) and cybercrime in a narrower sense (computer-focused crime) (Furnell, 2002). The first category includes crimes in which computers are used in the criminal process: fraud, theft or threats over the internet, for example, but also spying, or distributing child pornography. The second category, cybercrime in the narrow sense, comprises crimes such as distributed denial-of-service (DDoS) attacks or hacking, in which the computer or software itself is targeted.

The category of cybercrime in a broad sense also includes drug trafficking on cryptomarkets. There is considerable variation in the extent to which law enforcement services in Europe perceive the necessity of tackling the drug trade on the deep web. The question of how best to combat this phenomenon has not been discussed extensively at international events.

This chapter compares the cryptomarket drug trade with the conventional drug trade, describes how the various law enforcement services are combating the drug trade and assesses the effectiveness of their approach. Finally, it indicates on the basis of these findings how the approach to the drug trade on the dark web might look in the future.

The drug problem in Europe

From a law enforcement perspective, Europe's drug problem can be characterised as the trafficking and use of cocaine, opioids (e.g. heroin), cannabis, and synthetic drugs and new psychoactive substances. Europe is a major destination for controlled substances and also plays a more limited role as a transit point for drugs en route to other regions. In addition, Europe is also a producing region for cannabis and synthetic drugs. Whereas virtually all the cannabis produced in Europe is intended for local consumption, synthetic drugs (including new psychoactive substances) are also manufactured for export to other regions (EMCDDA, 2014).

In Europe, the law enforcement approach to drug-related problems has traditionally focused on large-scale trading by organised criminal groups operating at the international level, on the one hand, and on street dealing that causes public nuisance and health risks, on the other. In most national drugs legislation in the European Union, the emphasis is on the difference between offences related to possession of drugs for personal use and those related to the production and trafficking of drugs.

The trade in drugs over the dark net through cryptomarkets started in 2009 with a handful of websites that operated quietly, such as The Drug Store and Farmer's Market (Heintz, 2012). Their successors, such as Silk Road, were less discreet and seemed not to regard the risk of intervention by the authorities as a serious threat. Today, the turnover of the internet drug trade is considerable. It has been estimated that Dutch drug traders alone have an annual turnover of almost EUR 30 million from cryptomarkets (Kooistra, 2014). It is not surprising then, that the authorities, particularly in Europe, the United States and Australia, feel the need to intervene.

Similarities and differences between actual and digital marketplaces

The business of drug trading can be subdivided into the component processes of production, wholesale trade, transport, intermediary trade and retail trade. In

order to serve as a hub, or 'governal node', within this process, an organisation must have the following four elements at its disposal: mentalities, technologies, resources and institutions (Burris et al., 2005). This applies to both conventional criminal organisations and players in the cryptomarkets, although they are very different in nature. Where the conventional organisations are characterised by collective attitudes and predisposition, the cryptomarkets often pride themselves on organisational charters of an idealistic bent, which even allude to universal human rights and libertarian values. The court proceedings against Ross Ulbricht, founder of Silk Road, show a rather less attractive picture. Ulbricht stands accused of accruing the sum of USD 60 million from drug trading through Silk Road and of subsequently laundering this money. He is also alleged to have offered a contract killer USD 80 000 to deal with one of his enemies. However, the supposed contract killer turned out to be an undercover officer. Unexpectedly, at the trial in January 2015, Ulbricht tried to palm off responsibility for managing Silk Road onto Mark Karpless, CEO of Mt Gox, the company that owned 70 % of the bitcoin trade in 2014. In a separate court case, Karpless is accused of 'disappearing' USD 450 million worth of bitcoins. Thus, the trade on cryptomarkets involves not only the illicit drug trade itself, but also other criminal behaviour characteristic of the conventional drug trade.

The rise of internet sales, and more specifically cryptomarkets, has entailed only limited changes to the criminal business process. The production end of the process — whether of cocaine in South America, opiates in countries such as Afghanistan, or MDMA and cannabis in Western Europe — has, as yet, not really been affected by the introduction of cryptomarkets to the chain. If a European organised criminal group wishes to order a large consignment of heroin or cocaine in the source country, there is face-to-face contact between mandated representatives of the supplying and receiving criminal organisations. The basis for this trade is trust and creditworthiness, coupled with a ruthless system of sanctions if the purchasing party does not keep its side of the agreement. Numerous gangland killings occur in Europe as a result of drug transports that have gone wrong. Owing to these mores and the enormous financial interests that hinge on the success of each transaction, it is not likely that the primary negotiations will take place over the deep web. What we do see increasingly in European police investigations into criminal organisations, including those involved in the drug trade, is that communication between and within the organisations is carried out using encrypted internet facilities.

The transportation of the drugs, too, has seen few changes at the level of wholesale consignments. Shipping containers, air freight and couriers all remain popular methods of transporting drugs. The customs authorities in Western Europe and Australia do, however, estimate from the numbers of drug shipments they have intercepted in parcels that the use of parcel post for transporting drugs has increased sharply as a result of sales through cryptomarkets.

At the level of brokering, cryptomarkets increasingly seem to be playing a role. This can be deduced from the fact that many drugs vendors actively draw attention to the possibility of buying large quantities from cryptomarkets. Examples are also known from criminal investigations in the Netherlands and other countries, of buyers first purchasing small quantities of drugs and then, once a degree of trust has been established between the vendor and the purchaser, proceeding to purchase a large consignment for trade. In one of these cases, the purchaser drove from Scandinavia to the Netherlands to collect the drugs from the vendor by car.

The interaction between the retail trader and the purchaser or user does differ significantly from conventional street dealing. In many cases, there is no longer any face-to-face contact when the user receives the drugs. The retailer receives an order over the dark web and then sends off the drugs by post. His or her activities mainly consist in checking the orders, packaging the goods and delivering the parcel to a carrier. The buyer receives the parcel at home or has it delivered to a different address and collects it there. Payment generally takes place in bitcoins. As yet, criminal investigations have seldom, if ever, encountered the use of another cryptocurrency. Incidentally, there has also been a case of a buyer from the United States ordering a whole series of synthetic drug consignments from a supplier in the Netherlands over the dark web and paying with cash. The money was posted in envelopes to various addresses in the Netherlands and then collected by the supplier. Using a cryptocurrency is an obvious way to make payments in the drug trade over the dark web, but it is not a prerequisite.

One important advantage of buying and selling drugs via a cryptomarket is that the buyer and seller remain anonymous and thus do not have to worry about violence, extortion or robbery. Whereas the conventional drug trade is built on power and violent force, in the anonymous world of the deep web this is not an issue. However, there is another side to this anonymity: potential newcomers to these markets may feel extremely uncomfortable about not knowing who they are dealing with and who they are entrusting their

bitcoins or drugs to. From this point of view, street dealing, in which drugs and money change hands simultaneously, is easier to keep track of. A related issue is that if a buyer or seller is duped by fraud or theft on a cryptomarket, it is virtually impossible to call the perpetrator to account. Another disadvantage of anonymity is that there is always a reasonable chance that a buyer is actually selling to an undercover police officer.

Differences in the key players

If we are to devise an effective European law enforcement strategy in this area, it is important to thoroughly understand the workings of the criminal business process. As stated above, virtual marketplaces where buyers and vendors meet and do business together are an established forum, alongside the regular marketplaces that street dealers have been using for decades. In order to develop an effective strategy that will enable us to influence the sale of drugs, and the safety and security problems generated by the drug trade, it is important to know the profiles of the key players and what motivates them.

Let us examine the most important players within cryptomarkets.

The administrator is the manager of the website and determines what takes place on the site. He or she is responsible for authorising accounts, making new product categories, and permitting or forbidding the sale of certain products. One of the administrator's most important tasks is to ensure effective shielding. The administrator also fulfils the role of treasurer with regard to cryptocurrency. If approached by the police, the administrator is likely to take the stance that he or she facilitates the marketplace but is not responsible for the trade that takes place.

The moderator operates under the administrator. He or she has limited access to the website infrastructure and user information. The moderator's most important tasks are to answer questions from users and to scan for fraudulent deals.

The vendor registers with a website to be permitted to sell illegal goods through it. For this purpose, the vendor designs a seller page to offer the goods to prospective buyers. The vendor pays the administrator a fee of a few hundred euros for this service. In addition, the vendor pays the administrator a small percentage commission on each sale.

The buyer or consumer who buys goods on a cryptomarket can browse various seller pages to compare products. The buyer sets up a buyer account, free of charge, from which cryptocurrency can be transferred. After the purchase transaction, the buyer can indicate on the site whether the product and/or service met expectations.

Other, less prominent, players in the field of cryptomarkets include *internet service providers*, which host cryptomarkets, and *web design companies*, which may be called on to design professional cryptomarket sites for vendors. There also seems to be a *deep web marketing organisation* that offers expert marketing and advertising services for vendors (DeepDotWeb, 2014).

Payment can take two forms. The buyer can transfer the money owed directly to the vendor or can transfer it to the administrator (in escrow), who then releases the sum to the vendor once authorised by the buyer (after he or she has received the drugs). In the case of a large website, the sums the administrator holds in escrow can mount up. As in the traditional criminal world, here too it is a relatively common occurrence for third parties to steal the money (by hacking, for example) or for administrators to make off with the cryptocurrency themselves.

Some users of cryptomarkets view themselves as defending civil liberties and opposing government meddling. The terms 'crypto-libertarian' and 'crypto-anarchist' are used in this context (Curran and Gibson, 2013). These users see themselves as upstanding, law-abiding citizens who do not agree with the criminalisation of drug use and believe it should be a matter of individual choice. For this reason, they find it legitimate to use crypto-techniques to evade the 'meddlesome' authorities. The players on the cryptomarket go to great lengths to distinguish themselves from the conventional drug trade. In their communications, they emphasise their strong norms and values to justify their actions. In this vein, several vendors espouse harm reduction programmes and fair trade principles. However, the big money involved is a significant pull factor, and this market, like all trade markets, is attractive for criminals with less noble objectives.

One reason cryptomarkets can operate so 'successfully' is that they employ strict self-regulation. Both the cryptomarket administrators and moderators ensure that buyers and sellers comply with the rules imposed on them. This is reinforced by the application of sanctions, such as withdrawal of a user account.

One important question that occupies police and judicial authorities is whether the individuals who sell on the cryptomarket fit the same profile as that of street dealers. Have street dealers switched to the cryptomarket, and, if so, what advantages did they expect from this switch? Or are drug sellers on the deep web completely different from street dealers? Do they form a new group on the criminal market? What are the characteristics of these people, and what are their motives?

We can ask similar questions about the buyers. Did the people who are now buying drugs over the deep web previously buy drugs in the traditional way, or did they start buying drugs because of the ease of buying them over the deep web, which entails fewer risks? Is the profile of these buyers similar to the profile of drugs buyers in the traditional market? When it comes to combating this phenomenon, and particularly in determining priorities, it is relevant to know if there are differences between these two types of buyers from the point of view of problem drug use. European law enforcement has little expertise in profiling of this kind. It will be necessary to carry out further criminological and other research in this area to obtain a more thorough understanding of the phenomenon.

Strategy thus far in combating drug trading over the deep web

From an international perspective, until now law enforcement has focused its efforts in combating the drug trade over the deep web on dismantling websites that offer drugs for sale and on apprehending buyers with a higher than average turnover. The underlying assumption is that the website is indispensable as a sales platform and is difficult to replace because of the shielding requirements. The thinking is also that if the authorities take down a website, this may remove the anonymity of buyers and sellers, and thus make the marketplace less attractive to use. Although parcels containing drugs are intercepted and confiscated daily during customs checks, criminal prosecution of sellers has as yet been extremely limited in Europe.

The first website to sell drugs on a large scale was Silk Road. This online black market began its operations in February 2011. In March 2013, *The Guardian* counted 10 000 articles for sale on Silk Road, of which an estimated 70 % were drugs. In October 2013, Silk Road was 'defaced' (confiscated and stamped with a law enforcement notice), and Ross William Ulbricht was arrested by the FBI as the suspected owner of the website. During Ulbricht's trial in January 2015, the US prosecutor estimated the total turnover of Silk Road since it was set up at 9.5 million bitcoins (the equivalent of approximately EUR 1 billion). A month after Silk Road was shut down, Silk Road 2.0 was launched.

In February 2014, the Dutch police arrested five Dutch citizens after an undercover operation, Operation Commodore. Undercover agents managed to establish online contact with the main suspect behind Ruud.nl and subsequently arranged a meeting with him. The police took down the website Black Market Reloaded and put another website, Utopia, offline after just a week. The German police seized servers in Bochum and Düsseldorf. In the course of this operation, it emerged that, in addition to his online contacts, the main suspect also approached potential clients in the traditional manner. In Operation Commodore, there was little sign of the strict distinction between players on the cryptomarkets and drugs dealers in the 'regular' drug trade.

On 6 November 2014, Europol reported that an internationally coordinated police operation had taken place, Operation Onymous, in which law enforcement agencies all over the world worked together under the leadership of the FBI. In Europe, the network that existed as a result of Project ITOM (Illegal Trade on Online Marketplaces) (Netherlands Public Prosecution Service, 2014) was used to organise this operation. Hundreds of web domains were seized, according to Europol. Seventeen arrests were made, in seventeen countries, and more than a dozen black market websites were taken down, including Silk Road 2.0, Cloud 9, Hydra, Pandora, Blue Sky and Black Market. A total of 414 onion domains were seized.

The most important objective of these interventions, which focused on the largest cryptomarkets, was to put specific marketplaces out of action for good and to arrest and prosecute those responsible for drug trading. As in the fight against conventional drug trafficking, in tackling cryptomarkets the police attempt to confiscate the greatest possible proportion of assets obtained in the drug trade. In the case of Silk Road, they confiscated 26 000 bitcoins, worth EUR 2.5 million, and in Operation Commodore, 900 bitcoins, worth EUR 400 000. Operation Onymous included takedowns of money laundering websites such as Cash Machine, Cash Flow, Golden Nugget and Fast Cash. The police also confiscated USD 1 million in bitcoin, and USD 250 000 in cash.

Intended effects and actual effects of law enforcement activities

The interventions described above were intended to break through the aura of anonymity and the associated sense of untouchability. In the case of illegal proceeds, the aim of the interventions was to confiscate assets obtained in the drug trade. With regard to cryptocurrency, the aim was to seize large quantities of bitcoins, thus making it less attractive to use cryptocurrency for purchases on cryptomarkets.

It was difficult for law enforcement to foresee what effects these interventions would have. In the conventional drug trade, the arrest of a street dealer usually results in a competitor moving in to take his place. If the arrest was combined with closing the café the dealer operated out of, for example, the arrest might have longer-lasting effects. If enforcement was stepped up in the area and prevention programmes implemented, then a long-term effect might be achieved. However, predicting how those involved would respond to intervention in the cryptomarkets was trickier. Would the current actors lose faith in this system to such an extent that cryptomarket activity would decline in favour of street dealing? The lack of any previous experience with this new system, combined with the absence of solid sociological and social science data on the actors involved, makes the effect difficult to gauge.

After the fall of Silk Road, numerous websites tried to take over its market share, but many of these were short-lived. Problems with site security and instances of fraud among key players meant that the online market was much less stable than in the Silk Road period. It is now clear what choices buyers and sellers have when a cryptomarket site is brought down by the authorities:

1. they move to another, existing site on an individual basis;

2. the group of buyers and sellers set up a new cryptomarket as soon as possible, where the same 'community', or group of users, can continue to trade; or

3. they cease buying and selling on cryptomarkets.

The combined effects of mutual dependence, the risks involved in switching to an unknown cryptomarket, and the pressing need to buy drugs make option 2 the most appealing.

It is no longer enough for vendors to deposit a sum of money with the site administrator. The newer sites require potential new vendors to be introduced by someone the administrator already knows in order to be admitted. The prospective seller's history on the deep web is also considered.

Administrators have learned from the law enforcement operations that brought down Silk Road and Silk Road 2.0. Far from the impenetrable fortress it was once thought to be, the Tor Network has proved vulnerable. For this reason, investments in security measures to combat outside intervention have gone up (Van Buskirk et al., 2014).

The intended effect of removing a large proportion of the cryptomarkets available was not achieved, because a whole range of new drug supply sites popped up within no time. Even after Operation Onymous, major websites such as Agora, Evolution and Andromeda continued their activities. This does not mean, however, that the operations had no effect. Trust in the cryptomarkets took a hit, an effect that was only reinforced by the fact that newcomers to the market are not exactly known for their trustworthiness.

Recommendations for law enforcement

The issue of illicit drugs is multifaceted. At the global or even the European level, the approach to this complex issue varies widely from place to place. There is little disagreement on the need to tackle producers, major dealers and middlemen. The negative effects of their actions have such a strong impact that police crackdowns enjoy broad support. Policy on users is where the big differences are found. Some EU countries consider drug users criminals, while others treat the issue as a health problem. In the latter case, prevention, treatment and damage control take priority over tracking users down. Law enforcement is primarily charged with the repressive part of the approach.

Now that cryptomarkets are becoming popular forums for the drug trade, the question arises of whether or not they will edge out the brokers and street dealers. From a business perspective, a direct link between producers and users might mean more money and less risk for those involved.

Criminal groups that reap major profits from their position as brokers are accustomed to using violence to

defend or expand their share of the market. The risk is that these groups will not accept 'their' livelihood being taken away. Ongoing investigations show that cryptomarket sales are not limited to quantities for personal use. One vendor, HollandBest, offers special prices for bulk orders of more than 5 000 ecstasy pills. Another vendor, Dutchmarket, states that it is 'open to negotiations' on orders involving more than 500 g of cannabis, or over 1 000 ecstasy pills ([1]).

Proponents of cryptomarkets for the drug trade claim that their growth has nothing but advantages. The buyer or user faces lower risks because the quality of drugs can be better assessed through the system of feedback. The sites provide data on each vendor, including the number of transactions made, product quality and the level of service provided. Vendors cannot block or edit comments posted by buyers. The fact that vendors strongly encourage customers to voice any complaints directly shows that they do indeed fear the impact that negative comments in the feedback system can have on their business. The feedback system is not immune to manipulation, however. Vendors cannot change feedback posted by their buyers, but competitors are free to post negative feedback. Furthermore, vendors themselves can post sham feedback on deals that never took place to boost their creditworthiness score.

Another frequently cited advantage of cryptomarket drug deals over conventional drug dealing involves the absence of the violence and public nuisance so endemic to street dealing. A third common argument made by proponents is that the drug trade on cryptomarkets does not involve physical confrontations. This may be true, but the illicit drug trade has considerable negative effects. Morris (2013) indicates that the proliferation of cryptomarkets is unlikely to reduce the most serious forms of systemic drug crime, such as political corruption and violence.

From a perspective of feasibility and broad-based public support, the following approach is recommended for law enforcement in the coming years:

- Continue the current work of combating the main cryptomarkets, focusing on administrators and moderators.
- Prosecute the main vendors who, judging from the quantities ordered, operate as middlemen on cryptomarkets.
- Seize cryptocurrency wherever possible and dismantle cryptocurrency facilities that make it possible to make or receive payments for drugs.
- Confiscate goods paid for with the proceeds of crime.
- Invest in big data techniques, in order to link vendor nicknames and internet activity with certain IP addresses.
- Convince internet service providers that unknowingly host cryptomarkets to stop, by entering into public–private partnerships with ISPs. Tackle conscious facilitators (such as bulletproof hosts) by means of permit regulations or criminal prosecution, to ensure that providing this service is no longer profitable.
- Professionalise checks on parcel post to greatly reduce the odds of successfully shipping drugs by mail, a move that would hit both the conventional and the internet drug trade.
- Develop a strategy to diminish the trust of vendors and buyers in the reliability of cryptomarkets.

In selecting a law enforcement strategy, anticipating cryptomarket developments is key. A new challenge will be the decentralised marketplaces. In a decentralised set-up, no one owns the marketplace itself or is responsible for it; instead, it is a platform that individual vendors can use free of charge.

For libertarians with an idealised view of the cryptomarket drug trade, one can draw a parallel with cannabis in the Netherlands. An extremely liberal policy towards cannabis use led to a great number of 'coffeeshops' springing up in the Netherlands, where, under certain government-determined conditions, cannabis could be sold in small quantities for personal use. These days, the vast majority of cannabis production has been taken over by organised crime. The relaxed atmosphere and 1960s sentiment has made way for contract killings, extortion, and human trafficking and slave labour associated with cannabis production. It is estimated that at least 85 % of the cannabis grown in the Netherlands is exported. Criminal groups that were once active in the ecstasy trade have moved into cannabis, have made millions in profits and consider themselves untouchable. Outlaw motorcycle gangs such as the Hells Angels have also managed to get their hands on a sizeable proportion of the market. Their behaviour undermines law-abiding society and sets a bad example for the new generation. The innocence of the late 20th century has vanished.

([1]) http://www.volskrant.nl/binnenland/hoe-online-coffeeshops-een-milijoenenomzet-draaien~a3757208

As long as the production of and trade in drugs continue to be considered criminal acts in most of the Western world, and as long as the proceeds remain sufficiently high in relation to production costs to secure immense profits, organised crime will continue to be involved in this market. The percentage of the total drug trade represented by cryptomarket trade is as yet too limited to affect the profits of the larger organised criminal groups. If cryptomarket turnover were to increase substantially, then organised crime could be expected to annex the marketplaces. The idea that far-reaching security techniques would be able to prevent the influence of organised crime strikes may be naive. Given that criminal groups already use private servers and protected networks for communicating within the group, it is not inconceivable that they might move into managing their own cryptomarkets. Those in control of production can — by waging a price war while manipulating the payment system and competitors' feedback — squeeze other suppliers out of cryptomarkets. If the number of cryptomarket suppliers remains at current levels, or if the popularity of this form of drug trade declines, then the likelihood is that mafia-type criminal organisations will not consider it worth their while to intervene. From a law enforcement perspective, this is the most important argument for combating the sale of drugs on cryptomarkets. That way, we could put a stop to online criminal refuges, as well as all the other negative fallout from conventional drug crime in the virtual domain, with its concomitant effects on upstanding virtual citizens.

References

Burris, S., Drahos, P. and Shearing, C. (2005), 'Nodal governance', *Australian Journal of Legal Philosophy* 30, p. 30.

Curran, G. and Gibson, M. (2013), 'WikiLeaks, anarchism and technologies of dissent', *Antipode* 45(2), pp. 294–314.

DeepDotWeb (2014), 'Updated: list of hidden marketplaces (Tor & I2P)', https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/ (retrieved 30/5/2014).

EMCDDA (2014), *European Drug Report 2014: trends and developments*, European Monitoring Centre for Drugs and Drug Addiction, Lisbon.

Furnell, S. (2002), *Cybercrime: vandalizing the information society*, Addison-Wesley, London.

Heintz, L. (2012), 'Here's the indictment that blew the lid on the eBay of drug trafficking this week', *Motherboard* 20/4/2012. Available at: http://motherboard.vice.com/blog/here-s-the-indictment-that-blew-the-lid-on-the-amazon-of-drug-trafficking-this-week

Kooistra, S. (2014), 'Hoe Online coffeeshops een miljoenenomzet draaien', in *De Volkskrant*, 7 September edition. Available at htttp://www.volkskrant.nl

Morris, S. D. (2013), 'The impact of drug-related violence on corruption in Mexico', *The Latin Americanist* 57(1), pp. 43–64.

Netherlands Public Prosecution Service (2014), *Undercover investigation into illegal marketplaces on the internet*, Rotterdam.

Van Buskirk, J., Roxburgh, A., Farrell, M. and Burns, L. (2014), 'The closure of the Silk Road: what has this meant for online drug trading?', *Addiction* 109, pp. 517–518.

9

CHAPTER 9

How the use of the internet is affecting drug trafficking practices

Anita Lavorgna

Introduction

There is a consensus that the internet has expanded possibilities for drug supply and trafficking. The aim of this chapter is to present, from a criminological perspective, how the use of the internet has affected the different stages of drug trafficking (particularly the distribution stage) in relation to different types of recreational drugs. In particular, it will examine how the use of the internet is affecting the modus operandi of suppliers and their interactions with criminal peers and clients in numerous ways. Research indicates that drug markets have become — even if to a different extent — hybrid markets that combine the traditional social and economic opportunity structures with the new opportunities provided by the internet. Furthermore, not only has the internet opened the way for new criminal actors, but it has also reconfigured relations among suppliers, intermediaries and buyers.

Going cyber? The state of the art

The commercialisation of the internet, like any other technological change, modifies the environment in which crime operates, the opportunity structures available to criminals and the dynamics of criminal activities. An increasing number of investigative reports underline that the internet is a tool exploited by criminals in transnational trafficking flows, first and foremost in drug trafficking. Europol's *EU serious and organised crime threat assessment* (Europol, 2013) states that the internet has facilitated interaction between customers and suppliers and enabled the creation of a virtual subculture. Similarly, reports from the EMCDDA (2014) and the United Nations Office on Drugs and Crime (UNODC) (2014) emphasise the growing role of the internet and specifically of the deep web in the supply of drugs. The EMCDDA and Europol (2013) identified several features of online drug markets. In addition to pointing out the existence of various hotspots in the deep web where sellers can benefit from anonymous communication, the report underlines that the internet allows for different methods of payment, including virtual currencies. It also enables buyers to review the quality of drugs, sellers to build an online reputation and newcomers to access information that makes their entrance into the criminal market easier.

The use of the internet as a facilitator for drug supply and trafficking is also receiving increasing attention from the academic community. Over the last 15 years, the literature on internet-facilitated drug trafficking has highlighted the role of the internet as a facilitator of communications in the trafficking process owing to the enhanced possibilities for anonymity. Recent studies underline how suppliers at different levels are using new technologies not only to communicate through encrypted messages (hindering the work of law enforcement agencies), but also to deliver and distribute their products more effectively (Walsh, 2011; Christin, 2012). Researchers have explored vendor accounts in online marketplaces and described the possibilities that the internet offers for operating in a high-profit and relatively secure infrastructure (van Hout and Bingham, 2014). Potential changes to drug distribution networks have also been discussed (Martin, 2014). In a nutshell, in addition to facilitating the drug business, as any other communication tool could, the internet seems to have affected the drug market — as it has other commodity markets — in a deeper way, allowing buyers and sellers to exchange information and products very easily.

Most analyses focus on the use of the internet to reach clients in the deep web, and more and more research is being done on the use of cryptomarkets for trading drugs (Aldridge and Décary-Hétu, 2014; Martin, 2014). Silk Road, a website housed on the Tor Network and taken down by the FBI in 2013, is the most studied online drug marketplace (see, among others, Barratt, 2012; Christin, 2013). Although Silk Road has been described as 'an eBay for drugs' (Barratt, 2012), emphasising its popularity among drug consumers making personal

use-sized purchases, Aldridge and Décary-Hétu (2014) recently found that, although in most cases drugs were sold at prices consistent with purchases for personal use, a meaningful proportion of sales on Silk Road were best characterised as 'business-to-business' and key Silk Road customers were probably retail drug dealers sourcing stock for local street operations (see Chapter 2). Dolliver (2015) started looking at Silk Road 2.0, another online market that was launched soon after the Silk Road takedown (and which has recently also been seized). Specifically, she compared the metrics of Silk Road 2.0 to those of Silk Road to determine if there were signs of the presence of more sophisticated drug trafficking operations in the new marketplace. Findings, however, indicated not only that Silk Road 2.0 was smaller than the original one (with the United States being the number one origin and destination country for drug sales), but also that it was not intended as a drug market only: drug items constituted only 19 % of the total percentage of active items for sale, and, when considering the historical total number of transactions, drugs accounted for only 1 %. However, the growing popularity of other online marketplaces in the deep web (such as Agora, Abraxas and Outlaw to name just a few) suggests that the problem of the exploitation of the deep web for drug trafficking is ongoing and has certainly not been solved by the takedowns of the original Silk Road and Silk Road 2.0. Suffice to say that Silk Road Reloaded was subsequently released and made accessible through the I2P software.

The role of the surface web in drug trafficking and particularly the ways in which the internet is exploited throughout the trafficking chain have been seldom considered. As a consequence, although there is general agreement that online marketplaces for drugs have increasingly been used over recent years and will be used even more in the future, the extent to which the use of the internet is reconfiguring drug trafficking overall is still open to debate.

The internet as a facilitator: identifying criminal opportunities and their impact

In a recent study, the author aimed to gain an increased understanding of how the use of the internet is facilitating drug trafficking and the extent to which it is changing the criminal landscape (Lavorgna, 2014). By systematically analysing investigative cases of drug trafficking in some EU countries and in the United States, it was possible to identify nine major types of criminal opportunity that the internet, and specifically the surface web, provide for drug trafficking: communicative, informational, technical, managerial, organisational, promotional, persuasive, marketing/loyalty-building, and countermeasure opportunities. It was possible to observe how the use of the internet affects all phases of the trafficking chain — namely production (cultivation of plant-based drugs and/or production of chemicals), transit (passage through local and/or international middlemen, criminal networks and local retailers) and distribution (to the end-user) — albeit to different extents.

Among other findings, it was clear that, especially with regard to the transit and distribution stages, the internet offered the possibility of making drug trafficking less risky by enabling several phases of the criminal activity to be managed without interacting with anyone. Before use of the internet became commonplace, for instance, a criminal network had to be sophisticated and organised enough to be able to employ large-scale corruption, particularly in the transit and distribution phases, where dubious operations could be spotted by law-abiding citizens who might alert authorities. Nowadays, by contrast, online booking and online parcel tracking systems provide a safer way for criminals to arrange and track the supply process and to advertise their products. Moreover, given that for drug traders operating online it is easier and less risky to contact potential customers in a wide range of cyber-hotspots (that is, places where interactions among different actors involved in drug trafficking are facilitated) without having to meet them in person, suppliers can take full advantage of the anonymity that the internet provides. In this way, their online reputation is unrelated to their identity in the physical world. Online payment systems and virtual currencies are used by customers to hinder police detection and to avoid direct contact with drug dealers.

Overall, as regards communicative opportunities, internet phone services such as Skype are heavily used to avoid wiretapping. The internet is also used by traffickers to set up counterstrategy measures. Offenders generally seem to be very aware of and cautious about taking risks while operating online. For instance, during recent investigations it emerged that IP addresses were verified by criminals to be sure that the person they were interacting with online was a real potential customer and not, for instance, an undercover law enforcement officer (Lavorgna, 2014, 2015b).

It is worth mentioning the persuasive and marketing/loyalty-building opportunities offered by the internet. As explained by Lusthaus (2012), criminals operating on the

internet have developed a range of mechanisms to create and reinforce trust in their online activities. In the case of drug trafficking, the internet is used to reassure (potential) buyers about the anonymity and the secrecy of the sale, and as a retention tool for both new and old clients. For instance, membership discounts are offered to regular buyers to increase their loyalty, and new potential buyers are targeted by appealing to their sense of belonging to certain social communities online (Lavorgna, 2014, 2015a). Moreover, it should be kept in mind that the peculiarities of cyberspace are likely to have an impact also on users: 'virtuality' is considered to be a crime facilitator, since 'the warning signals that might deter or frighten a young person in the real world are minimized, and the filtering process by which an individual moves into physical contact with a criminal organization disappears' (INCB, 2011, p. 4).

To understand the effects the internet is having on drug trafficking in more detail, however, a distinction between cannabis and new psychoactive substances (new drugs, in pure form or in a preparation, that are not controlled under international drug control treaties but which may pose a public health threat comparable to that posed by controlled drugs), on the one hand, and drugs under international control, on the other, is necessary.

New psychoactive substances: hidden in plain sight

Generally speaking, although nowadays every type of drug can be found online, the internet seems to have boosted the market for new psychoactive substances in particular. For these substances, which have become more pervasive in the last few years than illicit drugs under international control (UNODC, 2013), the internet has become a major distribution point. As shown in Lavorgna (2014), the use of the internet has allowed criminals to arrange most phases of their activity directly from the destination country, from buying substances or chemicals online to selling the final products both in the deep web and in the surface web under the guise of licit products such as plant food and house deodorisers.

A major problem is that, in the case of new psychoactive substances, it is not always easy to draw a clear line between what is legal and what is not, given that some substances may also have a legitimate use, and some may even be legal in certain jurisdictions. In a context where each EU Member State has a different national approach to drug policies and advocates different solutions for tackling drug problems, offenders may exploit legal loopholes, as exemplified in what is probably the oldest investigation, carried out in Italy in 2003, regarding internet-facilitated drug trafficking: various types of synthetic drugs, new psychoactive substances and chemical precursors were ordered online from four Dutch websites and delivered to Italian buyers by ordinary mail. In eight months of investigation, about 1 000 packages were intercepted at Milan post offices, ordered by a total of 235 Italians, many of whom were underage. The Dutch websites were adamant that they did not have responsibility for the legal consequences of their sales in other countries (Polizia di Stato, n.a.).

For new psychoactive substances, the surface web plays a major role. From a simple Google search, several websites and forums can be identified offering information on both offline and online places to buy drugs, prices, how to cultivate plant-based drugs and how to manufacture synthetic drugs. Information about legislation and law enforcement attitudes (for instance, whether or not it is safe to bribe agents and to what extent restrictive legislation is enforced in a certain country) can also be easily found (Lavorgna, 2014). Overall, offenders do not even bother to move to the deep web to advertise their products, as the risk of their being caught remains minimal, given the enormity of the environment to be controlled, and the impression is that law enforcement operations dealing with these types of illicit trade reach only the tip of the iceberg (Lavorgna, 2015b). The need to contact potential clients seems to overcome the need to conceal trafficking activity where the drug trade is in a 'grey area' (as with new psychoactive substances) or is perceived by a relatively large part of the population as not socially reprehensible (as with cannabis).

Different patterns for controlled drugs

Regarding drugs under international control, the internet has not affected the opportunity structure in the initial stages of the trade substantially, probably because producers and drug dealers generally rely on already established opportunity structures for their businesses. Specifically, most drug producers and dealers still rely on their existing networks rather than on the internet to get in contact with local middlemen and retailers. When it comes to the trafficking of controlled drugs, therefore, the internet is used as a facilitator, particularly for communication and in the final phases of the trafficking chain.

Online criminal markets for hard drugs are present particularly in the deep web. When the trade occurs there, drugs are generally delivered via mail services, without physical interaction between buyers and suppliers. In addition, the surface web plays a role, with cyber-hotspots being frequently used as an extension of traditional hotspots: when operating in the open web to reach potential clients, traffickers apparently prefer to avoid using the internet to conclude the deal. For instance, there is evidence that illicit drugs (including cocaine, heroin and ecstasy) and prescription medicines (mostly opioid painkillers) are sometimes advertised under the guise of study aids or painkillers on popular commercial websites. In these cases, the sale is generally finalised offline, usually in public places. In addition to creating new cyber-hotspots, use of the internet for drug trafficking seems to also affect offline hotspots, by moving part of the distribution chain from city centres to suburban areas: clients do not have to travel to purchase drugs, but can easily order them online and have them delivered to their home by a drug courier or by mail (for further details, see Lavorgna, 2014).

Overall, as regards drugs under international control, cases of internet-facilitated trafficking still account for a small minority of drug trafficking cases, and generally criminals still seem to rely on traditional networks of contacts to enter and manage effectively their business. The impact of the massive use of the internet in Western countries seems to have had a major role, especially in relation to how criminals enter into contact with potential clients. Although the increasing role of new technologies in the everyday routines of all the actors involved in drug trafficking should be kept in mind, over-emphasising the cyber component in this criminal domain risks diverting attention from the traditional — but still prevalent — offline features of this complex criminal offence.

Challenging rhetoric

Drug trafficking is generally framed in the 'organised crime' narrative: it is often associated with highly structured criminal organisations such as the Italian 'Ndrangheta, as well as with more flexible and diffuse criminal networks such as Colombian gangs. However, when it comes to internet-facilitated drug trafficking, quite unexpectedly, evidence shows that individuals, couples and very loose networks are becoming key criminal actors thanks to the system of criminal opportunities provided by the internet. In particular, the use of the internet seems to have facilitated the entry into the market of smaller criminal groups that, owing to the possibility of managing almost all the phases of the trafficking activity efficiently from afar, can organise (almost) all stages of drug trafficking on their own, rather than relying on complex criminal networks. Moreover, if we consider how organised crime groups behave in cyberspace, we have to take into consideration that differences between the physical world and cyberspace could prevent criminal organisations that have proven successful in the real world being equally effective online (Lavorgna, 2015b). Indeed, the use of the internet has simplified the trafficking chain by reducing the organisational layers that are necessary: for instance, drugs ordered online are now delivered via mail, eliminating the need to rely on members of the criminal network. This is true especially when looser groups operate in areas where there is not a strong presence of endogenous sophisticated criminal networks already involved in the trafficking business.

At least potentially, in cyberspace criminal behaviour 'cuts across a wide spectrum of society' (Jaishankar, 2009, p. 289); in fact, offenders' ages and skill levels can be very difficult to determine, and most average people could hypothetically join a criminal group or start a criminal career on their own. Moreover, because of the so-called 'online disinhibition effect' (Suler, 2004), people in cyberspace behave with less restraint than in the physical world. It has been hypothesised that there is a risk of 'amateurisation' of drug-related crime, meaning that ordinary people (both users and potential drug chemists) without specific criminal contacts can easily locate drug suppliers (INCB, 2011) and therefore enter the criminal market. Although there is not enough evidence to support this claim, recent research points in this direction. For instance, as regards recent marketplaces such as Silk Road 2.0, Dolliver's analysis (2015) suggests that only a small minority of vendors had connections with more sophisticated criminal groups or upper-level retailers and that the majority were 'opportunistic' vendors. However, it is worth noting that, even when internet-related criminal opportunities allow drug trafficking to become an individual business, this criminal activity is generally carried out by professional offenders, full-timers for whom the trafficking activity is their main source of income (Lavorgna, 2014). The potential to reach a larger customer base via the internet could also precipitate greater involvement of occasional drug dealers, who might become 'professionals'.

Although many internet opportunities are exploited by looser gangs, couples and even individuals in the surface web, where more structured organised crime groups are involved there is greater use of the deep web. Since monitoring of and investigations into the deep web started only very recently, it is difficult to draw clear

conclusions in this regard, but this appears to be at least a preliminary trend deserving more scholarly attention (see, for instance, Martin, 2014).

The need for proactive online policing

As increasing use of the internet has allowed new criminal opportunities for drug suppliers, it has also significantly affected their vulnerabilities, giving law enforcement new tools for monitoring and investigating criminal markets for drugs. However, contemporary law enforcement and regulatory agencies still seem to lack the capacity to significantly control internet-facilitated drug trafficking. Apart from a few notable exceptions of best practices carried out in some countries by certain proactive units, online investigation of trafficking activities is not yet a tool commonly used by law enforcement, with specific protocols still to be developed (Lavorgna, 2014, 2015b). Moreover, existing legal frameworks still do not explicitly address the numerous and substantial procedural problems caused by use of the internet and they often do not offer enough room for manoeuvre or clear directives for law enforcement bodies operating on the internet (for instance, in many countries officers do not have the legal means to operate as online undercover officers, which limits their operative capacities). It is easy to see how these issues hinder investigations while offering a considerable advantage to offenders. It is advisable that the use of online investigations in drug trafficking cases become embedded in the routine practices of law enforcement agencies in all countries and at all levels.

Conclusion

Drug trafficking patterns are constantly changing. Identifying patterns of criminal behaviour and matching them to different cyber-hotspots could have important implications for tackling offenders and potential offenders in the internet age. In this way, it would be possible to manipulate the opportunity structures they exploit, to help law enforcement make the most of its (scarce) resources in monitoring and protecting the internet, and to help consumers make responsible choices when buying items online, while keeping to a minimum interventions that could jeopardise internet freedom and the open internet agenda. If we consider cyberspace an expansion of the physical social space where crime might happen, as in the physical world we can find crime concentrations online (cyber-hotspots, hot products, etc.). More criminological research is therefore needed to take into consideration transformations in technology, society and crime caused by the internet, and to allow new preventative thinking on reducing criminal opportunities in cyberspace. A genuine and trusting partnership between the academic world, relevant public institutions and law enforcement is necessary to tackle the new challenges of drug trafficking in an effective way.

References

Aldridge, J. and Décary-Hétu, D. (2014), 'Not an "eBay for drugs": the cryptomarket "Silk Road" as a paradigm shifting criminal innovation'. Available at: http://ssrn.com/abstract=2436643 or http://dx.doi.org/10.2139/ssrn.2436643

Barratt, M. J. (2012), 'Silk Road: eBay for drugs', *Addiction* 107, pp. 683–684.

Christin, N. (2013), 'Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace', WWW 2013, International World Wide Web Conference Committee (IW3C2), Rio de Janeiro, preliminary version revised in November 2012. Available at: https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf

Dolliver, D. S. (2015), 'Evaluating drug trafficking on the Tor Network: Silk Road 2.0, the sequel', *International Journal of Drug Policy*. Available at: http://www.sciencedirect.com/science/article/pii/S0955395915000110

EMCDDA (2014), *European drug report: trends and development*, European Monitoring Centre for Drugs and Drug Addiction, Publications Office of the European Union, Luxembourg.

EMCDDA and Europol (2013), *EU drug market report: a strategic analysis*, Publications Office of the European Union, Luxembourg.

Europol (2013), *EU serious and organized crime threat assessment (SOCTA)*, European Police Office, The Hague.

INCB (2011), *Report of the International Narcotics Control Board for 2010: annual report of the International Narcotics Control Board*, United Nations, New York.

Jaishankar, K. (2009), 'Space transition theory of cyber crimes', in Schmallager, F. and Pittaro, M. (eds), *Crimes of the Internet*, Prentice Hall, Upper Saddle River, New Jersey.

Lavorgna, A. (2014), 'Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics', *Trends in Organized Crime* 17(4), pp. 250–270.

Lavorgna, A. (2015a), 'The online trade in counterfeit pharmaceuticals: new criminal opportunities, trends, and challenges', *The European Journal of Criminology* 12, pp. 226–241.

- Lavorgna, A. (2015b), 'Organised crime goes online: realities and challenges', *Journal of Money Laundering Control* 18(2), pp. 153–168.
- Lusthaus, J. (2012), 'Trust in the world of cybercrime', *Global Crime* 13(2), pp. 71–94.
- Martin, J. (2014), 'Lost on the Silk Road: online drug distribution and the "cryptomarket" ', *Criminology and Criminal Justice* 14(3), pp. 351–367.
- Polizia Di Stato (n.a.) *Droga su Internet: maxi-operazione della Polizia*. Available at: http://www.poliziadistato.it/articolo/12255-Droga_su_Internet_maxi_operazione_della_Polizia/
- Suler, J. (2004), 'The online disinhibition effect', *CyberPsychology and Behavior* 7(3), pp. 321–326.
- UNODC (2013), *World drug report*, United Nations, New York.
- UNODC (2014), *World drug report*, United Nations, New York.
- Van Hout, M. C. and Bingham, T. (2014), 'Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading', *International Journal of Drug Policy* 25(2), pp. 183–189.
- Walsh, C. (2011), 'Drugs, the Internet and change', *Journal of Psychoactive Drugs* 43, pp. 55–63.

SECTION III

Surface web markets and social media

CHAPTER 10
A method for exploring the number of online shops selling new psychoactive substances: initial I-TREND project results

CHAPTER 11
Online supply of medicines to illicit drug markets: situation and responses

CHAPTER 12
Social media and drug markets

Overview

This section of the Insights includes three chapters which individually and from different perspectives explore virtual and online drug-related markets that operate primarily on the surface or clear web. The first two chapters examine the online supply of medicines and NPS, substances which in offline drug markets are increasingly supplied and used alongside established illicit drugs. What is less clear, however, is the extent to which the internet, particularly online pharmacies and legal high shops, represent a significant source of supply of these products when they are found on the illicit market.

Chapter 10 addresses the burgeoning online market for the sale and distribution of NPS, including legal highs and research chemicals, which has developed over the last decade. Magali Martinez and Daniela Kmetonyová, describe the methodology used and the crawling software that has been developed for monitoring this market by researchers in five European countries participating in the I-Trend project. They present preliminary results on server locations and provide a typology of online shops based on the products sold as well as describing marketing practices based on their ethnographic research.

In Chapter 11, Lynda Scammell and Alessandra Bo present what is currently known about the illicit online sale of medicinal products via online pharmacies, their possible role as a source for products such as benzodiazepines and opioids to supply illicit drug markets, and the responses implemented in Europe and internationally to tackle this problem.

Chapter 12 addresses the role played by social media and apps in online and virtual drug markets. Danica Thanki and Brian Frederick suggest that social media generally has an indirect role in relation to the supply and sale of drugs. Most sites and apps appear to be primarily used to communicate about drugs — discuss, share opinions and experiences — as well as to make arrangements to meet up to use them. The use of location-based apps, web cams and discussion forums is presented, as are the range of potential responses to problems linked with drugs and social media including interventions implemented by policymakers and law enforcement.

10

CHAPTER 10

A method for exploring the number of online shops selling new psychoactive substances: initial I-TREND project results

Magali Martinez (Observatoire Français des Drogues et des Toxicomanies — OFDT), Daniela Kmetonyová (Charles University in Prague — CUNI), Vendula Běláčková — CUNI([1])

Introduction

Since the late 2000s, new psychoactive substances (NPS) have attracted the attention of decision-makers, and several studies have explored the online supply of NPS through shops on the internet (Hillebrand et al., 2010; Schmidt et al., 2011; Bruno et al., 2013). For example, the Psychonaut 2002 project devised a methodology using search engine queries to identify websites with drug-related content, including those offering to supply psychoactive substances (Schifano et al., 2006). The methodology used in this study was labelled 'snapshot', because it produced a time-specific picture of the existing websites, which can rapidly change. The methodology was further developed by the EMCDDA to gather information about online sales of NPS', and a study was carried out at European level (EMCDDA, 2011a). In addition to providing a quantitative and qualitative assessment of the online supply of NPS, studies also revealed the need for more information on how online markets are structured and for continuous monitoring over time.

Building on these earlier studies, the European Commission-funded the I-TREND (Internet Tools for Research in Europe on New Drugs) project ([2]) aimed, among other things, to develop a software-automated tool for monitoring online shops using a less resource intensive method than had been available previously.

This chapter focuses on the new methodology used to monitor online NPS shops and their characteristics. It contains a description of the semi-automated tools designed for this purpose, which aimed to (i) minimise the human input and maximise the automation of the data-gathering process (ii), allow periodical rather than one-off monitoring and (iii) gather more extensive data than had previously been collected on online shops and their popularity.

Overview of the I-TREND project and its workstream

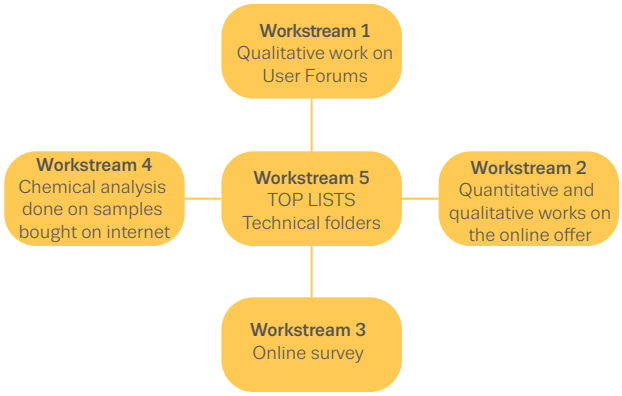
The overall objective of the I-TREND project, which involved researchers from five European countries ([3]), was to help prevent health and social harms linked to NPS and to inform the response to the emerging risks. The principal activities of the project were monitoring online user forums and online shops, conducting an online survey targeting users of NPS, the analysis of samples and the exchange of reference standards among laboratories, and the production of a 'top list' of NPS at national level and of 'technical folders' informed by the project activities. The study comprised five different but interconnected project workstreams, each complementing the others (Figure 10.1) and, to an extent, influencing one another's methodology.

([1]) And all those involved in this part of the I-TREND project: Martin Pažitný (CUNI), Agnès Cadet-Taïrou (OFDT), Amanda Atkinson (Liverpool John Moores University (LJMU)), Daan Van der Gouwe (Trimbos Institute), Damien Sainte-Croix (OFDT), Emma Begley (LJMU), Michał Kidawa (University of Social Sciences and Humanities, Warsaw), Tibor Brunt (Trimbos Institute).

([2]) European project JUST/2012/DPIP/AG/3641 co-financed by the Drug Prevention and Information Programme of the European Union.

([3]) Department of Addictology, First Faculty of Medicine, CUNI and General University Hospital, Prague, the Czech Republic; OFDT, Saint-Denis, France; Centre for Public Health, LJMU, United Kingdom; Trimbos Institute, Utrecht, the Netherlands; SWPS, Warsaw, Poland.

FIGURE 10.1
I-TREND project workstream



I-TREND methodology

Each project partner established a list of the substances considered to be used most frequently in their country (a 'top list') based on Reitox data sources; customs and/or police seizures; toxicovigilance indicators (hospitalisations and deaths); and general population survey results. Each partner could complement these sources with country-specific data, such as results on chemical analyses performed as part of national psychoactive substance investigation measures (Brunt and Van Den Brink, 2012; Lahaie and Cadet-Taïrou, 2012) or specific surveys. The substances included in the top list guided the implementation of other activities (i.e. for the snapshot, the core search terms were the substances included in the top list for the relevant country).

In addition to around 10 chemical names of substances selected per country, some commercial names (so-called branded products) were also included.

The online market for NPS consists of different segments targeting different user profiles (Lahaie et al., 2013). The so-called branded segment is that which offers branded products, with sophisticated packaging, in powder form and also as tablets or herbs. It aims to attract young people, who may be inexperienced and ill-informed about what they are consuming. By contrast, the 'informed segment' aims to reach experienced users, who have more knowledge about different types of NPS, their effects and dosages. In this segment, NPS are mostly referred to by their chemical names and by their chemical structure, and are often described as 'research chemicals'.

Monitoring online shops: a semi-automated software tool

A key aim of the project was to design computational tools to enable regular monitoring of NPS being offered for sale on the internet; these tools were to have the capacity to collect more data in a less time-consuming manner than had been possible in previous snapshot surveys.

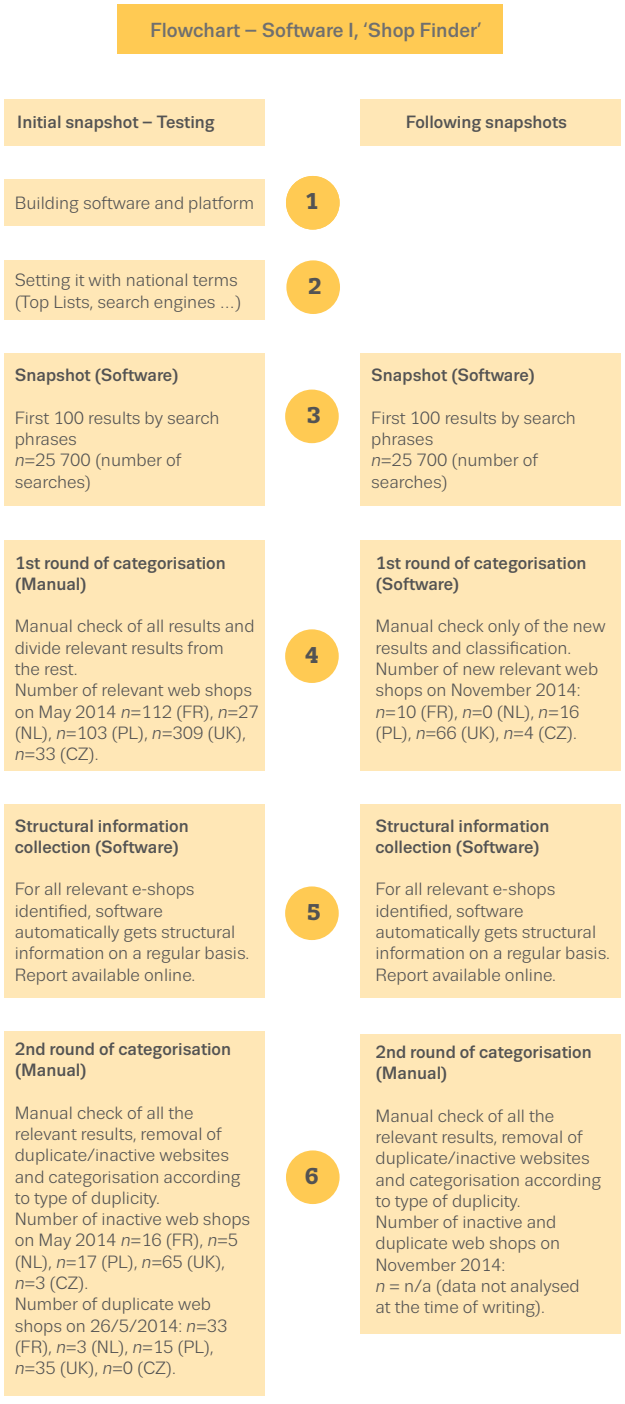
The work comprised two main phases in establishing the semi-automated scraping process: first, development of Software I, 'Shop Finder', then development of Software II, 'Product Scraper'. Both of these phases had three stages: developing the computational tool, setting it with national terms and testing it within a time period. The 'Shop Finder' was used from September 2013 until the end of the project and the 'Product Scraper' was used only between January and April 2015.

Shop Finder had a number of roles, including running the snapshot, categorising the search outcomes and feeding the selected information about shops into an online database on a regular basis. This, in practice, meant that a collaborative online platform was created allowing the partners to indicate for the whole period of the project country-specific search phrases and search engines (e.g. google.nl, yahoo.nl). After the launch of the software at the first snapshot, a manual classification had to be carried out on all of the results in order to separate relevant from non-relevant results. However, for the subsequent snapshots, the already classified sites automatically fell into the categories previously assigned to them — even if the websites in question had temporarily closed and reopened. Only new sites have to be manually classified, which is the key advantage of this process: time-consuming classification has to be done only once, at the beginning, whereas previous methodologies required a manual analysis of all results each time.

The software then automatically collects structural information ([4]) for all relevant online shops periodically. The report, with up-to-date information, is available online for users to download and for further analysis. Manual sifting is then required to remove duplicate web shops, as this process cannot yet be automated.

([4]) Structural information provides details about the physical identity of the site and its owner, as well as statistics about visit frequency for the site (e.g. the URL of the website, the site's IP address and its country of origin, the contact information of the domain owner and the corresponding country, the domain registration date). These data were provided using sites specialising in analysing global internet traffic: whois.com, websiteoutlook.com, alexa.com and websitetrafficspy.com.

FIGURE 10.2
Flowchart — Software I, 'Shop Finder



The most popular online shops were then identified among all the unique shops and selected for further analysis using Software II.

Product Scraper was developed in order to monitor prices and other characteristics of products marketed in those online shops. At the time of writing, only the outcomes from Software I were available; Software II was still in the testing phase.

Search phrases and query frequencies

Software I is designed to search the chosen national and international search engines once a week with the substances selected plus the term 'purchase' in the language of origin of each partner country (Table 10.1). The most popular search engines in the relevant country were used (Table 10.2) and there was a mean of approximately 12 search terms per partner. Names of substances and branded products were tested with different synonyms and spellings (e.g. 'NRG-3' can also be written as 'NRG3' or 'NRG 3', etc.). Generic expressions (e.g. 'party pills') were added in case they returned a substantial number of relevant results.

Only web shops in the national language of the partner country in question were considered relevant results. There were exceptions where appropriate, for example for the Netherlands, where the majority of the population speaks English. In the United Kingdom, all sites in English were taken as relevant, although, in reality, some of these sites may target not the United Kingdom but other English-speaking countries.

Classification of search results

The first 100 results for each search phrase are tracked by the software. This means, that for one search phrase and three search engines, the software tracks 300 results. In the case of duplicate results ([5]) the software takes only one into account. At this stage, human input is required in order to separate relevant results from the rest. This activity is not connected to the software schedule; however, it is better to check the results on a regular basis in order to get structural information on newly identified web shops as soon as possible.

During this process, the results are classified into three subcategories:

- 'e-shops' — all online shops selling NPS;
- 'fora' ([6]) — online fora with NPS-related topics;
- 'small ads' — websites where individuals or professionals post ads offering NPS for sale;

([5]) 'Duplicate results' refers to websites that have the same URL and were found by different search engines.
([6]) The term 'fora' was taken in its broadest sense, designating all websites where supposedly there were no NPS sales, but rather information on these substances and written discussions between people (e.g. comment threads).

TABLE 10.1
Substances and search terms used for the first snapshot

Czech Republic	France	Netherlands	Poland	United Kingdom
'3-MMC' koupit	'AM-2201' acheter	'25-I NBOME' kopen	'3,4-DMMC' sklep	'4-MEC' buy
'4-FA' koupit	'UR-144' acheter	'4-FA' kopen	'3-MMC' sklep	'5 APB' buy
'4-MEC' koupit	'MDPV' acheter	'4-FMP' kopen	'AM-2201' sklep	'5 meo dalt' buy
'6-APB' koupit	'4-MEC' acheter	'4-MEC' kopen	'Brefedron' sklep	'6 apb' buy
'AMT' koupit	'25-I NBOME' acheter	'5-APB' kopen	'Etkatynon' sklep	'AKB48' buy
'bk-MDMA' koupit	'5-MEO-DALT' acheter	'5-IT' kopen	'MDPBP' sklep	'AM-2201' buy
'MDPBP' koupit	'6-APB' acheter	'5-MEO-DALT' kopen	'Mefedron' sklep	'ur-144' buy
'methoxetamine' koupit	'5-APB' acheter	'6-APB' kopen	'Pentedron' sklep	'Ethylphenidate' buy
'ethcathinone' koupit	'Ethylphenidate' acheter	'aMT' kopen	'UR-144' sklep	'MPA' buy
'MPPP' koupit	'Methoxetamine' acheter	'Benzo Fury' kopen	'pMPPP' sklep	'Pentadrone' buy
'Funky' koupit	'NRG3' acheter	'Flava' kopen	'alfa-PVP' sklep	'Phenazepam' buy
'Cherry Cocolino' koupit	'3-MMC' acheter	'Flux' kopen	'6-apb' sklep	'PMA' buy
'Ethylphenidate' koupit	'Happy caps' acheter	'MDPV' kopen	'metoksetamina' sklep	'2-AI' buy
'MPA' koupit	'Party pills' acheter	'MXE' kopen	'funky' sklep	'5-EAPB' buy
'Wlodziu' koupit	'Bong bastic' acheter	'3-MMC' kopen	'mocarz' sklep	'Methoxphendine' buy
'Ex' koupit			'sztywny misza' sklep	'Etizolam' buy
'El Magico' koupit			'kokolino' sklep	'methalone' buy
'DMX' koupit			'włodziu' sklep	'mdai' buy
'Pentedrone' koupit			'dopalacze' sklep internetowy	'amt' buy

- 'inadequate' ([7]) — irrelevant results.

Before further categorisation of the validated online shops, the main automatically collected structural information ([8]) is manually checked to identify any duplicates (Figure 10.2, step 6, and Table 10.3).

After removing all duplicates, unique online shops are manually classified according to four different categories depending on the range of products offered. They are classified as:

- 'research chemical shops' if the substances are displayed mostly with their chemical names, often with an image of their chemical structure;
- 'commercial/branded shops' if the substances are mainly displayed with their trade names;
- 'herbal shops' if the site offers primarily plant-related substances as well as commercial products;
- 'other' if the sites offer products relating to sexual performance, health or general wellness.

These four categories aimed to differentiate sites aimed at informed users from those intended for a wider public, and also to determine the relative importance of each category.

Multi-criteria classification of the 'popularity' of online shops

For relevant online shops categorised as 'unique shops', a further analysis was undertaken to select the most popular online shops. The purpose of this was (i) so that these popular online shops could be scraped with

TABLE 10.2
Search engines used by partner countries

Czech Republic	France	Netherlands	Poland	United Kingdom
Google.cz	Google.fr	Google.nl	Google.pl	Google.com
Seznam.cz	Bing.fr	Yahoo.nl	Bing.com	Bing.com
Centrum.cz	Yahoo.fr	Vvinden.nl		Yahoo.com
		Bing.nl		

([7]) For example, the abbreviation MMC, in addition to referring to a drug, can be used to refer to the thickness of protective gear for sporting activities, as well as having other meanings.
([8]) The site's IP country of origin, the contact information of the domain owner and the corresponding country, the domain registration date and five indicators on popularity from www.alexa.com. Since IP addresses are legally considered personal data, they were encrypted and stored on secure media.

TABLE 10.3

Comparison of online shops collected between November 2013 and May 2014 and their status in May 2014 (1)

	Czech Republic	France	Netherlands	Poland	United Kingdom
Number of shops identified between November 2013 and May 2014	33	112	27	103	309
Number of active shops remaining in May 2014	30	96	22	86	244
Number of active shops remaining in May 2014 with duplicates removed	30	64	19	72	207

(1) New online shops collected in November 2014 have not been included in this table.

Software II and (ii) so that test purchases could be made from these sites.

For this purpose, nine additional categories of automatically collected structural information were used ([9]). Among them, five were given special consideration ([10]), but the global index ranking given by a website specialising in the supply of commercial web traffic data ([11]) was primarily used. To a certain extent, this index is a summary of other information on popularity and, unlike the other popularity indicators, it was available for most of the websites. In addition to these data, other criteria were used to rank the popularity of online shops, such as whether or not the site had been captured by the previous EMCDDA snapshot. In addition, the quality of the translation of the site was taken into account. For example, a real translation, and not an automatic one, was considered to constitute an effort by the site operator to make the site more accessible to users in the target country.

Preliminary findings from the monitoring of online shops

A total of 584 online shops were found by the project partners, with 15 % (88 shops) found identically for multiple countries. The data were gathered between 5 November 2013 and 26 May 2014. Of the 584 identified shops, 18 % (106 shops) were no longer active at the end of the monitoring period on 26 May 2014 (Table 10.3).

Elimination of duplicates and exploring configuration

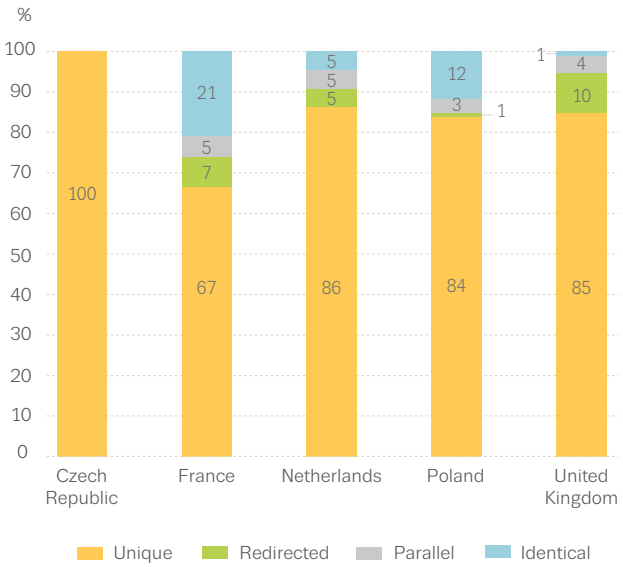
To improve their visibility, some sites deliberately create duplicates (Schmidt et al., 2011). These so-called spamdexing practices move the site in question up the list of results displayed by search engines. By using and cross-checking more structural information from up-to-date snapshot surveys, a more precise estimation of the number of site operators can be achieved. For instance, the project found that it is not possible to identify all duplicates only on the basis of visual information available on the website, such as the URL. This suggests that sites may use rough spamdexing practices and also sophisticated means to increase their visibility. The structural information drawn from active online shops (total: 478) established that 18 % (86) of active websites were duplicate sites (Table 10.3 and Figure 10.3). Consequently, previous studies may have over-estimated the number of online shops.

The proportion of duplicates varies by country; for example, France has the biggest number of duplicates (33 %), where the biggest proportion is made up of identical web pages. The Netherlands, Poland and the United Kingdom have approximately the same portion of duplicates ranging from 14 to 16 %. The Czech Republic stands out for its lack of site duplication. It may be that, as the number of online shops identified for this country is small, duplicate retailers are less likely to be observed.

([9]) The daily revenue generated by the small ads on the site, the number of daily and monthly views of the pages, the global popularity ranking of the website, the number of external links bringing web users to the site, the number of monthly users, etc.
([10]) The global index ranking on search engines, the number of monthly visitors, the number of monthly page views, the number of daily page views, the daily revenue generated by the small ads on the site.
([11]) www.alexa.com

FIGURE 10.3

Breakdown of active online shops by status in May 2014 — same IP, identical, parallel, redirected, unique



Unique	Online shops with a unique design and IP address
Redirected	Online shops redirecting to another online shop already in the category 'Unique'
Parallel	Online shops with the same graphic design as but a different URL and IP address from an existing shop in 'Unique'
Identical	Online shops with the same IP address and graphic design as but a different URL from an existing shop in 'Unique'

National breakdown of supply in a global market

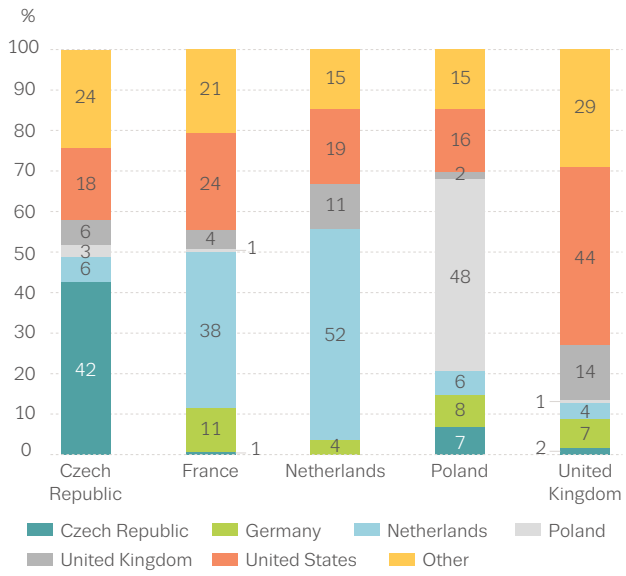
The geographical information about sales sites (e.g. physical location of the sales team, site of the server) can refer to several countries at a time (EMCDDA, 2011). However, building internet search phrases from those substances most frequently present in a particular country can facilitate the understanding of the information collected in the context of national demand.

The unique sales sites intended for the Czech, Dutch and Polish markets are more likely to be locally based (CZ, 42 %; NL, 52 %; PL, 48 %) than those intended for, for example, France, where sites are often located in the Netherlands (38 %) and the United States (24 %). This is also the case for the United Kingdom (44 % located in the United States) ([12]). This point is consistent with the breakdown of web shops by IP location (Figure 10.4).

For France, the servers for the sales sites taken into account are generally outside French territory and often in non-French-speaking countries. This observation may be explained by the fact that, in this country, unlike the four other countries, there is no tradition of 'smart', 'herbal' or 'head' shops, or even of smoking paraphernalia shops.

FIGURE 10.4

Breakdown of active online shops by IP location in May 2014

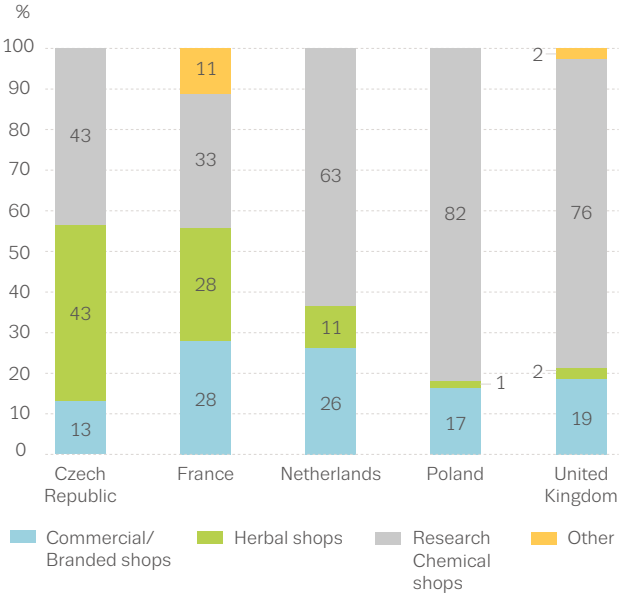


Typology of online shops

The breakdown by site type differs from one surveyed country to another (Figure 10.5). The most popular web shops seem to be RC shops for all countries, although the Czech Republic and France have the same or similar numbers of RC shops and herbal shops. In France, in fact, there is an even distribution between the three main categories of online shops.

FIGURE 10.5

Types of online shops



([12]) Breakdown based on the country location of the IP address of the server hosting the online shop.

Discussion

The collection of quantitative data and qualitative information, using 'a convergent-parallel model' (Condomines and Hennequin, 2014), allows a more meaningful analysis of the online market. At the beginning of the commercial NPS phenomenon, the market could have been seen as an open scene, where retailers were operating in plain sight (Power, 2013). It has, however, become more fragmented and there are different levels of visibility. Between public, private and underground spaces, some sales take place in interstices, between light and shadow. Suppliers use two types of strategies: either maximum internet visibility or a discreet, targeted presence. As they act as companies, they try to be more visible than their competitors, but at the same time, some of them prefer to maintain anonymity and offer specialised supply in spaces undetectable by snapshots. They organise the digital space with gateways, a sort of grey zone, between the surface web and the deep web.

Some online shops try to improve their visibility through spamdexing practices, which helps them to appear at the top of search engine results. In this way they are accessible to the largest possible population, even by people who are not accustomed to using the internet or who have no experience with drugs. At the same time, the qualitative study of user forums indicates that some site operators employ camouflage strategies. Not all websites on the surface internet are detectable by search engines or indeed by the snapshot methodology. Some sites remain invisible either by not using any keywords in their content or by designing their websites so that one part is not accessible on the internet.

The use of codenames to mask the sale of substances is a well-known practice; however, the practice of using legal products to create a diversion is not so well documented. The sites may display only legal products (such as catnip, car maintenance products or laboratory equipment), without mentioning that they can be used for recreational purposes (Giannasi et al., 2012). One finding is that, particularly in such cases, and even when online shops advertise NPS sales on their front page, the sites often don't allow access to their product catalogue, or they restrict the visibility and accessibility of certain substances. NPS are visible only after a user is invited by a person who is already a site customer. The invitation takes the form of a guest code or a URL (e.g. for the deep web). In such cases, the online shop is hardly visible or invisible using the snapshot method.

Conclusion

During the period of the study, the semi-automated tool enabled us to follow the evolution of a number of online shops offering NPS for sale. It reinforces the existing picture of a market that is extremely dynamic and characterised by the closing and opening of new sites. The study shows the need to take duplicate sites into consideration to understand the reality of online supply. The collection and analysis of structural data illustrated the variety of techniques used by retailers to increase their visibility. The data also show notable differences between countries with respect to IP address location and types of site. The NPS phenomenon shows national variation, and continuous monitoring, plus greater efforts to take corresponding national markets into consideration, could help increase our understanding of how the online supply, targeting individual countries, is structured.

Although the process as a whole still requires a large amount of manual input, the main improvement is a reduction in the time needed to run the snapshot and create a preliminary list of online sites to approximately two days. These results could not have been obtained without the implementation of specific technical tools that did not previously exist on the e-reputation software market ([13]). The automation of data collection (including structural information, their indexation, and the establishment of an iterative system that documents a database at each loop) allow, researchers and institutions to take over the snapshot methodology. Whereas it has been used for one-off tasks, it can be now used for continuous monitoring.

The choice of substances used to establish the list of queries is the main limitation of this study, because the results of the snapshot depend on it. In particular, the choice of trade names is more difficult because there are many and, unlike the chemical names of the substances, they are not systematically reported by the Reitox data sources (e.g. customs seizures, health alerts). Nevertheless, taking them into account remains essential because this maintains the link between retail and supply.

Finally, part of the online supply of NPS on the surface web takes place in a grey area that cannot be quantitatively monitored, and there may, therefore, be a difference between measuring NPS accessibility and measuring NPS availability. Sites that are completely

([13]) E-reputation software performs surveillance of a given subject by cross-checking information automatically collected on sites that pertain to the subject (blogs, forms, media) and the reactions of internet users on these same sites or on related social networks.

invisible on the surface web cannot be found using the snapshot methodology. Such an observation of the online NPS supply can only be made if some of the supply and demand remains on the surface web in visible spaces. As a result of the regulations and legislation that Member States adopt, both with respect to NPS (European Commission, 2013) and internet functioning, the 'balloon effect' ([14]) may lead to the NPS online market becoming increasingly less visible and more difficult to monitor.

References

- Bruno, R., Poesiat, R. and Matthews, A. J. (2013), 'Monitoring the Internet for emerging psychoactive substances available to Australia', *Drug and Alcohol Review* 32(5), pp. 541–544.
- Brunt, T. M. and Van den Brink, W. (2012), 'Monitoring illicit psychostimulants and related health issues', in Thèse de M. Oisterwijk (ed.), BOXPress.
- Condomines, B. and Hennequin, E. (2014), 'Studying sensitive issues: the contributions of a mixed approach', *RIMHE: Revue Interdisciplinaire Management, Homme(s) & Entreprise* 14(5), pp. 3–19.
- EMCDDA (2011a), 'Online sales of new psychoactive substances/'legal highs': summary of results from the 2011 multilingual snapshots', *Briefing paper* 15/11/2011, European Monitoring Centre for Drugs and Drug Addiction, Lisbon.
- EMCDDA (2011b), 'Responding to new psychoactive substances', *Drugs in Focus* 22, pp. 1–4.
- European Commission (2013), 'Report on the proposal for a regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC, 2002/22/EC, and Regulations (EC) No 1211/2009 and (EU) No 531/2012 (COM(2013)0627 - C7-0267/2013 - 2013/0309(COD))', European Commission, Brussels.
- Giannasi, P., Pazos, D., Esseiva, P. and Rossy, Q. (2012), 'Détection et analyse des sites de vente de GBL sur Internet : perspectives en matière de renseignement criminel', *Revue Internationale de Criminologie et de Police Technique et Scientifique* 65(4), pp. 468–479.
- Hillebrand, J., Olszewski, D. and Sedefov, R. (2010), 'Legal highs on the Internet', *Substance Use and Misuse* 45(3), pp. 330–340.
- Lahaie, E. and Cadet-Taïrou, A. (2012), 'France — early warning system', *Early warning system —national profiles*, Office of the European Union, Luxembourg, pp. 53–57.
- Lahaie, E., Martinez, M. and Cadet-Taïrou, A. (2013), 'New psychoactive substances and the Internet: current situations and issues', *Tendances* 84, OFDT, Paris.
- Power, M. (2013), *Drugs 2.0: The web revolution that's changing how the world gets high*, Portobello Books, London.
- Schifano, F., Deluca, P., Baldacchion, A., et al. (2006), 'Drugs on the web; the Psychonaut 2002 EU project', *Progress in Neuro-Psychopharmacology and Biological Psychiatry* 30(4), pp. 640–646.
- Schmidt, M. M., Sharma, A., Schifano, F. and Feinmann, C. (2011), '"Legal highs" on the net-Evaluation of UK-based Websites, products and product information', *Forensic Science International* 206(1–3), pp. 92–97.

([14]) The balloon effect refers to the displacement of criminal activities from one geographical area to another.

11

CHAPTER 11

Online supply of medicines to illicit drug markets: situation and responses

Lynda Scammell and Alessandra Bo

Introduction

This chapter explores what is known about the online supply of medicines and medicinal products, with a focus on the sale of psychoactive medicines via online pharmacies and/or other virtual platforms and their potential role as a source for the illicit drug market. In Europe, the misuse of medicines such as methadone, buprenorphine, fentanyls and benzodiazepines among high-risk drug users has been reported more frequently in recent years, for example among clients entering drug treatment centres (EMCDDA, 2015). The source of supply of these drugs is not always clear, but it is likely to include diversion from legitimate medical sources, the global unregulated trade in medicines and illicit production (Griffiths et al., 2014). Whatever the source of production, or mechanism of diversion, recent years have witnessed an increase in the illicit online sale of medicines. What is less clear is whether the internet in general, and online pharmacies in particular, have a significant role as a source of supply of medicines to illicit drug markets in Europe.

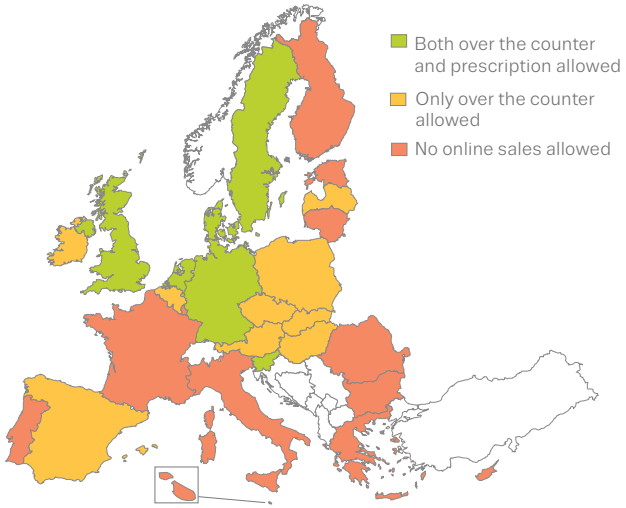
The subject of illicit internet supply of medicines and responses to it is a complex one, and this chapter briefly addresses the broader topics of licit and illicit online pharmacies, as well as counterfeit and falsified medicines, before looking at the limited evidence of links with illicit drug markets. It finishes on the issue of policy and practice responses in the area. The lead author has many years of experience working in the United Kingdom in the field of medicines regulation, and includes here examples and case studies from this country for illustrative purposes.

Types of medicinal products sold online

The online sale of medicines took off in the early 2000s (Forman, 2006a) and, although various platforms have been used, online pharmacies have been a primary source of distribution. In the early days, the most popular products to be supplied on the web were natural and herbal medicinal products, smoking cessation aids, and beauty and sexual performance enhancement products (such as Viagra®) (Orizio et al., 2011). More recently, the market for enhancement drugs such as muscle builders, diet pills and sunless self-tanning sprays has been expanding (Evans-Browns et al., 2012) and there have been reports of cancer drugs and stem cells being marketed over the internet (Fittler et al., 2013).

Medicines sold online are typically categorised by national regulatory agencies into ‘over the counter’ (OTC) and ‘prescription-only medications’ (POMs). The legal position surrounding the online supply of medicines varies across the European Union. Some countries, such as the United Kingdom and Germany, allow all classes of medicines (POMs and OTC medicines) to be sold online. Others allow only OTC medicines to be supplied online, and some countries, such as Italy, prohibit the supply of medicines online altogether (see Figure 11.1). The advertising of a POMs is not permitted anywhere in the European Union and therefore any website advertising a POMs is in breach of legislative requirements and action can be taken to remove the website.

FIGURE 11.1
Different legislative positions in the European Union on the online sale of medicines



Source: L. Scammell, presentation at expert meeting held at the EMCDDA, 30–31 October 2014.

In addition to the sale of OTC medicines and POMs, increasing attention has been paid to the topic of counterfeit and falsified medicines in recent years. According to the European Medicines Agency, 'falsified medicines are fake medicines that are designed to mimic real medicines' — that is, a product that passes itself off as a real, authorised medicine — while 'counterfeit medicines are medicines that do not comply with intellectual-property rights or that infringe trademark law' — that is, a product made by someone other than the genuine manufacturer, by copying or imitating an original product without authority or rights (EMA, 2015). Internationally, there is not an agreed definition, and the World Health Organization (WHO) addresses the problem with a broader definition that encapsulates both concepts: 'A counterfeit medicine is one which is deliberately and fraudulently mislabelled with respect to identity and/or source. Counterfeiting can apply to both branded and generic products and counterfeit products may include products with the correct ingredients or with the wrong ingredients, without active ingredients, with insufficient active ingredients or with fake packaging' ([1]).

Counterfeit medicines include all types of medicinal product, both OTC medicines and POMs, as well as enhancement drugs, and the WHO called the problem of counterfeit medicines 'a growing threat to public health around the world' (WHO, 2010). The criminal market for counterfeit medicines was estimated to be worth GBP 55 billion (approximately EUR 78 billion) in 2010 (Jackson, 2009). The central role of the internet in facilitating and enhancing this global market is widely acknowledged, posing an increased threat to public health. According to WHO, around 50 % of the medicines sold online from illegal sites concealing their physical identity are counterfeits (WHO, 2010).

Finally, cases of online sales of food and dietary supplements such as phenibut have also been on the rise. Phenibut is an authorised medicine in Russia used for treating anxiety, alcohol withdrawal, OCD,

The United Kingdom position on the online sale of medicines

The United Kingdom has strict legal controls on the sale, supply and advertisement of medicinal products. Under medicines legislation, it is unlawful for medicinal products for human use to be marketed, manufactured, imported from a third country, distributed and sold or supplied in the United Kingdom except in accordance with the appropriate licences or exemptions. The United Kingdom has three legal classes of authorised medicines:

- General sale list (GSL) medicines are suitable for sale and normal use without supervision or advice from a pharmacist or doctor.
- Pharmacy (P) medicines can only be obtained from a pharmacy and are sold or supplied under the supervision of a pharmacist.
- Prescription-only medicines (POMs) must be prescribed by an authorised healthcare professional, for example a doctor, dentist or independent prescriber.

A UK registered pharmacy may have a presence on the internet; however, the legislative requirements apply equally to UK internet pharmacies and bricks-and-mortar premises; for example, POMs cannot be advertised directly to the public. These legal controls also apply equally to medicines for human use sold or supplied via the internet or through email transactions. Some POMs are 'controlled drugs' (such as benzodiazepines) and their availability to patients can be subject to additional control under the Misuse of Drugs Act 1971, which is administered by the Home Office.

([1]) See: http://www.who.int/medicines/regulation/ssffc/definitions/en/

stammering and insomnia, but it is not licensed as a medicine in Europe or approved as a pharmaceutical in the United States.

Sales platforms

Online pharmacies: legitimate and illegitimate

Online pharmacies, of varying degrees of legitimacy, are the major online market platform for medicines. Online (or internet) pharmacies are retail companies that operate partially or exclusively over the internet and sell medicinal preparations, including prescription-only drugs, via online ordering and mail delivery (Orizio et al., 2011; Lavorgna, 2014).

Online pharmacies have been classified in several ways (Arruñada, 2004; Mäkinen et al., 2005; Jena et al., 2011; NABP, 2014b; LegitScript, 2015), but the different classification criteria all have a focus on consumer safety at their core. According to the latest US Internet Drug Outlet Identification Program progress report, of the 10 866 internet drug outlets selling prescription medications reviewed between April and September 2014, '96.4 % (10 473) were found not to be in compliance with American State and Federal laws and/or National Association of Boards of Pharmacy patient safety and pharmacy practice standards' (NABP, 2014a). These data resonate with the information provided by LegitScript, a US-based initiative with the largest database of health-related websites; it monitors over 331 430 websites, of which currently 35 610 are active internet pharmacies and 33 579 (94.3 %) are not operating legitimately (LegitScript, 2015).

From a consumer safety perspective, online pharmacies can be classified into two main categories: (i) legitimate and (ii) illegitimate. Legitimate websites comply with national and international regulations and standards, guaranteeing the quality of the product, requiring a valid medical prescription when buying controlled medicines and ultimately assuring consumer safety. On the other hand, illegitimate online pharmacies are, often, not registered with any recognised accreditation system and do not abide by regulations and professional standards, and are therefore operating illegally. They typically sell medicines without prescriptions, or they market counterfeit or falsified products, putting consumer safety at risk. Illegitimate pharmacies can be further divided into sub-categories depending on the degree of compliance with national and international standards.

A recent systematic review by Orizio et al. (2011) outlined some of the major features of online pharmacies described in the literature (see Table 11.1). These include affiliation to any internationally recognised accreditation system; the disclosure of geographical location and contact details; the types of medicines available; the quality of the product (from the packaging and instructions to the chemical composition); the availability of information on the product; the requirement of a valid prescription for controlled medicines; and the availability of an online medical consultation.

As highlighted in the criminological research by Lavorgna (2014), the advent of Web 2.0 provided new

TABLE 11.1
Selected features of online pharmacies — summary of analytical frameworks used in research

	Legitimate sites	Illegitimate sites
Affiliation to any internationally recognised accreditation system	Affiliation to internationally recognised accreditation systems are clear and visible	Usually no affiliation to internationally recognised accreditation system
Disclosure of the geographical location and contact details	Geographical location and contact details are disclosed	Typically concealment of both geographical location and contact details
Types of medicines available	Any medical product available in a physical pharmacy	Anything, but usually specialising in prescription-only medicines
Quality of the product	Product is genuine Instructions included	Spectrometry analysis is more likely to indicate counterfeit products Packaging and instructions can be problematic
Availability of information on the product	Comprehensive information on the product	Often limited information on the product
Requirement of a valid prescription for controlled medicines	Valid prescription required	No valid prescription required
Availability of online medical consultation/ information	Optimal medical consultation/information	Often sub-optimal medical consultation/information

criminal opportunities in the online trade in counterfeit medicines and affected the market in a number of different ways. The internet not only affected communication and transportation, enhancing their efficiency, but also changed the modus operandi of criminal networks. For example, the internet has allowed more streamlined management of the distribution process and has opened up opportunities for new actors who are not affiliated to established criminal networks or organisations to enter the market. A new trend identified by Lavorgna (2014) is the online purchase of medicinal products in larger quantities than previously, for the purpose of resale, mainly in local, offline markets. The online market allows individuals to step easily into the trafficking chain, and to target sales at certain consumer segments, particularly in the area of lifestyle and doping products.

Furthermore, Lavorgna suggests that the internet has influenced interactions with clients and allowed suppliers to use promotional tactics, persuasive marketing and loyalty-building strategies to market their products to a larger potential customer base.

Diversification of retail outlets: eBay, Amazon

Online pharmacies are not the only type of retail outlet selling medicines over the internet. Dedicated forums, social media and online magazines increasingly play a role in the sale and advertisement of medicines, particularly with regard to doping products, lifestyle products and 'enhancement' drugs (Lavorgna, 2014).

Trading platforms such as eBay and Amazon also run advertisements offering to supply medicines. In Europe, the legality of this will vary from Member State to Member State. POMs, medicines that are required to be dispensed by a pharmacist (or under their direct supervision) and unlicensed medicines cannot be legally sold and supplied in this way.

In the United Kingdom, the MHRA has arrangements in place with eBay and Amazon to ensure that advertisements and listings for medicines that legally should not be supplied in this way are removed (usually within 24 hours).

A source for the illicit drug market?

Although there is increasing concern about the potential role of illegally operating online pharmacies in the supply of psychoactive medicines for misuse, there are disappointingly few studies in this area (Forman et al., 2006a; Nielsen and Barratt, 2009; Ghodse, 2010), and these are mostly from outside Europe. The scientific evidence on general population behaviour with regard to the online purchase of medicines relies on two types of data: surveys and clinical case studies. A systematic review by Orizio (2011) found that the percentage of people reporting that they had purchased medicines online, mostly from US studies, is generally low, at between 1 and 6 % of the population, and slightly higher in studies where the intention to buy online was also considered.

The misuse of controlled substances obtained online is a growing and well-documented concern in the United States (Forman et al., 2006b; Jena et al., 2011). One study used state-level data to investigate whether or not the rise in prescription drug abuse between 2000 and 2007 was associated with the growth in high-speed internet access. The regression analysis showed that for every 10 % growth of high-speed internet use there was a 1 % increase in substance abuse treatment admissions for drugs readily available on the internet, for example prescription opioids, benzodiazepines, sedative hypnotics and stimulants (including amphetamine), while the correlation was not there for substances not available online, such as alcohol, heroin or cocaine (Goldman and Jena, 2011). However, despite well-documented evidence of an increase in the misuse and abuse of prescription drugs (Lipman and Jackson, 2006; SAMSHA, 2012), there is a lack of evidence to suggest that the source of these drugs at the level of an individual user is the internet.

Although the use of prescription opioids has purportedly reached its peak in the United States, the average level of use in the European Union is currently 4.5 times lower (ALICE RAP, 2013). Several system-level factors have been hypothesised to contribute to this difference, such as the less severe regulatory systems operating in the United States and the different prescription and dispensing practices (Fischer et al., 2014). However, patterns are changing and also in Europe the misuse of opioid substitution treatment medicines has been reported more frequently in drug treatment centres (EMCDDA, 2015). The source of these drugs within the EU borders has been associated with the global unregulated trade of medicines as well as the complex market of new psychoactive substances (Griffiths et al., 2014), yet no specific research is available on the role of the internet and online retailers.

Inciardi et al. (2010) carried out a specific study in the United States investigating who the end-users of prescription drugs purchased over the internet were. Five key datasets focusing on the potential populations of end-users (including national and college surveys and

opioid maintenance treatment programmes) were considered. The results were consistent across the different populations: the internet is a relatively minor source for the illicit purchase of prescription drugs. The main sources of supply varied across the groups but were typically drug dealers, friends or relatives, and the medical system itself. The authors suggest that, although the internet might not be a major source for end-users, it may play a larger role at the dealer level.

A more recent study (Bachhuber and Cunningham, 2013) investigated the online purchase of the synthetic opioid buprenorphine without a prescription. After screening for unique sites and testing their stability over a six-month period, the study identified 20 illegitimate sites selling buprenorphine and only two legitimate sites. The price of a 30-day supply offered on the illegitimate sites varied between USD 232 and USD 1 163, whereas the same dose was sold in the legitimate sites for as low as USD 58 and not over USD 135. The authors conclude that sites on the surface web are unlikely to be reliable sources of buprenorphine supply and that the growing dark net markets may provide a more reliable and less expensive alternative (Aldridge and Décary-Hétu, 2014).

Responding to the problem of the illicit online supply of medicines

The criminal market in pharmaceuticals thrives in an environment characterised by a lack of stable and harmonised legislation within and across countries. Specific supply-focused responses do, however, exist and they tackle the problem at different levels:

- regulating the trade of online pharmacies;
- monitoring prescription drugs;
- implementing coordinated international supply reduction activities.

In June 2014, the European Commission passed a new Implementing Regulation (699/2014) that gave Member States one year to apply a common logo to the websites of all retailers of medicines legally operating in the European Union (European Commission, 2014). The regulation was implemented across the European Union on 1 July 2015 and also involves a national database listing details of legal suppliers in each Member State. Although the logo could be forged by the illegal sites, it is, nevertheless, an important first step in regulating online pharmacies across Europe (Figure 11.2).

FIGURE 11.2
Promotional campaign for the EU logo for online retailers of medicines

Source: European Commission, available at: http://ec.europa.eu/health/human-use/eu-logo/index_en.htm

Different international accreditation/verification systems already exist to ensure consumer safety, as they warrant that online retailers follow quality standards in their practice. One example is the HON-Code (Health on the Net Code), which is based on ethical standards in offering medical information on the web ([2]).

With regard to responses to counterfeit and falsified medicines, the US Food and Drug Administration has developed a dedicated section on its website for consumers on 'Buying medicines over the Internet' (FDA, 2015). The European Medicines Agency has also developed dedicated resources to warn consumers about falsified medicines (EMA, 2015), and several pan-European initiatives, representing a broad range of interests, have been set up to inform patients on how to buy medicines safely online (e.g. the European Alliance for Access to Safe Medicines and the Alliance for Safe Online Pharmacies).

In terms of law enforcement responses, international efforts are led by Interpol through Operation Pangea. This initiative was started by the MHRA in the United Kingdom in 2004 and has expanded each year until Interpol took on a coordination role. The operation started in 2008 and runs for a week each year. It brings together several law enforcement bodies from countries around the world including customs, health regulators and national police, and includes the private sector. It tackles the online sale of counterfeit medicines and

([2]) The HON-Code is the most widely accepted reference for online health and medical publishers. Currently, the Code is used by over 7 300 certified websites more than 10 million pages, covering 102 countries and translated in to 35 different languages. Health on the Net Foundation (HON) was granted non-governmental organisation status on 23 July 2002 by the Economic and Social Council of the United Nations. HON also has a partnership at the French governmental level, when it was accredited in 2007 by the French National Authority (HAS) to be the official certifying body for all French health websites. Source: https://www.healthonnet.org/HONcode/Patients/Visitor/visitor.html

highlights the dangers of buying medicines online. The last operation took place in June 2015 (Interpol, 2015) and resulted in 20.7 million counterfeit medicines (worth more than USD 81 million) being seized, 156 arrests and more than 2 410 websites being taken offline.

At European level, there is not a common legislative approach to tackling the problem of counterfeit medicines. National initiatives such as those implemented by the MHRA in the United Kingdom include routine monitoring of medicines offered for sale online, investigative activities of illegal activity taking place on a website and, where appropriate, taking enforcement action against suppliers who operate outside the legal requirements. It also runs campaigns with patient associations and the General Pharmaceutical Council (the UK regulator for the retail pharmacy sector) and collaborates with industry to test-purchase medicines from websites. With the assistance of the Metropolitan Police Central e-Crime Unit and cooperation from domain name providers, such as Nominet (the provider of the Dot UK domain space), the MHRA has closed down thousands of websites (including sites based overseas) and brought hundreds more into compliance.

Conclusion and future trends

This review has shown that the online supply of medicines is a complex issue and of growing concern. However, in relation to illicit drug markets, the available evidence suggests that currently online retailers play a minor role in the supply of medicines to illicit marketplaces. New evidence also indicates that cryptomarkets on the deep web may become more involved in the supply of controlled prescription drugs in the future.

Overall, this review has highlighted the need for a better understanding of the role of surface web retailers, such as online pharmacies, in the diversion of prescription medicines, and the need for more targeted consumer-level research focusing on sources of drug supply. Moreover, owing to the very different regulatory systems and prescription and dispensing practices in the United States and Europe, specific EU studies would be desirable.

References

Aldridge, J. and Décary-Hétu, D. (2014), 'Not an "eBay for drugs": the cryptomarket "Silk Road" as a paradigm shifting criminal innovation'. Available at: http://ssrn.com/abstract=2436643 or http://dx.doi.org/10.2139/ssrn.2436643

ALICE RAP (2013), *Prescription opioids and public health in the European Union*, AR Policy Paper 4, http://www.alicerap.eu/resources/documents/cat_view/1-alice-rap-project-documents/19-policy-paper-series.html

Arruñada, B. (2004), 'Quality safeguards and regulation of online pharmacies', *Health Economics* 13(4), pp. 329–344.

Bachhuber, M. A. and Cunningham, C. O. (2013), 'Availability of buprenorphine on the Internet for purchase without a prescription', *Drug and Alcohol Dependence* 130(0), pp. 238–240.

EMA (European Medicines Agency) (2015), 'Falsified medicines' http://www.ema.europa.eu/ema/index.jsp?curl=pages/special_topics/general/general_content_000186.jsp&mid=WC0b01ac058002d4e8

EMCDDA (2015), *European drug report 2014: trends and developments*, Publications Office of the European Union, Luxembourg. Available at: http://www.emcdda.europa.eu/publications/edr/trends-developments/2015

European Commission (2014), Commission Implementing Regulation (EU) No 699/2014 of 24 June 2014 on the design of the common logo to identify persons offering medicinal products for sale at a distance to the public and the technical, electronic and cryptographic requirements for verification of its authenticity, *Official Journal of the European Union*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2014_184_R_0004&from=EN

Evans-Brown, M., McVeigh, J., Perkins, C. and Bellis, M. A. (2012), *Human enhancement drugs: the emerging challenges to public health*, North West Public Health Observatory Centre for Public Health, Faculty of Health and Applied Social Sciences, Liverpool John Moores University. Available at: http://www.erpho.org.uk/viewResource.aspx?id=22342

FDA (US Food and Drug Administration) (2015), US Department of Health and Human Services, 'Buying medicines over the Internet', http://www.fda.gov/Drugs/ResourcesForYou/Consumers/BuyingUsingMedicineSafely/BuyingMedicinesOvertheInternet/default.htm

Fischer, B., Keates, A., Bühringer, G., Reimer, J. and Rehm, J. (2014), 'Non-medical use of prescription opioids and prescription opioid-related harms: why so markedly higher in North America compared to the rest of the world?', *Addiction* 109, pp. 177–181.

Fittler, A., Bösze, G. and Botz, L. (2013), 'Evaluating aspects of online medication safety in long-term follow-up of 136 Internet pharmacies: illegal rogue online pharmacies flourish and are long-lived', *Journal of Medical Internet Research* 15(9), e199.

Forman, R. F., Marlowe, D. B. and McLellan, A. T. (2006a), 'The Internet as a source of drugs of abuse', *Current Psychiatry Reports* 8, pp. 377–382.

Forman, R. F., Woody, G. E., McLellan, T. and Lynch, K. G. (2006b), 'The availability of web sites offering to sell opioid

medications without prescriptions', *American Journal of Psychiatry* 163(7), pp. 1233–1238.

Ghodse, H. (2010), 'Watching Internet pharmacies', *British Journal of Psychiatry* 196(3), pp. 169–170.

Goldman, D. P. and Jena, A. B. (2011), 'Growing Internet use may help explain the rise in prescription drug abuse in the United States', *Health Affairs* (Millwood) 30(6), doi:10.1377/hlthaff.2011.0155

Grabosky, P. N. and Smith R. G. (2001), 'Telecommunication fraud in the digital age: the convergence of technologies', in Wall, D. S. (ed.), *Crime and the Internet*, Routledge, London/New York.

Griffiths, P., Evans-Brown, M. and Sedefov, R. (2014), 'Commentary on Fischer et al: Non-medical use of prescription opioids and prescription opioid-related harms: why so markedly higher in North America compared to the rest of the world?', *Addiction* 109(2), pp. 177–181.

Inciardi, J. A., Surratt, H. L., Cicero, T. J. et al. (2010), 'Prescription drugs purchased through the Internet: who are the end users?', *Drug and Alcohol Dependence* 110(1–2), pp. 21–29.

Interpol (2015), Operation Pangea, 2015, http://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea

Jackson, G. (2009), 'Faking it: The dangers of counterfeit medicine on the Internet', *International Journal of Clinical Practice* 63(2), p. 181

Jena, A. B., Goldman, D. P., Foster, S.E. and Califano Jr, J. A. (2011), 'Prescription medication abuse and illegitimate Internet-based pharmacies', *Annals of Internal Medicine*, 155, pp. 848–850.

Lavorgna, A. (2014), 'The online trade in counterfeit pharmaceuticals: new criminal opportunities, trends and challenges', *European Journal of Criminology* 1–16, doi: 10.1177/1477370814554722

LegitScript (2015), 'Internet pharmacy classifications', http://www.legitscript.com/pharmacies/classifications/

Lipman, A. G. and Jackson, K. C. (2006), 'Controlled prescription drug abuse at epidemic level', *Journal of Pain and Palliative Care Pharmacotherapy* 20, pp. 61–64.

Mäkinen, M. M., Rautava P. T. and Forsström, J. J. (2005), 'Do online pharmacies fit European internal markets?', *Health Policy* 72(2), pp. 245–252.

NABP (National Association of Boards of Pharmacy) (2014a), *Internet drug outlet identification program progress report for state and federal regulators*, http://safeonlinerx.com/wp-content/uploads/2014/11/idoi-report-oct2014.pdf

NABP (2014b), See the website for details at: http://www.nabp.net/programs/consumer-protection/buying-medicine-online

Nielsen, S. and Barratt, M. J. (2009), 'Prescription drug misuse: is technology friend or foe?', *Drug and Alcohol Review* 28, pp. 81–86.

Orizio, G., Merla, A., Schulz, P. J. and Gelatti, U. (2011), 'Quality of online pharmacies and websites selling prescription drugs: a systematic review', *Journal of Medical Internet Research* 13(3), e74.

RADARS System (2015), www.radars.org SAMHSA (Substance Abuse and Mental Health Services Administration) (2012), *Results from the 2012 National Survey on Drug Use and Health: summary of national findings*, http://www.samhsa.gov/data/NSDUH/2012SummNatFindDetTables/NationalFindings/NSDUHresults2012.pdf

WHO (2010), *Bulletin of the World Health Organization* 88(4), pp. 241–320.

12

CHAPTER 12
Social media and drug markets

Danica Thanki and Brian Frederick

Introduction

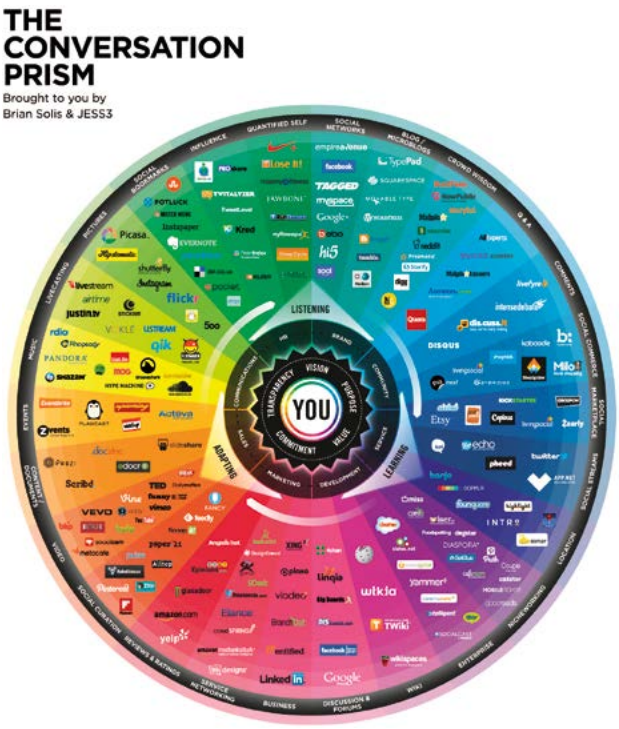
This chapter provides an overview of social media platforms and how they can affect drug markets. Drawing on the literature to explore the drug-related content existing on various social media channels, the chapter discusses how social media have both a direct impact on drug supply and an indirect impact on demand for drugs. The chapter goes on to provide a summary of responses and discusses the need for future research to develop our understanding of social media and how they affect drug supply and demand.

Social media

Social media, according to Mandiberg (2012), are new technological frameworks that enable 'formerly passive media consumers to make and disseminate their own media'. They reflect the evolution of Web 2.0 technologies, which allow users to continuously create, modify and/or publish content and applications 'in a participatory and collaborative fashion' (Kaplan and Haenlein, 2010, p. 61). Social media sites predominantly exist on the surface web and are, therefore, visible to all internet users, although they require varying levels of user registration for participation. Nevertheless, user-modified content also exists on the deep web, for example in forum discussions such as Silk Road's 'Ask a Drug Expert Physician about Drugs and Health' (see Chapter 7), while some social media sites established on the surface web, including the social networking giant Facebook, have recently allowed users anonymous access on the deep web through the Tor Browser.

The term 'social media' encompasses numerous types of social interaction sites and apps, including social networking sites, photo- and video-sharing sites, blogs and micro-blogs, discussion and forum sites, review and ratings sites, and social streams. Figure 12.1 provides a visual overview of the different types of social media through what Solis (2015) calls the 'conversation prism'. Although sites differ in communication mode, they all feature significant user interactivity and participation, as well as multidirectional lines of communication, and represent a transformation in the way in which we use the internet.

FIGURE 12.1
The different types of social media



Source: Brian Solis and Jesse Thomas.

The recent exponential growth of the internet, and in particular of social media, and the impact it has had on contemporary society is vast. According to Nielsen (2012), a US- and Netherlands-based global information and measurement company, internet users spend more time engaging with social media sites and applications than on any other type of site. Facebook, which became publicly accessible at the end of 2006, currently has more than 1.6 billion registered users worldwide, 1.35 billion of whom have been active in the previous 30 days; YouTube, the video-sharing site, has more than 1 billion active users; and Twitter, the social streaming site, has more than 500 million registered users. In

addition to providing opportunities for increased communication and knowledge sharing among individuals, social media have substantially changed the way that businesses, organisations, communities and individuals interact.

As the world of social media develops at a rapid pace, many new technologies go 'viral' before their potential impact can be determined. Although there are undoubtedly benefits to the increased opportunities for social interaction, there are also well-documented concerns around the negative impact of social media, particularly in relation to bullying and sexual exploitation. There are also reports of social media being used to orchestrate the activities of subversive and extremist groups (Schils and Pauwels, 2013), organised crime syndicates (Kingston, 2014) and terrorist organisations (Zeng et al., 2010).

Although some social media users concerned about their privacy may protect their identity, many others do not take precautions and may have poor security levels. Similarly, some users may refrain from posting content that may be unlawful or that they know to be unlawful on social media platforms, while others may succumb to what has been called an 'illusion of anonymity' and openly post content that transgresses legal and/or moral thresholds (Zheleva and Getoor, 2009).

Social media and drug markets

In general, social media can affect drug markets in two ways. First, social media may have an impact on the supply of drugs by providing opportunities for buying and selling drugs (direct impact). Second, they may have an impact on the market by affecting the demand for drugs in general and for individual drugs through, for example, the impact of drug-related experience sharing, drug-themed photo and video sharing, and drug-focused opinion forming (indirect impact).

There are, however, few research studies exploring social media and drug markets. Where research on social media does address drugs, it tends to be in the fields of behavioural health, epidemiology and public health, rather than criminology. Research, therefore, tends to focus on the influence of drug-related social media content on young people's demand for drugs rather than on the supply of drugs through social media channels. Although concerns exist about the impact of greater exposure to drug-related content on demand for drugs, particularly among young people, the evidence of its impact remains scarce, although some studies have shown that traditional media coverage of drugs can increase interest in buying drugs (Forsyth, 2012). Nevertheless, there remains insufficient evidence to provide us with a good understanding of the impact of social media on the demand for drugs.

In order to better understand the role of social media in drug markets, systematic analyses of numerous social media platforms are needed, incorporating a wide range of different perspectives. Currently, research studies looking at a specific social media application are more common in peer-reviewed journals (as well as in 'grey' literature). These often focus only on the existence of drug-related content rather than its impact, generally on the premise that this content increases the demand for drugs. Examples of the different types of drug-related content on social media and of current knowledge and research are given below.

Supply of drugs

Social media can facilitate the supply of drugs in a number of ways. One way is that users can directly advertise drugs for sale. In 2014, drugabuse.com published an infographic documenting drug dealer activity on the picture- and video-sharing service Instagram (drugabuse.com, 2014). By searching for hashtags relating to drug sales, the researchers were able to identify 50 drug dealer accounts in a day. Many contained photographs of drugs for sale. Social media were used to advertise the drugs for sale, but the transactions took place through other communication channels, such as mobile phones or messaging apps, which often allow users to remain anonymous. However, the researchers found that more than one-third of the drug dealers identified displayed a photograph of their face. There have also been numerous media reports of dealers caught by law enforcement agencies after posting details of their drug dealing activities through personal social media accounts, for example through Facebook accounts. Some researchers have begun to use web analytics to discover the presence of drugs for sale on social media.

Social media can also provide potential buyers with information on how and where they can purchase drugs, as well as evidence of successful purchases in the form of positive feedback. In his article 'Teens on Tumblr can't stop bragging about Silk Road drug deals', journalist Patrick Howell O'Neill analysed the microblogging site Tumblr for material posted by teenagers who were interested in how to buy drugs on the dark web site Silk Road (O'Neill, 2013). The posts included details and

pictures (including selfies) of users, as well as advice on how to shop on Silk Road. O'Neill discovered that adolescents often implicated their friends, girlfriends and boyfriends in their Tumblr posts; some even mentioned their parents: '5/5, package came on schedule. My dad intercepted the package though, so no Xanax for me!'

Research has consistently found that young people obtain drugs through their social networks (Duffy et al., 2008), with friends being the most common source of drugs (European Commission, 2014). It stands to reason that, as social networks move increasingly from the real world to the digital world, the buying and selling of drugs will follow suit. Nevertheless, although social media can facilitate drug supply, the exchange of the product must still take place in the physical environment, through the postal service or face-to-face.

Drug-related content on social networking sites

There are concerns that the presence of drug-related content on social networking sites could influence normative behaviours regarding drug use and increase demand for drugs, particularly among young people. Cavazos-Rehg et al. (2014) analysed the demographics of the almost 1 million followers of a pro-marijuana Twitter handle ('handle' being Twitter jargon for a user's screen name) and the content of the tweets posted using that handle. They found that the majority of the followers were 19 years old or under (73 %) and that 54 % of them were female. The content mainly concerned positive cannabis discourse; many of the tweets were perceived as humorous. The authors warned of the influence of social media during adolescence and the potential impact on drug using behaviours.

Another study by Hanson et al. (2013a) performed a qualitative analysis of the quantity and content of tweets containing the drug name 'Adderall'. The study reported 213 633 Adderall-related tweets over a six-month period, with a peak coinciding during the examinations period. Tweets were also analysed for content related to motives, side effects, poly-use and possible normative influence. The authors concluded that Adderall discussions through social media such as Twitter may contribute to normative behaviour regarding its abuse. A similar conclusion was drawn by Hanson et al. (2013b) in relation to social circles and prescription drug abuse.

Concerns around online social networks mirror those related to offline social networks; principally, that exposure to certain behaviours within a social network will affect an individual's behaviour and social norms. However, what is unclear is the added impact that easier access to groups of like-minded individuals through online communities has on individual behavioural norms. This may be of particular importance for traditionally hidden activities such as drug use and supply, with individuals able to seek out online groups easily and anonymously.

Specific drug forums

There are a large number of user forums dedicated to the discussion of illicit drugs, such as Bluelight.ru, Erowid and Drugs-forum.com. Most research has explored the harm reduction aspects of these forums, with the majority of users claiming that they access the sites primarily to learn how to use drugs more safely (Chiauzzi et al., 2013). Research often highlights the opportunity to use forums for targeted prevention (Soussan and Kjellgren, 2014). Nevertheless, there are concerns that the forums' content could encourage experimentation with a wider range of drugs and increase demand for certain substances. For example, information about how to extract active ingredients from pharmaceuticals may increase demand for such substances. Conversely, bad trip reports on forums and warnings about individual substances and methods of drug use may decrease demand for particular substances and influence types of use. Although there is limited evidence of the impact of forums on drug use behaviours, the ability to monitor discussions can be a useful tool for the identification of emerging trends in drug use and markets and to inform policy and practice (Davey et al., 2012).

Video and picture sharing

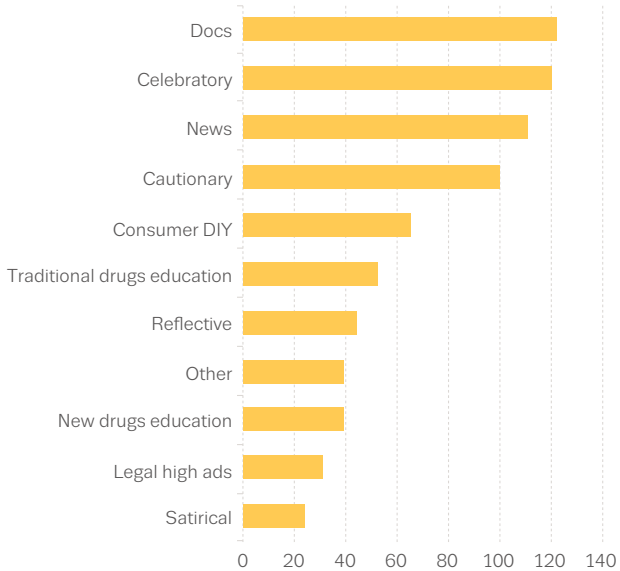
YouTube is the most popular video-sharing site, while the picture-sharing sites Flickr and Instagram are also very popular at the time of writing. In addition, many other social media channels not specifically viewed as focused on picture or video sharing provide users with opportunities to share these types of media. Lau et al. (2012) highlight the potential negative impact of social media content depicting behaviours such as drug use, although the authors suggest that further research is needed on how this online content is disseminated and how individuals process it.

Much research focuses on the content of social media. For example, Manning (2013) examined the link between YouTube, drug videos and drug education. The study involved a content analysis of 750 drug videos (sampled from over 300 000 individual YouTube videos), of which 12 % had been posted by official agencies (see Figure 12.2). The study found that a minority (16 %) of the drug-related videos on YouTube were celebratory (i.e., hedonistic), but that these differed by drug — for example, no celebratory videos about heroin or crystal meth were found. Many cautionary videos (also known as 'vernacular prevention' videos) were also identified. 'Do-it-yourself' (DIY) videos (e.g. videos that provided instructions on how to grow your own cannabis) and legal high advertisements were also identified. The study concluded that official prevention campaigns should use more modern methods to reach individuals.

A similar study (Lange et al., 2010) also identified a large number of drug use-related videos on YouTube. It found that the researchers were able to analyse the effects and side effects of *Salvia divinorum* solely by viewing YouTube user-uploaded videos. Walsh (2011) argued that the existence of *Salvia* videos on YouTube increased public awareness of the substance and stimulated demand, but also put it on the agenda of law-makers in the United Kingdom, thus contributing to its prohibition and attempts to restrict the market.

FIGURE 12.2

The sample of YouTube drug videos coded by drug discourses



Source: Manning (2013).

Drug-themed apps

There are a large number of drug-themed apps available from app stores such as Google Play and Apple's App Store. These include apps designed to prevent drug use such as Your Face on Meth, which allows users to upload a picture and see the physical degradation that would result over time from using methamphetamine. Other apps promote drug use. Research by Bindham et al. (2014) focused on apps promoting illicit drug use, with the author observing an increase in these types of apps over a three-month period. By the end of the study (in 2012), 410 drug-promoting apps were identified, the majority of which (98 %) were found to promote cannabis, with many providing a forum for like-minded drug-users. Some examples of the types of apps that were found included drug-themed 'wallpaper' apps; apps that provided information on drug use; drug-themed gaming apps; drug use simulations; drug-themed clock widgets; a drug-themed battery icon widget; drug-related stickers; and apps that were used to share substance use stories. Others, such as the How to Sell Weed app, provide instructions for the production and selling of cannabis. The authors of the study voiced public health concerns, particularly in relation to young people, and suggested government intervention as a means 'to enforce [the] proper standardisation of app-rating processes'.

In the United States, where the sale of cannabis in licensed outlets has recently become legal in some states, news reports have highlighted the existence of apps related to the cannabis trade. For example, one report likened the Leafy App (launched on 26 January 2015) to a 'Grindr for weed' in that the app 'offers an interactive catalogue of different varieties of cannabis, their characteristics and availability (mostly in medical cannabis outlets) based on the nearest GPS location' (Neal, 2014). Another journalist reported on Weedhire — an app that was designed to 'connect pot labs, dispensaries and even government regulators' to potential employees in the (legal) cannabis industry (O'Neill, 2013).

Social media sites and networks facilitating drug-related encounters between men who have sex with men

One of the most common ways to access and interact with social media is through smartphone and tablet apps. Some geosocial networking apps employ location-based mobile social computing using the Global

Positioning System to establish a user's proximity to other users. Grindr, which claims to have 5 million users in 192 countries worldwide ([1]), is an example of this type of app and is used primarily by men who have sex with men (MSM). It has recently been reported to be a conduit for the facilitation of high-risk behaviours (such as drug-seeking). For example, Bourne et al. (2014) reported that some men use Grindr to locate partners for 'chemsex' or 'party-and-play' (PNP) sessions. Chemsex and PNP refer to sex among MSM while using various drugs, including methamphetamine, cocaine, gamma-hydroxybutyrate (GHB), gamma-butyrolactone (GBL) and mephedrone. Grindr can also facilitate 'slamming parties' — prolonged MSM sex parties that involve the injection of illicit drugs (Frederick, 2015).

In addition to Grindr, there also exist numerous MSM virtual social networks (VSNs) that feature a high number of self-identified drug users.

This sort of social networking is best described as taking place on VSNs, rather than online social networks, as much communication takes place via smart phones and tablets. VSNs can be categorised into static networks, which are more permanent and may include user profiles and terms of use (e.g. Facebook), and dynamic networks (e.g. Skype or ooVoo video chat), which are temporary and often by invitation only. A feature of VSNs is the creative use of slang and argot to get around moderation. Static (and especially) dynamic VSNs that use webcams have been recently associated with 'chemsex' parties and/or 'slamming' among MSM.

A few examples of MSM VSNs include PlanetRomeo.com (a German-based VSN), which has at least 11 member-created drug-themed 'clubs'; NastyKinkPigs.com (a US-based VSN with members throughout the United States, the United Kingdom and Europe), which allows individuals to specify drug use preferences in their member 'profiles'; and Get2ThePoint (ynotmingle.com), which describes itself as 'an online clubhouse for Slamming enthusiasts' (ynotmingle.com, 2015). '2ThePoint' refers to the injection of methamphetamine and/or mephedrone, in particular, as well as other drugs. Unlike Get2ThePoint, PlanetRomeo and NastyKinkPigs also have smartphone apps that employ location-based technology.

Another recent trend among MSM drug users is the online sharing of sexualised drug ingestion experiences via real-time webcam broadcasts — either on MSM VSNs with webcam chat rooms, in group conference calls (Skype or Zoom) or privately (Skype). MSM seeking webcam drug experiences can often locate other Skype members and/or active Zoom conference calls through services such as Google+ Communities.

Some MSM share their drug ingestion experiences by uploading video content to video-sharing websites. Gay pornography producer Treasure Island Media maintains one such site, ToxxxicTube, which features hundreds of user-uploaded videos of men apparently smoking or injecting illicit drugs such as crystal methamphetamine.

As well as sharing drug use experiences, there are suggestions that sites may also facilitate drug supply. A recent online article by Vice found that 'One of the most common profile names or sub-headings on Grindr has become "GMTV" which implies that the person is using, has to share, or has to sell, G (GBL), M (mephedrone), T (Tina AKA crystal meth) or V (Viagra). By using colloquial slang for drugs, and using search fields on certain sites, you can hunt for the drug you're after, or people who are using it who might be willing to hook you up electronically with someone who'll get some for you' (Daly, 2015).

Using web analytical methods to monitor drug use and markets

Recently, researchers have analysed social media data using data mining techniques to explore the different ways in which large numbers of social media data might be processed and how social media analysis can provide an additional source of data on drug use and markets. Yakushev and Mityagin (2014) found that, through data mining, the level of interest in drugs among the users of these media could be determined. In addition, the authors were able to obtain information on the interests of individuals who had posted drug-related content. They suggest that social media can provide a better picture of those with 'light' addiction problems than traditional sources of data on drug use.

Web analytics have also been used by criminal justice researchers to explore social media and drug supply. One of these studies (Watters and Phair, 2012) developed a new methodology known as Automated Social Media Intelligence Analysis to analyse social media platforms for the presence of drug buying and selling. The search found many examples of sellers advertising drugs and buyers requesting drugs on social media. They also found that no examples of illicit drug advertising were found among paid advertisements.

([1]) See Grindr.com

Social media policies, supply and demand reduction responses

Owing to the large volume of drug-related social media user content, the numerous and varied types of environments in which such content is posted and a lack of understanding about the impact of different types of social media content, a comprehensive response to drug-related social media content is not anticipated any time soon. Although law enforcement agencies continue to develop their practices to respond to evolving online methods of drug supply, other stakeholders will be important in tackling the negative impact of drug-related social media content. For example, the policies and practices of social media owners are under scrutiny, particularly with respect to the monitoring of member-user activities. The research world also has a role to play in creating a better understanding of the impact of different types of social media content on behaviour and in developing methods of online social media monitoring. In addition, researchers can use the opportunities provided by increased online social contact to recruit hitherto hidden research subjects. Similarly, professionals in the prevention, harm reduction and treatment fields need to develop their services to align them better with today's digital modes of communication.

Tackling the buying and selling of drugs: law enforcement responses

According to numerous sources (e.g. grey literature, news media reports, peer-reviewed journal articles), the drug-related monitoring of social media by police and other law enforcement entities does occur. However, because of the sheer volume of data involved, the automatic (or semi-automatic) screening of drug-related social media content by law enforcement can often be very tedious, making such operations difficult or even impracticable (Watters and Phair, 2012). Moreover, the results of such screenings often include false positives. Where law enforcement monitoring does lead to arrests, media reports suggest that they often involve young people found with small amounts of illicit drugs and who have little to no prior history of criminal behaviour, or small-scale dealers who lack sophistication in their operations (Knibbs, 2013; Storm, 2013; Chicoer, 2014; Taylor, 2014).

An additional complication for law enforcement agencies monitoring social media is that member-users often employ special language when communicating about drugs or drug-related activities and behaviours, as described in the section on sites and apps for MSM. This argot, or drug-related slang words, develops over time, making it exceedingly difficult for those monitoring to keep up with the changing use of language. This is because the purpose of drug-related argot is to 'maintain secrecy so as to hide subculture communications from outsiders' (Johnson et al., 2006), especially law enforcement agents.

Some law enforcement actions are successful, though. Some social media-related drug arrests concern the illegal sale of prescription drugs (rather than the dealing of illicit drugs). Others are made in conjunction with larger 'sting' operations. For example, an August 2013 Instagram-related 'gun bust' sting operation in New York City led to hundreds of arrests (the largest in NYC history) and in April 2014 a large US-wide sting operation (conducted by the US DEA and the FBI) led to the arrest of more than 350 drug dealers, all of whom had posted drug-related content on Instagram.

Social media policies and practices

The British Broadcasting Corporation (BBC) recently reported that most social media owners do not actively monitor and/or remove drug-related content (BBC Trending, 2013a). Some social media owners responded to these accusations, citing reasons of impracticality or invasiveness. Legal reasons were also cited. Others claimed to take a 'reactive' approach to the presence of drug-related content on member-user pages. Typically, social media owners give their member-users the opportunity to report inappropriate or illegal content, and some owners stress their commitment to reviewing such reports within a short period of time, usually 48 hours.

In a follow-up to its original investigative report, the BBC noted that Instagram had responded by blocking numerous drug-related hashtags on its site (BBC Trending, 2013b). Still, many lay and professional members of the public have demanded that Instagram and other social media owner-operators take a more proactive approach to removing drug-related and other content of an illegal nature.

Further research and monitoring

Research exploring the link between new forms of media, in particular social media, and drug supply and

demand is still in its infancy. In particular, the extent of drug supply through social media channels is underexplored. Improved methods of monitoring online social media content, possibly through web analytics, and also research with drug users themselves will be required to understand fully the role of online supply in drug markets. Research needs to move beyond merely identifying drug-related social media content to assessing its impact on drug use behaviours.

There has been a growing acknowledgement of the need to incorporate digital monitoring into drug monitoring systems through the identification of drug-related content on social media apps and sites. For example, the University of Maryland's Center for Substance Abuse Research has been commissioned by the US National Institute on Drug Abuse (NIDA) to run the National Drug Early Warning System (NDEWS) for the next five years; part of its role will be, for the first time, to collect data from social media and web platforms in order to identify emerging illicit drug trends. NIDA is also funding a USD 11 million, three-year research programme to explore the use of social media to improve our understanding of drug use, addiction, prevention and treatment ([2]).

As well as using social media to identify emerging trends and understand drug use behaviours, some researchers have used it to assess the impact of responses aimed at reducing drug misuse. For example, McNaughton et al. (2014) analysed social media to assess the impact of the introduction of reformulated opioid analgesics designed to prevent abuse. The European I-TREND project (see Chapter 10) also used social media to inform its online monitoring of shops selling new psychoactive substances, and Ledberg (2015) used internet forums to explore interest in new psychoactive substances before and after control.

Demand reduction responses

Health services have been slow to adapt to changing modes of communication and to develop new methods of reaching target groups (EU Task Force on eHealth, 2012). Manning (2013) found some examples of official drug prevention videos on YouTube, but, unlike other drug videos, these did not allow user comments. Social media engage users in conversations, and services, need to adapt, moving away from one-way messaging to more participatory approaches (Neiger et al., 2013). In the absence of appropriately delivered services, other actors will fill the void. Thus, forums may become the go-to place for harm reduction advice, despite concerns about the quality of the information provided. Analysis of forums has identified demand for harm reduction and treatment advice, particularly among users who may not feel comfortable attending treatment services, such as socially integrated recreational drug users. Social media provide opportunities for engaging with hard-to-reach client groups (Davey et al., 2012) and show similar levels of use across ethnic groups. Targeted messaging using demographic and other information (such as interest in nightlife) may provide a cost-effective way of reaching the right individuals and tailoring messages and responses to their specific needs. In addition, social media can provide opportunities for creating online communities that support recovery from drug dependence.

Conclusion

The growth of social media has revolutionised methods of communication and affected the way we interact with each other. In terms of the direct impact on drug markets, there remains insufficient evidence of its role in the supply of drugs. More vigilant controls by social media owners, and greater clarity about their level of responsibility for ensuring that services are not used to facilitate criminal activity, may help to restrict drug supply through these channels.

In terms of the indirect impact on drug markets in relation to demand for drugs, the impact of increased exposure to drug-related content online, particularly on younger people, needs better exploration. This will not only increase our understanding of how social media influence behaviour but also allow us to target responses to the areas with the greatest potential negative effects and help us to design more appropriate responses. At the same time, there is a need to have a balanced approach to the issue, identifying and responding to the negative aspects but also identifying ways in which social media can be harnessed by the research and monitoring community and prevention and treatment agencies to better understand drug use and to improve demand reduction responses.

References

BBC Trending (2013a), 'Instagram blocks some drugs advert tags after BBC probe', http://www.bbc.co.uk/news/technology-24842750

([2]) http://www.drugabuse.gov/news-events/news-releases/2014/10/using-social-media-to-better-understand-prevent-treat-substance-use

BBC Trending (2013b), 'How drugs are offered on Instagram', 7/11/2013, http://www.bbc.co.uk/news/magazine-24849537

Bindham, N. F., Naicker, S., Freeman, B., McGeechan, K. and Trevena, L. (2014), 'Apps promoting illicit drugs: a need for tighter regulation?', *Journal of Consumer Health on the Internet* 18(1), pp. 31–43.

Bourne, A., Reid, D., Hickson, F. and Torres Rueda, S. W. P. (2014), *The chemsex study: drug use in sexual settings among gay and bisexual men in Lambeth, Southwark and Lewisham*, Sigma Research, London School of Hygiene and Tropical Medicine, London.

Cavazos-Rehg, P., Krauss, M., Grucza, R. and Bierut, L. (2014), 'Characterizing the followers and tweets of a marijuana-focused twitter handle', *Journal of Medical Internet Research* 16(6), p 157, doi: 10.2196/jmir.3247

Chiauzzi, E., Dasmahapatra, P., Lobo, K. and Barratt, M. J. (2013), 'Participatory research with an online drug forum: a survey of user characteristics, information sharing, and harm reduction views', *Substance Use and Misuse* 48(8), pp. 661–670.

Chicoer (2014), 'Six drug arrests in Chico, undercover operation included social media', http://www.chicoer.com/general-news/20141101/six-drug-arrests-in-chico-undercover-operation-included-social-media

Daly, M. (2015), 'The future of drugs according to Vice', http://www.vice.com/en_uk/read/the-future-of-drugs-max-daly-according-to-vice-531

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

Drugabuse.com (2014), 'Drug dealer profiles on Instagram', http://drugabuse.com/featured/instagram-drug-dealers/

Duffy, M., Schaefer, N., Coomber, R., O'Connell, L. and Turnbull, P. J. (2008), *Cannabis supply and young people — 'It's a social thing'*, Joseph Rowntree Foundation, York.

European Commission (2014), 'Young people and drugs: Flash Eurobarometer 401'.

EU Task Force on eHealth (2012), *Redesigning health in Europe for 2020*, http://www.e-health-com.eu/fileadmin/user_upload/dateien/Downloads/redesigning_health-eu-for2020-ehtf-report2012_01.pdf

Forsyth, A. J. (2012), 'Virtually a drug scare: mephedrone and the impact of the Internet on drug news transmission', *International Journal of Drug Policy* 23(3), pp. 198–209.

Frederick, B. J. (2015), ' "Slam camming": exploring the link between men-for-men drug pornography and the emergence of webcam drug use among gay and queer men', Annual Meeting of the American Society of Criminology, Washington, DC.

Get2ThePoint (2015), http://ynotmingle.com/

Hanson, C. L., Burton, S. H., Giraud-Carrier, C., et al. (2013a), 'Tweaking and tweeting: exploring Twitter for nonmedical use of a psychostimulant drug (Adderall) among college students', *Journal of Medical Internet Research* 15(4), e62, doi: 10.2196/jmir.2741

Hanson, C. L, Cannon, B., Burton, S. and Giraud-Carrier, C. (2013b), 'An exploration of social circles and prescription drug abuse through Twitter', *Journal of Medical Internet Research* 15(9), e189, doi:10.2196/jmir.2741

Hoffner, C., Plotkin, R., Buchanan, M., et al. (2006), 'The third-person effect in perceptions of the influence of television violence', *Journal of Communication* 51(2), pp. 283–299.

Holt, M. (2014), 'Sex, drugs, and HIV: let's avoid panic', *The Lancet HIV* 1(1), e4–e5.

Johnson, B. D., Bardhi, F., Sifaneck, S. J. and Dunlap, E. (2006), 'Marijuana argot as subculture threads: social constructions by users in New York City', *British Journal of Criminology* 46(1), pp. 46–77.

Kaplan, A. M. and Haenlein, M. (2010), 'Users of the world, unite! The challenges and opportunities of social media', *Business Horizons* 53(1), pp. 59–68.

Kingston, T. (2014), 'Italians enraged at rise of Sicily's new Facebook mafia', *The Telegraph*, http://www.telegraph.co.uk/news/worldnews/europe/italy/11008060/Italians-enraged-at-rise-of-Sicilys-new-Facebook-mafia.html

Knibbs, K. (2013), 'Meet social media's drug dealers, also known as "the stupidest people on the internet" ', http://www.digitaltrends.com/social-media/selling-drugs-on-social-media-the-stupidest-people-on-the-internet-vol-1/

Lange, J. E., Daniel, J., Homer, K., Reed, M. B. and Clapp, J. D. (2010), '*Salvia divinorum*: effects and use among YouTube users', *Drug and Alcohol Dependence* 108(1), pp. 138–140.

Lau, A., Gabarron, E., Fernandez-Luque, L. and Armayones, M. (2012), 'Social media in health: what are the safety concerns for health consumers?', *Health Information Management Journal* 41(2), p. 30.

Ledberg, A. (2015), 'The interest in eight new psychoactive substances before and after scheduling', *Drug and Alcohol Dependence* 152, pp. 73–78.

Livingstone, S., Ólafsson, K. and Staksrud, E. (2013), 'Risky social networking practices among "underage" users: lessons for evidence based policy', *Journal of Computer Mediated Communication* 18(3), pp. 303–320.

McNaughton, E. C., Coplan, P. M., Black, R. A., et al. (2014), 'Monitoring of internet forums to evaluate reactions to the introduction of reformulated OxyContin to deter abuse', *Journal of Medical Internet Research* 16(5), e119, doi: 10.2196/jmir.3397

Mandiberg, M. (ed.) (2012), *The social media reader,* NYU Press, New York, pp. 1–10.

Manning, P. (2013), 'YouTube, "drug videos" and drugs education', *Drugs: Education, Prevention and Policy* 20(2), pp. 120–130.

Neal, M. (2014), 'The Leafly App is like Grindr for weed', http://motherboard.vice.com/blog/the-leafly-app-is-like-grindr-for-weed

Neiger, B. L., Thackeray, R., Burton, S. H., Giraud-Carrier, C. G. and Fagen, M. C. (2013), 'Evaluating social media's capacity to develop engaged audiences in health promotion settings: use of Twitter metrics as a case study', *Health Promotion and Practice* 14, pp. 157–162.

Nielsen (2012), *State of the media: the social media report 2012*, http://www.nielsen.com/us/en/insights/reports/2012/state-of-the-media-the-social-media-report-2012.html

O'Neill, P. H. (2013), 'Teens on Tumblr can't stop bragging about Silk Road drug deals', http://www.dailydot.com/crime/tumblr-teens-silk-road-drug-deals/

Paul, B., Salwen, M. B. and Dupagne, M. (2007), 'The third person effect: a meta-analysis of the perceptual hypothesis', in Preiss, R., Gayle, B., Burrell, N., et al. (eds), *mass media effects research: advances through meta-analysis*, Lawrence Erlbaum, Mahway, New Jersey, pp. 81–102.

Schils, N. and Pauwels, L. (2013), 'Explaining violent extremism: the role of new social media', European Society of Criminology 2013 Conference abstracts. Available at: https://biblio.ugent.be/publication/4147823

Solis, B. (2015), 'The Conversation Prism: Version 4', https://conversationprism.com/

Soussan, C. and Kjellgren, A. (2014), 'Harm reduction and knowledge exchange: a qualitative analysis of drug-related Internet discussion forums', *Harm Reduction Journal* 11, p. 25.

Storm, D. (2013), 'Busted! Cops arrest teenager after she posted a picture of pot on Instagram', http://www.computerworld.com/article/2474831/data-privacy/busted--cops-arrest-teenager-after-she-posted-a-picture-of-pot-on-instagram.html

Taylor, V. (2014), 'Facebook him! Florida man arrested after posting drug-related selfie'. 10/5/2014, http://www.nydailynews.com/news/crime/florida-man-arrested-posting-drug-related-selfie-article-1.1787366

Vandoninck, S., d'Haenens, L. and Roe, K. (2013), 'Online risks: coping strategies of less resilient children and teenagers across Europe', *Journal of Children and Media* 7(1), pp. 60–78.

Walsh, C. (2011), 'Drugs, the Internet and change', *Journal of Psychoactive Drugs* 43(1), pp. 55–63.

Watters, P. A. and Phair, N. (2012), 'Detecting illicit drugs on social media using automated social media intelligence analysis (ASMIA)', in *Cyberspace Safety and Security*, Springer, Berlin and Heidelberg, pp. 66–76.

Yakushev, A. and Mityagin, S. (2014), 'Social networks mining for analysis and modeling drugs usage', *Procedia Computer Science* 29, pp. 2462–2471.

Zeng, D., Chen, H., Lusch, R. and Li, S. H. (2010), 'Social media analytics and intelligence', *Intelligent Systems* 25(6), pp. 13–16.

Zheleva, E. and Getoor, L. (2009), 'To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles', in *Proceedings of the 18th international conference on World Wide Web,* ACM, New York, pp. 531–540.

IV

SECTION IV

Insights and implications

CHAPTER 13

What is the future for internet drug markets?

13

CHAPTER 13

What is the future for internet drug markets?

Jane Mounteney, Paul Griffiths and Liesbeth Vandam

Introduction

In gathering together contributions from a variety of experts in the field, this publication has sought to set out what is known about the nature and functioning of drug markets on the internet with a view to enhancing our understanding of their current and potential importance as a source of supply for illicit drugs. At the time of writing and reflected in the balance of contributions to this publication, there is noticeably more academic interest in, and output on, the functioning of drug marketplaces in the deep web, an area that has witnessed rapid growth since 2010. Given the diversity and complexity of surface web markets, operating across a diffuse internet landscape, it is particularly difficult to map their structure and functioning. The constant and rapid evolution of social media sites and apps both offer an entry to online markets and represent additional platforms where drugs are discussed and offered for sale.

Despite evidence of drug selling on both the surface and the deep web, the size and scale of these markets is far from clear. We have reasonably good descriptions of dark net markets, less so for surface web markets, but overall there is little evidence on the relative importance of online markets as a source of supply. With regard to those substances for which there is some legal ambiguity or regulatory loophole, the majority of sales appear to take place on the surface web. By contrast, the majority of sales activity linked to illicit drugs appears to take place on the deep web. Although the online sale of fake and counterfeit medicines represents a major global enterprise, at present, evidence of sourcing of medicines for the illicit drug market from online pharmacies is slim. We note that more information on the online sales of new psychoactive substances and research chemicals is now emerging, with some evidence of overlap with illicit markets, via so-called grey marketplaces.

Drivers of change

A wide range of factors appear to be driving change and development in internet drug markets, mostly linked to technology, globalisation and market innovation. Digital literacy and knowledge are increasing and thereby expanding the pool of potential market users. The technology is clearly important, and new developments are changing how we interact both commercially and socially across the board. Developments in encryption, digital currencies and anonymous browsing are among the technologies driving change in dark net markets. We also note the influence of marketing innovations, for example the establishment of the deep web search engine GRAMS. This search engine for Tor-based dark net markets allows users to search multiple markets for products such as drugs and guns from a simple search interface.

As discussed in Chapter 3, Tor is the largest and best-known 'onion router' network, offering a level of anonymity that has made it a popular tool among internet users wishing to avoid government or corporate censorship and/or to engage in illicit activities online. One of the challenges associated with private browsing can be its speed, and this is an area where technology is driving innovation. In a recent paper, Chen et al. (2015) describe their development of a new anonymising network called HORNET (High-speed Onion Routing at the NETwork layer), which is an onion-routing network that could be the next generation of anonymising technology.

Recent years have witnessed a global and exponential growth in e-commerce across the board and, in some respects, recent trends in the growth of online drug marketplaces may merely reflect this broader social phenomenon. In this context, the rapid development of easy online payment systems has been a major facilitator of new developments. Nevertheless, at present, e-commerce is still dwarfed by traditional

modes of commerce and, despite online shopping having seen a massive increase, data on 2014 retail sales (direct to the final consumer) show a European average of 7.2 % ([1]). By analogy, it is not unreasonable to assume that, at present, most transactions in the sphere of illicit drug supply still take place in offline markets, and will probably continue to do so for some time.

Social and cultural dynamics have also been a central feature in the rise of dark net markets. Reports highlight the charismatic figures involved in running marketplaces, such as Ross Ulbricht, Silk Road's Dread Pirate Roberts. In the early iterations of cryptomarkets such as Silk Road, there was an emphasis on the value given to participation in online communities of like-minded people, and the importance of online activism. Undoubtedly, an additional major driver of public interest in, and use of, these dark net markets has been the widespread media reporting, bringing them to the attention of a new audience. Buxton and Bingham (2015) suggest that as a result of a combination of factors — including expanding internet access, a tech-savvy generation, new security tools, cryptocurrencies and sustained international demand for drugs — the expansion of dark net markets is likely to continue.

The internet and drug markets: mapping and market demarcation

With regard to the size and segmentation of drug markets on the internet, some issues have become clearer. First, there are a number of different but overlapping online drug markets, although the relative size of the various markets is hard to quantify. An approximate demarcation can be made between markets open to all on the clear or surface web; markets that are not accessible to traditional browsers on the deep web; and actively concealed and anonymised dark net markets or cryptomarkets.

The deep web represents the largest part of the internet, incorporating as it does all elements stored in databases, private networks, unlinked sites and hidden services. It is impossible to measure, and hard to estimate, the size of the deep web because the majority of the information is hidden or locked inside databases. Early estimates suggested that the deep web was 400 to 550 times larger than the surface web. However, since more information and sites are always being added, it can be assumed that the deep web is growing exponentially at a rate that cannot be quantified ([2]). By comparison, the part of the web accessible to traditional search engines, the clear or surface web, is estimated to be fairly small. Cryptomarkets or dark net markets represent only a minuscule element, in terms of the space they take up, of the deep web.

There is also some differentiation between the availability of products in surface and deep web markets. It is estimated that, for medicines and new psychoactive substances, most online drug market transactions are likely to take place on the surface web, via online shops and pharmacies, but also via classified ads and research chemical websites. Medicines and new psychoactive substances are available on dark net markets, but sale of illicit drugs is more common on these platforms. Soska and Christin (2015) note that around 70 % of all sales on the sites they were monitoring were of cannabis, ecstasy and cocaine-related products. Heroin, other opioids and new psychoactive substances were also available for sale.

A further area of uncertainty is at what level of the market online transactions take place, particularly those made on the deep web. In Chapter 8, Joost van Slobbe argues that, if a European organised criminal group wished to order a large consignment of heroin or cocaine, there would necessarily be face-to-face contact between representatives of the supplying and receiving criminal organisations. Martin (2013), however, suggests that dark net markets open up the possibility of a direct link between drug-using buyers and producers or synthesisers of illicit drugs, and may eventually serve to cut out some of the middle level of the market. In Chapter 2, Aldridge and Décary-Hétu suggest that direct producer–user transactions are more likely for the kinds of drugs where small-scale producers can operate without large-scale international networks (e.g. cannabis, mushrooms, NBOMe). They highlight the fact that a substantial proportion of dark net market customers are buying in bulk, probably sourcing stock to sell offline and thereby making these markets the very location of the middle market for certain products. Dolliver's analysis (2015) suggests that only a small minority of vendor accounts may have connections to more sophisticated criminal groups or upper-level retailers markets and that the majority are 'opportunistic' vendors. Soska and Christin (2015) note that the vast majority of vendors in their study earned less than USD 10 000 over the three-year monitoring period, concluding that these markets are primarily competing with street dealers in the retail space. Taken together, this evidence suggests

(1) http://www.retailresearch.org/onlineretailing.php

([2]) Wikipedia: https://en.wikipedia.org/wiki/Deep_web_ %28search %29

that dark net markets are linked with criminal innovation and a new breed of entrepreneurial drug dealer engaging in what could be described as 'disorganised crime'.

Online versus offline drug markets

The internet offers a relatively open and global virtual marketplace, in contrast to the closed networks of dealers and buyers more recently associated with the use of mobile phone technology. From the perspective of the seller, Silk Road has been described as a paradigm shifting, transformative criminal innovation, as it provided drug dealers with a range of new opportunities and potential benefits compared with offline markets. The gain: an expanded market for their products; the capacity to sell to customers not already known to them; and the ability to trade anonymously and in a relatively low-risk environment (Aldridge and Décary-Hétu, 2014). Online marketplaces may also offer the benefit of increased personal safety (buyer and seller) and reduce the possibility of violence, as buyers and sellers never reveal their identities and never meet face to face. Improved product quality (purity, price, type of product) and reduced risk of detection have also been cited as perceived advantages in studies. Nevertheless, there appears to be a relatively high risk of financial scamming in both online and street markets.

In terms of the number of transactions or heaviness of traffic, commerce on dark net markets is estimated by commentators to be a fraction of all drug commerce, with the bulk of illicit activity still likely to take place using offline communication. It seems reasonable to suggest, however, that this situation will not necessarily remain the case for long. Revenues are very hard to estimate. According to Christin (2014), the billion-dollar amounts alleged in the criminal complaint regarding the shutdown of Silk Road in October 2013 (Barratt et al., 2014) are highly inflated as a result of erroneous conversion rates between bitcoins and US dollars. In their more recent study, Soska and Christin (2015) suggest that total volumes of sales during the three years they were monitoring dark web markets averaged around USD 300 000 to USD 500 000 a day.

Global versus national markets

Although the internet offers a virtual global marketplace, with the increased accessibility this brings, geographical place remains important to buyers and sellers. It appears that selling internationally is not the norm. Although internet markets have global reach, national characteristics still have a significant impact. Many buyers prefer home sellers, perceiving less risk with fewer borders to cross. It appears that most US and Australian vendors on Silk Road were not willing to ship drugs across international borders, and Australian buyers preferred local sellers. After Silk Road closed, a new Finnish marketplace was established on the deep web to cater for national customers. Exceptions include when overseas markets provide access to different products or higher-quality goods or offer price advantages to buyers and sellers. Sellers may run the increased risk of shipping products abroad when there is a lot of competition on the home market or where the home market is considered unsafe or vulnerable to police infiltration.

Results presented by the I-TREND project team in Chapter 10 show that the preference for national markets also holds true for new psychoactive substances sales. Although online shops may target two or more countries, it is more likely that an online shop will be aimed at one country and has logistical operations in the same country. This finding suggests that the distribution of online shops among different categories could be related to cultural factors; product choices also appear to be linked, to some extent, to country and cultural preferences for particular substances.

Finally, there are evidently certain global trends expressed within 'local' online subcultures or communities. These loosely affiliated groups may centre on discussion forums or social media sites. Many deep web markets do not operate in isolation, but tend to be accompanied by user forums and discussion boards which allow peer-to-peer information and expertise exchange and contact. This publication has identified, for example, virtual social networks of men who have sex with men engaging in chemsex; the early Silk Road 'libertarian' community; the product-testing LSD Avengers; and forums for psychonauts exploring the effects of research chemicals and new psychoactive substances.

Security measures and regulatory mechanisms

A central challenge for dark net markets is the instability associated with their functioning. This is primarily a reaction to threats of market disruption from external sources, in particular law enforcement infiltration, but also to internal scams and risks. As highlighted within

this publication, these marketplaces are relatively transitory and unstable entities. They are also unique in particular in the combination of a number of 'security measures' that increase possibilities for relative anonymity: the use of cryptocurrencies (bitcoin), encryption (PGP) and secure web hosting (Tor). They also tend to integrate a set of regulatory mechanisms to support financial security: escrow services, reputation and feedback systems, use of digital contracts (e.g. Alphabay) and dispute adjudication. Finally, in order to try and ensure safe delivery of goods, stealth packaging is used to conceal products.

Market trader scams and police takedowns also act as a catalyst for new security developments. New markets have sought to combat rogue operators through the use of multi-signature escrow, which requires a second key from the buyer or seller to access the money. Increasingly, sites are not open access but require invitation from a member and the use of a guest code or URL. In Chapter 3, Lewman suggests how markets are likely to further evolve in a bid to evade law enforcement infiltration, with the decentralised OpenBazaar marketplace offering a potential model. This involves distributing the transactions of the e-commerce software throughout all participants in the market using the basics of the bitcoin block chain. This creates the potential for a fully distributed marketplace spread across millions of computers around the globe, with each computer handling only a part of the marketplace, and leaving no single server vulnerable to takedown.

Trafficking and supply reduction challenges

An important question raised in this publication is the extent to which the internet provides new criminal opportunities for drug trafficking. As discussed above, there are certainly indications that, in some circumstances, dark net markets may be used more by suppliers for wholesale purchasing than by consumers at a retail level. The extent of involvement of organised crime in online drug markets is unclear at present. However, if online drug trading offers significant threats or opportunities, there will undoubtedly be a presence. In Chapter 8, Van Slobbe makes an interesting point on this subject: currently, the percentage of the drug trade that takes place on the dark net is too limited to affect the profits of the larger organised criminal groups. However, if cryptomarket turnover and profit potential were to rise substantially, then organised crime would undoubtedly enter the marketplaces. Given that criminal groups already use private servers and protected networks for communicating within the group, a move into deep web markets represents no technological challenge.

Although marketing and sales activities may take place online, in terms of trafficking flows there remains a physical component in internet drug-dealing activities, primarily at the cultivation/production stage and at the distribution stage (e.g. postal systems may be involved). Criminals are exploiting legal loopholes, for example taking advantage of differences in national regulation. Postal systems are seen as the major bottleneck of the system, as the substances sold still need to be delivered through the (inter)national mail system. We note the growth of stealth packaging in this context — and the fact that online suppliers' reputations are linked to their creativity in concealing purchases.

This publication highlights a number of conundrums for law enforcement: their activity, for example, in infiltrating and taking down markets on the deep web can have undesirable effects. This includes both the 'balloon effect', in terms of scattering market activity, and the driving of more sophisticated encryption software and concealment activities. It is also interesting to consider what drug sources online markets replace and, if internet markets are closed, removed or seized, what drug sources people use instead.

The buyer's perspective

A number of studies cited in this publication have explored reasons why experienced drug users choose to use online drug markets rather than conventional sources of supply. Among this population, recurrent themes include easy accessibility, availability of their drugs of choice and good quality of products. Main factors hindering use include the need for a certain level of technical competence and fear of financial scams.

The 2015 Global Drug Survey provides further insight on this issue with an analysis of respondents who reported making web purchases of drugs ([3]). These results shed light on buyers' considerations when comparing purchasing drugs in dark net markets with buying from alternative sources. Respondents were asked to report the problems they had experienced both with dark net markets and with the alternative sources of drugs that they would use if they did not have access to those sites.

([3]) Available at http://www.globaldrugsurvey.com/the-global-drug-survey-2015-findings/

The results show that buyers found the dark net to be safer than their alternative sources in terms of fewer experiences of threats and violence. They were also less likely to experience receiving products not containing the expected substance. However, dark net users were more likely to report losing money as a result of theft, seizure of drugs by authorities or exit scams, in which site administrators disappear with money being held in escrow on their sites.

Harm reduction opportunities

In addition to supporting drug markets, both the surface and deep web offer new ways for drug users to access help, and potentially to reduce barriers to help seeking. There exist drug user harm reduction communities through drug forums on the surface web. These, for example, circulate warnings about pills with dangerous content, and the sharing of information in forums could potentially deter users from buying certain drugs. Studies presented here on Silk Road suggest this dark net market offered certain benefits to users when compared with street-based drug marketplaces. Examples include the abovementioned sale of high-quality products with low risk for contamination, vendor-tested products, trip reporting and online discussions on harm reduction with resources for people who wish to reduce their consumption (Barratt et al., 2013; Van Hout and Bingham, 2013, 2014). Barratt et al. conclude that Silk Road contributed positively to harm reduction, by helping users to make informed decisions and enabling them to access relevant information more comprehensive than was available elsewhere. 'DoctorX' provides harm reduction advice at point of sale and, in Chapter 7, gives concrete examples of his work with dark net market users offering drug-related information, advice and harm reduction services. Nevertheless, the rapid turnover of markets make them an insecure longer-term platform, and the limited number of dark net marketplaces in existence means the space for large-scale input from web outreach workers and health service personnel is probably limited.

Researching online markets

As pointed out by Aldridge and Décary-Hétu in Chapter 2, our understanding of internet drug markets has to a large extent been informed by investigative journalists and bloggers, with the body of academic research literature, at least in the area of dark net markets, lagging somewhat behind. Nevertheless, despite their associations with secrecy, it seems that, from a research perspective, these markets are a relatively visible phenomenon. In many respects, we now have more information than was previously available on illicit drug markets, and covering many angles. The existence of a defined marketplace, Silk Road, has assisted with this. As dark net markets become more decentralised and diffuse, they will undoubtedly become more difficult to monitor, research and understand. In fact, the current challenges associated with monitoring the complex surface web markets demonstrate this. And important questions remain. Does the monitoring of online shops and the products they offer actually reflect what is available to users on the market? In this respect, it is important to bear in mind that the offer of drugs for sale does not necessarily equate with supply in these online markets and that, from a research perspective, the association between offer and availability is not known. Potential rich sources of information are drug user forums, which have the ability to provide insight into what substances are being used by whom. It is possible that enhanced monitoring in this area may better predict and inform about market changes and trends. Like online markets themselves, drug forums provide access to a larger population of drug users than was previously accessible to researchers. The qualitative information gained from these forums can be rich in itself and can also inform further quantitative research.

A range of new methodological issues arise with regard to researching the web. In some respects, this opens up the potential for a golden age of ethnographic research, accompanied by innovative developments in online research methodologies such as netnography and infodemiology. It also brings with it the requirement for new ethical considerations, as highlighted by I-TREND's forum monitoring. The recent opening up for public use of a database of over 80 dark net markets by Gwern Branwen ([4]) has increased substantially the potential opportunities for academic research and understanding of dark net markets. It is likely that this will be a rich source for studies in future years.

Questions for future research

Throughout this publication, authors have raised issues that they consider to be important for future research. In a number of areas, the absence of a body of scientific evidence hampers our ability to make valid conclusions on market dynamics and function. This is particularly true for the online sale of medicinal products and for our

([4]) http://www.gwern.net/Black-market%20survival

understanding of the role of social media and apps in the demand for and supply of illicit substances. At present, there is very limited evidence on the role of social media in drug supply, and the limited knowledge and vastness of social media platforms suggest that this is an important area for further study.

A number of relevant queries have been raised about drug markets. Above all else, markets are rational entities and a central question raised by the evidence is whether or not online markets (all types) are challenging established ones and, if so, where they have a competitive advantage. Christin (2014) asks whether deep web markets primarily displace drug purchases from traditional markets or provide access to drugs for those without previous access. It is also important to get a better understanding of how the online offer of drugs affects use and consequences. Do people purchase more when they buy online and what effect does that have on use? The impact may differ for different types of drug user and for different substances; for some substances, such as new psychoactive substances, the internet may have played a central role in the evolution of the trade. Exploring its impact may contribute to a wider understanding of the factors that impact on drug markets.

There is also clearly a need to better understand the net harm/benefit of dark net markets. In particular, as some commentators suggest, the extent to which harm might actually be reduced by dark net markets requires systematic empirical research.

From the perspective of drug supply, it is interesting to further assess whether or not the individuals who sell on dark net markets fit the same profile as street dealers. Or are drug vendors on the deep web, the so-called new criminal entrepreneurs, completely different from street dealers? Or have street dealers switched to the online markets and, if so, what advantages did they expect and gain from this switch?

We can ask similar questions about the buyers. Did the people who are now buying drugs over the deep web previously buy drugs in the traditional way, or did they start buying drugs because of the ease of buying them over the deep web, which entails fewer risks? Is the profile of these buyers similar to the profile of drug buyers in the traditional market?

Latest market trends and developments

As is now well known, in October 2013, the FBI shut down the original Silk Road and arrested its founder, Ross Ulbricht, known as 'Dread Pirate Roberts'. A new version of Silk Road (Silk Road 2.0) was launched on 6 November 2013. On 6 November 2014, Interpol announced the closing down of 400 deep web sites, including Silk Road 2.0. However, the number of sites detected had almost returned to previous levels by April 2015. Other websites have been closing down since, supposedly trying to evade arrest, and taking the bitcoin money stored in their accounts ([5]). The most well-known instance was the disappearance of the Evolution marketplace; in March 2015, the administrators of this site disappeared with the equivalent of more than USD 12 million (GBP 8 million). In May 2015, Ross Ulbricht was sentenced to life in prison in the United States, and ordered to forfeit USD 183 million. In August 2015, Agora ceased trading due to security issues; at the time, it was the largest marketplace trading on the deep web.

Conclusions

This analysis has highlighted a number of significant new trends in the fast-changing world of internet drug markets. Authors in this publication highlight a tendency towards decentralisation of dark net market structures and activities. Dark net markets are seeing a move to more covert communication and sophisticated encryption techniques, in part as a response to the cat-and-mouse game of avoiding detection by law enforcement. Similarly, we have noted the growth of multi-signature escrow and rating systems to try and ensure financial trust and security for buyers in the wake of recent scams.

The internet facilitates movement of products, money and information across global borders. It also allows the movement of drugs, new psychoactive substances, precursors, medicines and information on production techniques. Social media play a role in facilitating interaction, advertising and marketing drugs, in addition to providing sales forums, shop access via apps, and

([5]) See https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/

classified ads. The dividing line between surface websites (e.g. selling so-called legal highs) and cryptomarkets seems to be increasingly blurred, as one level can increasingly provide access to another. At present, the extent of internet-enabled drug transactions taking place on the deep web is very limited; however, growth has been exponential and there is no evidence to suggest these markets will remain restricted for long. Online new psychoactive substance markets and dark net markets have certain things in common. Both are extremely dynamic and characterised by the closing and opening of new sites. In both surface and dark net markets, suppliers may use strategies that promote maximum internet visibility — for example through spamdexing practices, which help them to appear at the top of search engine results — or, alternatively, they may choose a discreet, targeted presence often using argot.

In Chapter 2, Aldridge and Décary-Hétu explain how in recent years many drug markets have moved from 'open' to 'closed', in which drug dealers sell only to those customers with whom they have trusted relationships. They describe how dark net markets have reversed this trend, opening up marketplaces that allow sellers to transact with anonymous customers whom they only meet in the virtual sphere (Aldridge, 2012; Aldridge and Décary-Hétu, 2014). We would suggest that, after a brief period of operation, recent trends suggest that dark net markets may once again be moving from open to at least partially closed as a result of scams and takedowns. This has been manifested in the recent restrictions placed on market entry, such as the need for invitation from an existing member. Another sign of market closure has been cited: in some cases, users have formed relationships with their favourite suppliers, enabling them to make private transactions via secured email, bypassing the dark net markets altogether.

To date, it appears that buyers and sellers adjust rather easily to dark net market takedowns, in a similar way to buyers and sellers using surface web stores: when one shop closes, others quickly appear to replace them. This resilience to both law enforcement takedowns and exit scams is also noted by Soska and Christin (2015). However, as noted, most dark net markets tend to have a fairly short life, with their longevity hampered more by scams than by law enforcement intervention. The longer-term impact on buyer trust and vendor reputation may yet slow down or stall what, to date, has been exponential growth. Nevertheless, as highlighted by Van Buskirk et al. (2013), the speed with which the internet allows transformation to occur in drug markets will continue to present major challenges across the board, to law enforcement, public health and research and monitoring agencies.

References

Aldridge, J. (2012), 'Dealers in disguise: the virtualisation of retail level drugs markets', http://www.youtube.com/watch?v=q4ZsNuC2kqg

Aldridge, J. and Décary-Hétu, D. (2014), 'Not an "eBay for drugs": the cryptomarket "Silk Road" as a paradigm shifting criminal innovation'. Available at: http://ssrn.com/abstract=2436643 or http://dx.doi.org/10.2139/ssrn.2436643

Barratt, M. J., Ferris, J. A. and Winstock, A. R. (2014), 'Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States', *Addiction* 109, pp. 774–783.

Barratt, M. J., Lenton, S. and Allen, M. (2013), 'Internet content regulation, public drug websites and the growth in hidden Internet services', *Drugs: Education, Prevention, and Policy* 20, pp. 195–202.

Buxton J. and Bingham T. (2015), *The rise and challenge of dark net drug markets*, Policy Brief 7, Global Drug Policy Observatory, http://www.swansea.ac.uk/media/The %20Rise %20and %20Challenge %20of %20Dark %20Net %20Drug %20Markets.pdf

Chen, C., Asoni, D. E., Barrera, D., Danezis, G. and Perrig, A. (2015), 'HORNET: high-speed onion routing at the network layer, cryptography and security', http://arxiv.org/pdf/1507.05724v1.pdf

Christin, N. (2014), 'Commentary on Barratt et al. (2014): steps towards characterizing online anonymous drug marketplace customers', *Addiction* 109, pp. 784–785.

Dolliver, D. S. (2015), 'Evaluating drug trafficking on the Tor Network: Silk Road 2.0, the sequel', *International Journal of Drug Policy* 26, pp. 1113–1123.

Martin, J. (2013). 'Lost on the Silk Road: online drug distribution and the "cryptomarket" ', *Criminology and Criminal Justice* 14, pp. 351–367.

Soska, K. and Christin, N. (2015), 'Measuring the longitudinal evolution of the online anonymous marketplace ecosystem', *Proceedings of the 24th USENIX Security Symposium*, 12–14 August 2015, Washington DC, https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska.pdf

Van Buskirk, J., Roxburgh, A., Bruno, R. and Burns, L. (2013), 'Drugs and the Internet (No. 1)', *NIDIP Bulletin*, National Drug and Alcohol Research Centre, Sydney, pp. 1–11.

Van Hout, M. C. and Bingham, T. (2013), ' "Surfing the Silk Road": a study of users' experiences', *International Journal of Drug Policy* 24, pp. 524–529.

Van Hout, M. C. and Bingham, T. (2014), 'Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading', *International Journal of Drug Policy* 25, pp. 183–189.

Glossary

Block chain is a transaction database shared by all nodes participating in a system based on the bitcoin protocol. A full copy of a currency's block chain contains every transaction ever executed in the currency. https://en.bitcoin.it/wiki/Block_chain

Chemsex refers to sex while on various drugs, such as mephedrone, methamphetamine, cocaine; 'slamming' refers to the injection of these and other drugs by gay men/men who have sex with men in the context of chem sex parties.

Cryptomarkets are anonymous drug markets located in the dark web and accessed via Tor (see later). A cryptomarket can be defined as an online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities. It is not necessarily a site for the commission of cybercrime, as legal exchanges may also be conducted in such a forum (Martin, 2013, p. 356).

The **dark web** or **dark net** may be defined as a small portion of the deep web that has been intentionally hidden and is inaccessible through standard web browsers. This is the portion of the internet most widely known for illicit activities, because of the anonymity associated with this network.

The **deep web** is a part of the internet not accessible to conventional search engines; the only way to access the deep web is by conducting a search within a particular website; for example, government databases and libraries contain huge numbers of deep web data.

A **distributed hash table** (DHT) is a class of decentralised distributed system that provides a look-up service similar to a hash table; (key, value) pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key.

Doxing is the internet-based practice of researching and broadcasting personally identifiable information about an individual. This is a practice that drug sellers on the deep web can use to coerce or blackmail customers once they have obtained personal information (e.g. postal address) to make the shipment. At this point in the transaction, buyers have no guarantee that sellers will delete their data once the deal has been finalised.

Dread Pirate Roberts is the pseudonym used by Ross Ulbricht, alleged founder and former owner of the first Silk Road. He gained popularity due to his active involvement in forums, where he promoted his business model under a libertarian ideology. He was arrested following the shutting down of the website by the FBI in October 2013. He has been found guilty of several drug and criminal charges and was sentenced to life in prison in 2015.

An **eepsite** is a website hosted anonymously via I2P.

Escrow is a financial instrument held by a third party on behalf of the other two parties in a transaction. The funds are held by the escrow service until it receives the appropriate written or oral instructions or until obligations have been fulfilled. Securities, funds and other assets can be held in escrow.

Fiat currency is currency that a government has declared to be legal tender, but which is not backed by a physical commodity. The value of fiat money is derived from the relationship between supply and demand rather than the value of the material that the money is made of.

Garlic routing is a variant of onion routing that encrypts multiple messages together to make it more difficult for attackers to perform traffic analysis. Garlic routing is one of the key factors that distinguishes I2P from Tor and other privacy or encryption networks.

Hidden services are a feature provided by the Tor Browser that enables a user to anonymously host and browse content and services within a vast address space.

Internet forums are online discussion sites where people can hold conversations in the form of posted messages. Their structure is hierarchical: a forum can contain different sub-forums dedicated to different themes covering several topics or threads.

The Invisible Internet Project (I2P) is an alternative to Tor hidden services. It is an overlay network based on passing messages between routers using garlic routing with a distributed hash table for a global directory of available routers. All users of I2P are also running routers to pass encrypted traffic between other routers. A few cryptomarkets have recently started to use I2P as an alternative to Tor hidden services (O'Neill, 2013).

I-TREND was a European project co-financed by the Drug Prevention and Information Programme of the European Union, involving researchers from five European countries (the Czech Republic, France, the Netherlands, Poland and the United Kingdom). The project activities included monitoring online user forums and shops, conducting an online survey targeting users of new psychoactive substances, and analysis of samples and exchange of reference standards.

New psychoactive substances (NPS, also known as 'legal highs') are new narcotic or psychotropic drugs, in pure form or in preparation, that are not controlled by the United Nations drug conventions, but which may pose a public health threat comparable to that posed by substances listed in these conventions.

Off-the-record (OTR) is a method for encrypting instant messaging services, such as Google Talk, Facebook or Jabber. The software typically comes as a plug-in that is installed alongside another chat programme. This method of communication doesn't use the messaging system of a cryptomarket, but vendors may advertise their OTR contact details on a site.

Onion routing is a technique for anonymous communication over a computer network. In an onion network, messages are encapsulated in layers of encryption. The encrypted data are transmitted through a series of network nodes called onion routers, each of which 'peels away' a single layer, uncovering the data's next destination. When the final layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes.

OpenBazaar is an open source project to create a decentralised network for peer-to-peer commerce online. Each computer handles only a part of the marketplace, rather than everything being handled by one single computer or server. Use of Tor hidden services or I2P eepsites could be possible with this model, to further protect the identity and privacy of users involved in the marketplace.

Operation Onymous was a joint operation by US and European law enforcement agencies targeting the dark net that resulted in the shutting down of Silk Road 2.0 (and the arrest of its alleged administrator) and another 26 dark net websites in November 2014. The operation involved the police forces of 17 countries. In total, there were 17 arrests.

Operation Pangea is an operation that tackles the online sale of counterfeit and illicit medicines and highlights the dangers of buying medicines online. It brings together several law enforcement bodies from countries around the world including customs, health regulators and national police and includes the private sector. It started in 2008 and runs for a week on an annual basis. The last operation took place in June 2015 (Interpol, 2015) and resulted in 9.6 million fake and illicit medicines (worth more than USD 32 million) seized, 434 arrests and more than 11 800 websites shut down.

Pretty Good Privacy (PGP) is a data encryption and decryption computer programme that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, emails, files, directories and whole disk partitions and to increase the security of email communications.

Relays are computers that switch internet traffic from one computer to another before it reaches its destination. The Tor Network comprises around 7 000 of these relays.

Silk Road was a cryptomarket that operated as a Tor hidden service and used bitcoin as its exchange currency. Silk Road was the archetypical cryptomarket, being the most well-known and remaining the largest for a long period.

Spamdexing is the deliberate manipulation of search engine indexes. It involves a number of methods, such as repeating unrelated phrases, to manipulate the relevance or prominence of resources indexed in a manner inconsistent with the purpose of the indexing system.

The **surface web** or **clear web** or **clear net** is the internet that can be found by the link-crawling techniques used by a typical search engine such as Google, Bing or Yahoo. It refers to the unencrypted non-dark, non-Tor internet.

Tor (The Onion Router) is a free software that enables online anonymity by hiding a computer's IP address. The Tor Network is a group of volunteer-operated servers that allows people to improve their privacy and security on the internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organisations and individuals to share information over public networks without compromising their privacy. It has many societal benefits, such as enabling users to avoid censorship and allowing anonymous communication with victims of abuse, but it is also used for illegal matters, such as drug dealing.

A **virtual circuit** is a means of transporting data over a computer network in such a way that it appears as though there is a dedicated physical layer link between the source and destination end systems of these data.

Web 2.0 describes world wide web sites that emphasise user-generated content, usability and interoperability. Examples of Web 2.0 sites include social networking sites, blogs, wikis, folksonomies, video-sharing sites, hosted services, web applications and mashups.

HOW TO OBTAIN EU PUBLICATIONS

Free publications

one copy:
via EU Bookshop (http://bookshop.europa.eu)

more than one copy or posters/maps:
from the European Union's representations (http://ec.europa.eu/represent_en.htm);
from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications

via EU Bookshop (http://bookshop.europa.eu)

TD-XD-16-001-EN-N

emcdda

About the EMCDDA

The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) is the central source and confirmed authority on drug-related issues in Europe. For over 20 years, it has been collecting, analysing and disseminating scientifically sound information on drugs and drug addiction and their consequences, providing its audiences with an evidence-based picture of the drug phenomenon at European level.

The EMCDDA's publications are a prime source of information for a wide range of audiences including: policymakers and their advisors; professionals and researchers working in the drugs field; and, more broadly, the media and general public. Based in Lisbon, the EMCDDA is one of the decentralised agencies of the European Union.

About this series

EMCDDA Insights are topic-based reports that bring together current research and study findings on a particular issue in the drugs field. This publication describes how the proliferation of social media and development of web technologies have brought greater user interaction and have the potential to influence customer and user involvement in drug markets.

Publications Office

doi:10.2810/324608