European Monitoring Centre
for Drugs and Drug Addiction

EUROPOL

Drugs and the darknet

Perspectives for enforcement, research and policy








European Monitoring Centre
for Drugs and Drug Addiction

EUROPOL

Drugs and the darknet

Perspectives for enforcement, research and policy

2017

Legal notice

This publication of the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol is protected by copyright. Neither the EMCDDA, Europol nor any person acting on behalf of either the EMCDDA or Europol is responsible for the use that might be made of the following information.

More information on the European Union is available on the internet (http://europa.eu).

Luxembourg: Publications Office of the European Union, 2017

Print	ISBN 978-92-9497-241-5	doi:10.2810/834620	TD-04-17-834-EN-C
PDF	ISBN 978-92-9497-240-8	doi:10.2810/783427	TD-04-17-834-EN-N

Reproduction is authorised provided the source is acknowledged.

© European Monitoring Centre for Drugs and Drug Addiction, 2017
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

© Europol, 2017
The Hague, the Netherlands
File No: EDOC# 918590
Publications: https://www.europol.europa.eu/publications/

Credits for cover photos (from left to right): © iStockphoto (photos 1, 2 and 4); IDC 2.0 Market (photo 3).

Recommended citation: European Monitoring Centre for Drugs and Drug Addiction and Europol (2017), *Drugs and the darknet: Perspectives for enforcement, research and policy,* EMCDDA–Europol Joint publications, Publications Office of the European Union, Luxembourg.

Contents

5 | Foreword
7 | Acknowledgements
9 | Executive summary

15 | CHAPTER 1
Key concepts

31 | CHAPTER 2
Global phenomenon — EU focus

51 | CHAPTER 3
Law enforcement perspectives

67 | CHAPTER 4
Conclusions and recommendations

73 | References
77 | Glossary
81 | Annex 1
83 | Annex 2
85 | Abbreviations

Foreword

Illicit trade on darknet markets is one manifestation of the increasingly complex nature of transnational organised crime in the European Union (EU). Darknet markets, also known as cryptomarkets, provide a largely anonymous platform for trading in illicit goods and services. Drugs are estimated to account for around two thirds of darknet market activity. Almost any type of drug is accessible to buyers with basic technical understanding within a few clicks, including new psychoactive substances. This development poses a significant threat to the health and security of citizens and communities across the EU.

This report summarises our current understanding of the functioning of darknet markets and outlines potential countermeasures for policymakers and law enforcement professionals engaged in the fight against this phenomenon. Our point of departure is a review of the threat we face in this area, bringing together the latest findings from international research, fresh empirical data, operational information and intelligence. This analysis provides us with the opportunity to identify priority areas for targeted actions, and leads us to the conclusion that Europe needs greater investment and continuous innovation, if we are to keep pace with the challenges we face in this area.

For this report, the EMCDDA and Europol have combined the latest available data and outlined law enforcement strategies to reduce criminal opportunities in the darknet ecosystem. We present a multidisciplinary analysis of how darknet markets function and how they relate to criminal behaviour. We explore the implications of this for drug control policies, research and monitoring approaches, and law enforcement activities. We would like to particularly acknowledge the input from experts in academia and law enforcement officials, without which this report would not have been possible.

This analysis is timely, following the recent takedown, in July 2017, of Alphabay and Hansa, two of the largest darknet markets. We can learn from this achievement, while at the same time recognising that those involved in the online trade in drugs are likely to be quick to adapt and develop new strategies and business models to reduce the risk of detection. This means that on-going research, monitoring and surveillance will remain critically important for both agencies. We believe that the new insights provided by this joint EMCDDA–Europol analysis will make an important contribution to informing and preparing Europe's response to the growing threat posed by darknet drug sales. The online trade in illicit goods and services has been recognised as a key threat to the safety of EU citizens in the SOCTA 2017 and is being tackled as part of the EU's coordinated response to serious and organised crime – the EU Policy Cycle for organised and serious international crime from 2018 to 2021. Our analysis is necessarily forward-looking, as the challenges we face in this area are constantly evolving. It demonstrates the added value of bringing together the analytical

expertise of both agencies, allowing us to approach the topic with scientific rigour and the informed perspective that comes from operational experience. Our successful partnership also underlines, in our view, one of the key messages running throughout this report: European-level cooperation and coordination are likely to be critically important for an effective response in this area.

Alexis Goosdeel
Director, EMCDDA



Rob Wainwright
Executive Director, Europol



Acknowledgements

This joint EMCDDA–Europol publication is based on a synthesis of information from a range of sources. The EMCDDA and Europol would like to acknowledge the work carried out by Nicolas Christin (Carnegie Mellon University, USA), which has informed parts of this publication. This work was made possible by original funding from the United States Department of Homeland Security Science and Technology Directorate, Cyber Security Division.

We would like to highlight the contributions of the many partners, in EU Member States and outside the EU, who have contributed data to this report and continue to work closely with the EMCDDA and Europol to counter the trade in illicit drugs online. We would particularly like to thank the European Commission for its continued support.

We would also to like to acknowledge the insightful input we have received from experts and members of the EMCDDA Scientific Committee, who have made an invaluable contribution to this analysis. A full list of acknowledgements can be found in Annex 2 of this report.

Executive summary

Report background and context

Developments in information technology are transforming many aspects of modern life and this includes the way that illicit goods are traded. This report focuses on online anonymous markets (or 'cryptomarkets'). Such markets are a relatively recent development that enables sellers and buyers to transact online without disclosing any personal details, hence creating a considerable degree of anonymity. This development has led to the proliferation of the trade in illicit goods online, and it is now recognised as a growth area for the activities of organised crime in the European Union (EU) that is undermining conventional law enforcement approaches. It is estimated that about two thirds of the offers on darknet markets are drug related, with the remainder related to a range of other illicit goods and services. However, any analysis has to be made with caution because of not only the difficulties inherent in monitoring developments but also simply the pace of change in this extremely dynamic area.

Europol's 2017 European Union Serious and Organised Crime Threat Assessment (EU SOCTA) identified the online trade in illicit goods and services as one of the engines of organised crime. An improved intelligence picture and a coordinated law enforcement approach across the EU in addressing criminality on the darknet are now at the heart of the EU Policy Cycle for organised and serious international crime (2018-2021). This has been reflected in law enforcement approaches, as illustrated by two recent significant coordinated international law enforcement operations on two of the largest darknet markets.

Structure of the report

This report has three main chapters. The first reviews the key concepts necessary to understand the development of darknet markets. The second chapter highlights the growing importance of this area for drug sales within the EU through the presentation of an analysis of market activity. This includes an analysis of drug supply on global darknet markets (2011-2015). The analysis focuses on drug supply originating from the EU, and includes an assessment of the relative significance of EU suppliers in both the global darknet drug trade and the overall European retail drug market. This second chapter then also considers non-English language darknet markets for specific European countries, before providing an analysis focused on AlphaBay — one of the largest markets to have existed thus far — from its original emergence to its recent closure (2015-2017). In the third chapter, the darknet phenomenon is reviewed from a law-enforcement perspective. Not only are the challenges for law enforcement elaborated, but examples of successful recent actions are also provided, which are useful for informing discussions on future interventions in this area. Taken together, this analysis provides a comprehensive but accessible policy-orientated review, intended to facilitate discussions at EU level on how to respond to the growth of darknet drug markets. This is accompanied by the identification of key priority areas that require attention and where activities are likely to have most impact. When interpreting the findings from any analysis of this topic, the considerable difficulties of collecting data on an area of activity that is, by definition, designed to remain hidden needs to be borne in mind. Notwithstanding this, some key findings and recommendations for action emerge from this report.

Understanding the threat

All markets, including illicit ones, function to facilitate the exchange of goods or services. Therefore, markets will prosper if they confer advantages to both buyers and sellers. Considerations for consumers can include the level of choice, ease of availability, convenience, perceived quality and price. For illicit drug markets, the level of risk is also an important factor, as vendors and consumers will be attracted to markets that are associated with relatively low risks of detection, experiencing market-related violence and 'rip offs'. Darknet markets provide a convenient sales channel to technologically knowledgeable customers. This approach to drug sales appears to have considerable potential to grow. It is possible that darknet markets will disrupt traditional drug markets in the same way as has been seen in some areas for legitimate commodities. This is especially likely to occur if darknet markets become more accessible to new consumers and are viewed as a relatively low-risk way of acquiring drugs.

Importantly, such changes will not occur in isolation but will be influenced by other developments in the illicit drug market. These may include the potential use of other technologies and platforms; the overall impact of law enforcement and regulatory efforts; and broader social and policy developments which may shape the supply of and demand for drugs in more general ways. The need to keep pace with changes in this area is illustrated by the fact that, recently, evidence has emerged of the use of instant messaging and social media applications using GPS (global positioning system) technologies for drug distribution in some European cities. This underlines the need for the systematic monitoring and assessment of the anonymous online ecosystem, conducted in the context of understanding the operation of the illicit drug market overall.

A number of potential threats can be identified that may increase the challenges of responding to online-facilitated drug transactions. These include the development of decentralised software and new encryption technology; new forms of parcel delivery and collection systems; the greater integration of darknet markets with existing local drug markets; nationally based darknet markets; and the growing use of GPS-enabled apps for distribution at the local level.

Key findings

- The trade in illicit drugs on darknet markets is a dynamic area subject to rapid change as marketplaces appear and disappear. Overall, the importance of this area seems to be expanding and it now affects most EU Member States in some way.
- When compared with current estimates of the annual retail value of the overall EU drug market, sales volumes on darknet markets are currently modest, but are significant and have the potential to grow.
- EU-based suppliers are important players in the darknet ecosystem. In the 2011-2015 period, they accounted for around 46 % of all drug sales in terms of revenue on the darknet markets analysed.
- Between 2015 and 2017 on AlphaBay, which, at the time, was the largest darknet marketplace, EU-based suppliers accounted for around 28 % of all drug sales.
- In both study periods Germany, the Netherlands and the United Kingdom were the most important countries with respect to EU-based darknet drug supply. Stimulant drugs represented the majority of all European drug sales.

- New psychoactive substances (NPS) are less commonly sold than illicit drugs on the darknet market, probably reflecting the significant role played by surface web sales in this sector. The United Kingdom was the most frequently noted origin of NPS sales, which may reflect both patterns of demand and recent changes in legislation.

- The rationale underpinning darknet markets suggests that they will be most commonly used for mid- or low-volume market sales or sales directly to consumers. This is supported by the data presented here. Large-volume sales (wholesale) are relatively uncommon.

- The highest market activity in terms of number of transactions was observed at the retail level, and retail sales values were greatest for cannabis and cocaine. The picture was different for MDMA and opioids, however, where mid-level sales represented a relatively large proportion of all sales (although still less in absolute terms), and the value of the mid-level sales was greater than the value of the retail sales. This suggests that darknet markets may play a different role in the supply chain for these substances.

- Law enforcement interventions in the form of darknet market takedowns disrupt darknet markets, although the overall ecosystem appears to be fairly resilient with new markets quickly becoming established.

- Significant knowledge gaps exist with respect to the role of traditional organised crime groups (OCGs) in darknet markets. In particular, the extent to which OCGs are involved in the production, trafficking and distribution of drugs supplied on online markets is unclear.

Conclusions and recommendations

There are obvious methodological and practical difficulties that need to be taken into consideration in any analysis of darknet markets. Despite these limitations, the data presented in this report allow us to draw some conclusions that support recommendations for action. An important caveat here is that, as the pace of change is considerable in this area, any recommendations will require regular review. Conclusions and recommendations are grouped together according to their relevance to law enforcement practice, monitoring and research, and policy development. It should be noted that, while this approach is conceptually helpful, it results in some unavoidable overlap.

Law enforcement

- Established and proven intelligence-led policing approaches, conducted in a technologically coordinated and collaborative manner, are likely to be important components if law enforcement activities are to have a sustained impact.

- There is a need for capacity building and increased investment. EU Member States are often faced with significant skills gaps for conducting investigations on the darknet, and many authorities lack experts who have both a technical understanding of cybercrime investigation and expertise in operational drug-related crime activities. Capacity-building efforts in this area also need to consider the needs of the judiciary.

- The resilience of the online ecosystem to targeted market disruption and the scale and diversity of drug market activity mean that operational models appropriate for addressing

illicit firearms or crimes against children may not be directly transferable to, or sufficient for, tackling online drug supply.

- In order to prevent the displacement of activities to new or other existing marketplaces, authorities need to pursue a multi-agency approach to target the latter. In addition to targeting individual marketplaces, this implies the need to prioritise other high-level threats and/or targets (major vendors or their suppliers), engage with industry and develop other measures.

- Since a small number of vendors appear to be responsible for a disproportionately large volume of overall sales, specialist law enforcement tactics should prioritise investigations that will have the largest impact. This prioritisation should be done on the basis of predefined high-value, high-number, or high-risk transaction criteria following an intelligence-led policing approach. Identifying the origin of drugs sold on the darknet market is important for both targeting law enforcement efforts and a better understanding of overall market dynamics.

- Pooling capacity resources by, for instance, establishing darknet investigations units, joint operational international taskforces and coordinated actions such as cyberpatrolling is likely to improve efficiency and enhance the strategic understanding of the role of the darknet trade in drugs in serious and organised crime, as well as mitigating some of the investigative challenges in the field.

- The success of law enforcement operations against cyber-enabled crime often depends on the cooperation of technology industry actors. In this context, there is a need for standardised rules of engagement with private industry and the development of flexible cooperation models that can allow effective action while striking an appropriate balance between the interests of individuals, the general public and businesses concerned.

Research and monitoring

- There is a need to further increase and develop monitoring capacity to support the strategic analysis required to inform future policy and operational responses, and reduce both the health- and security-related threats deriving from the online supply of drugs and other illicit commodities.

- Existing early warning approaches may be limited to detecting changes in drug consumption once they have already been established. This can be improved by supplementing such systems with data and information on darknet drug market sales.

- There is evidence that drugs bought on the darknet are likely to be intended for redistribution or supply on local markets (based on revenue and transaction-size data). Further investigation should be conducted into the destination of drugs bought on the darknet.

- Research is needed to explore the interaction between traditional drug markets and darknet drug markets. This should include consideration of how consumers view these different marketplaces and their relative impacts on health risks and harm.

- Future research and monitoring activities should address national non-English-language markets — the study of such markets will improve understanding and provide insights into the interactions between traditional offline and darknet market drug flows and networks.

Policy

- Health and security issues related to drug markets are increasingly interlinked. This needs to be recognised, and synergies between relevant actors in EU Member States, EU institutions and relevant agencies need to be further developed to allow the development of more joined-up and integrated responses.

- The dynamic nature of online markets, their ability to evolve to respond to threats and exploit new opportunities, and the introduction or adoption of new technologies mean that enhanced monitoring capacity in this area is crucial to ensure that responses keep pace with new developments.

- In the light of the relative ease and convenience of the darknet as a sales channel, it is essential that measures are considered to prevent and discourage consumers from using online platforms for obtaining drugs. This will require the development of appropriate prevention and risk communication approaches.

- Existing legislation should be reviewed and, if necessary, adapted to provide a more harmonised legal environment — to equip the judiciary and law enforcement authorities with the tools they need to respond in a more coordinated manner to criminality on the darknet.

- The complex nature of criminality on the darknet requires a multi-agency and collaborative approach. At the European level, the EU Policy Cycle provides an important platform for achieving this.

- Engagement with key industries, such as the information technology, social media, payment services, and commercial product distribution and collection industries, is likely to be increasingly important for both identifying new threats in this area and developing effective responses.

- Engagement with the private sector and the research community is also likely to be increasingly important as a means of leveraging the expertise held outside the remit of law enforcement to identify new threats and combat the existing ones.

1

CHAPTER 1

Key concepts

This chapter outlines the scope and aims of the report. It introduces the key concepts and themes used throughout the chapters, including the online anonymous marketplaces and the various technologies at play.

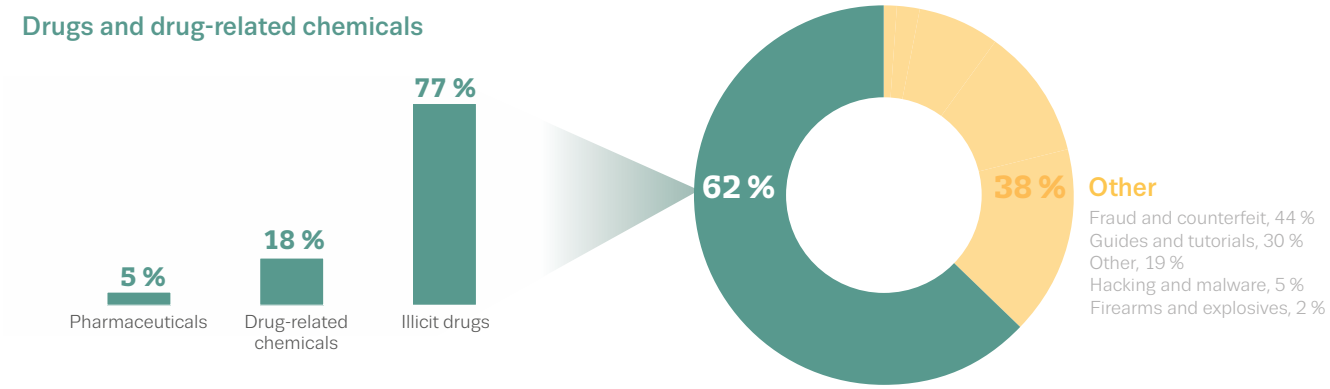
1.1 Scope and aims of this report

Illicit trade on darknet markets is recognised as one of the engines of organised crime in the European Union (EU). It is estimated that about two-thirds of the offers on darknet markets are drug related, with the remainder related to a range of other illicit goods and services (see Figure 1.1) ([1]).

This report focuses on online drug sales. More specifically, it examines sales that are carried out on an encrypted part of the internet called the *darknet*. It does not cover drug sales on the *surface web,* that is, the part of the internet that can be accessed through typical search engines such as Google and Bing. The darknet is part of the deep web, the part of the internet that is not accessible by standard web browsers, but is used for storing encrypted data such as government files and personal banking records (EMCDDA, 2016a).

This report is intended to stimulate further discussion on the topic of drugs available on online anonymous markets by providing a conceptual framework for understanding the key components, empirical sales data with an EU focus and additional, new market analysis. It sheds light on the darknet markets and highlights some of the implications for the EU, as well as addressing the challenges they pose for policy and law enforcement.

FIGURE 1.1
Darknet markets content



Source: Web-IQ (2017).

([1]) Based on active listings data from AlphaBay, Dream Market, Hansa, TradeRoute and Valhalla darknet marketplaces, spanning from the launch of each marketplace through to 21 August 2017 (or market closure). It should be noted that the number of listings is susceptible to manipulation to serve the purposes of the vendors or the marketplace.

1.2 Background

The very first online drug transaction is thought to have taken place in the early 1970s and involved cannabis exchange between students at Massachusetts Institute of Technology (MIT) and Stanford University (Markoff, 2005). Illicit drugs have therefore been sold on the internet in small volumes almost since its inception. Web-based discussion forums, related to drug use and manufacture, have also been present online since the late 1990s ([2]). It is only recently, however, that, fuelled by the global proliferation of powerful communications and encryption technologies, illicit drugs have become much more readily accessible online.

The earliest modern online anonymous markets, often referred to as *darknet markets* (Owen and Savage, 2016) or *cryptomarkets* (Martin, 2014), appeared in early 2010 (see Figure 1.2), and evolved from an encrypted email service and migrated on to a Tor (The Onion Router) anonymity network to guarantee better anonymity to users (Schwartz, 2012).

A number of key terms used in this report are explained here, and a more elaborate glossary of terms is provided at the end of the report.

1.3 Darknet markets

Darknet markets consist of websites, which are in many ways similar to other online platforms that facilitate trade, such as eBay or Amazon. The key difference is the anonymity afforded by accessing darknet markets. Access to such markets can be achieved in a number of ways. Commonly, there are surface websites that provide listings of '.onion' addresses for darknet markets, thus enabling ready access; there are also mirror sites on the surface web that provide hyperlinks to corresponding hidden sites; and there are 'invitation-only' markets where users need to be referred by a current user (see Figure 1.2). Among the technologies used to achieve this are anonymisation services, encrypted communication services and cryptocurrencies, each one of which mitigates the risk of detection of the buyers and sellers and presents its own particular challenges to investigators.

The first darknet market of notoriety was Silk Road, which opened at the end of January 2011 and was seized by the US Federal Bureau of Investigation (FBI) in October 2013 (DEA, 2013). Silk Road 2.0 was launched soon after the original Silk Road was seized and since that time there has been a proliferation of darknet markets, with an estimate of over 100 markets having emerged to date.

Markets close for a number of reasons. Based on an analysis of the closure of 89 online marketplaces, the most common reason for closure thus far is a so-called 'exit scam', where the market operators close the site down suddenly, taking the money held in escrow without fulfilling the orders (n = 31). The next most common reason for closure is 'voluntary exit', where the market is closed with the mutual consent of those involved and without known losses to users (n = 24). Law enforcement may also decide to target markets and close them down (n = 14). Finally, a market closure may be precipitated by a hack or as a result of de-anonymisation (n = 11). For 2 of the 89 marketplaces studied, it could not be established, based on the available sources, whether the closure occurred as a result of a scam or a hack, and in 7 cases the reason is unknown (Figure 1.2).

On average, the darknet markets observed (n = 103) remained active for just over eight months (8.5 months ± 10.1 months). The most enduring markets (n = 3: Valhalla, Dream Market and Outlaw Market) operated for a mean of just under four years (43 months ± 2.0 months). Nine marketplaces (Silk Road, AlphaBay, Silk Road 3.0, Black Market Reloaded, T•chka, Diabolus/SR3, The Farmer's Market, Darknet Heroes League and Crypto Market) lasted for a period of between two and three years (28.4 months ± 2.8 months), and a further group of 13 marketplaces (Hansa, Agora, Nucleus Marketplace, TheRealDeal, Acropolis, Middle Earth Marketplace, Apple Market, BlackBank Market, House of Lions Market, Evolution, Silk Road Reloaded, Silk Road 2.0 and Anarchia) lasted for between one and two years (16.2 months ± 3.2 months). The majority of marketplaces (n = 78) did not last more than a year — the average duration in this group is just under four months (3.8 months ± 3.5 months). In this latter group, 14 marketplaces were operational for less than one month. No start date could be determined for the OW Market and it was therefore not included in the analysis.

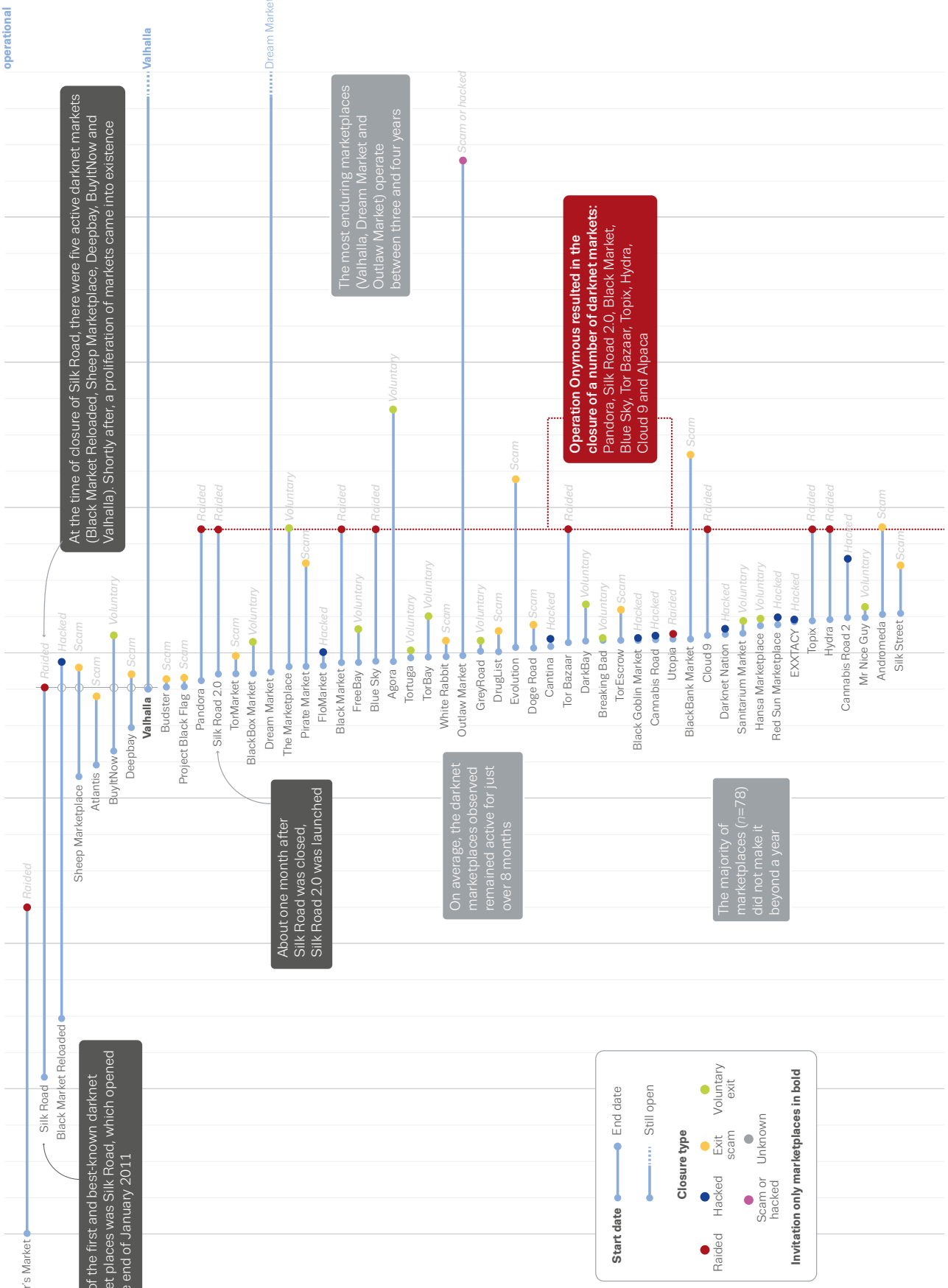
At the time of writing, there appeared to be 14 active and operational marketplaces (Valhalla, Dream Market, Silk Road 3.0, T•chka, Darknet Heroes League, Apple Market, House of Lions Market, TradeRoute, Wall Street Market, RSClub Market, Zion Market, Infinite Market, CGMC and OW Market) — these have been in existence for between 2 and 45 months (mean 18.3 months ± 14.8 months).

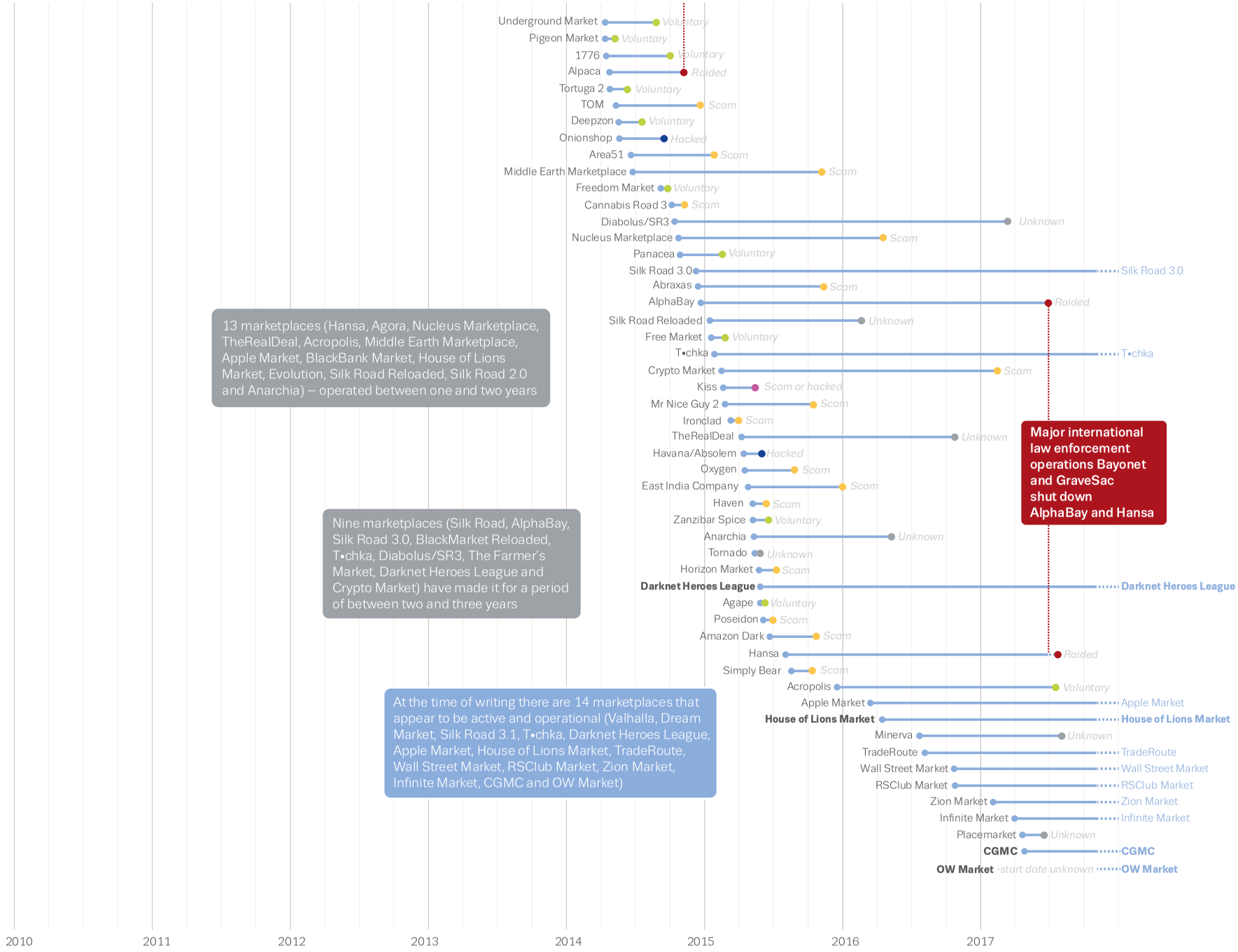
([2]) The Hive is one of these earlier forums: https://the-hive.archive.erowid.org/ (accessed on 19 September 2017).

FIGURE 1.2

Darknet markets ecosystem

Lifetimes of a selection of over 100 global darknet markets offering drugs, sorted by when a market opened and categorised by how it closed





Notes: A total of 103 darknet markets were identified along with key features. Start and end dates — the date of the first and last known sales/withdrawals (no start date could be determined for OW Market). Closure type — the reason for a market shut-down. Market status last checked on 28 June 2017 (except for AlphaBay and Hansa, for which data and information were updated to reflect closure on 4 July 2017 and 20 July 2017 respectively).
Sources: EMCDDA (2016a); DarkNet Stats (2017); DarkWebNews (2017); DeepDotWeb (2017); Gwern Archives (2017); Reddit (2017).

What drugs are offered on the darknet?

Once the darknet has been accessed using Tor software, it is possible to use the built-in search engine capabilities to browse the items offered. The format of the Google search engine has been appropriated in the form of *Grams*, a well-known search engine associated with finding illicit goods and services (see box on page 21).

With regard to looking at the drugs on offer, each marketplace lists the categories of substances in its own way. This is typically by category of drug, such as stimulants or opioids, though categorisation may not be systematic. For example, in the opioids category, other relevant drug types such as benzodiazepines may be listed. In some cases, categories have been intentionally misdeclared to promote them to users of other drugs (Duxbury and Haynie, 2017) or perhaps even to prevent drawing the attention of law enforcement. New psychoactive substances (NPS) appear to play a relatively minor role in the darknet drug market when compared with their presence on the surface web (Dolliver and Kuhns, 2016; Roxburgh et al., 2017). The level of retail transactions for NPS on the surface web is expected to be far greater than on the darknet (Van Buskirk et al., 2017a; Van Hout and Hearne, 2017; Wadsworth et al., 2017).

Currently, it would appear that precursors are not traded significantly on the darknet. This may reflect the fact that most precursor trading is conducted through established, existing links between organised crime groups (OCGs). Alternatively, it is also possible that some unregulated pre-precursors are sourced from commercial chemical websites in a similar way to that seen for some NPS. Given the potential for precursor availability to impact on drug manufacture, particularly in the area of synthetic drug production, it is important to monitor this area closely.

The legitimate use of anonymisation services

In addition to their illicit functions, there are valid uses for anonymisation services. The origins of Tor, the most prominent network supporting cryptographically hidden sites, can be traced back to the early 1990s and the US Naval Research Laboratory and, subsequently, to a collaborative project between independent developers and the non-profit organisation Free Haven Project (Dingledine et al., 2004). The intention was to provide anonymous access to the internet in politically repressive regimes.

These services are legal to download and there are legitimate reasons for using them. It is estimated that about 3-6 % of overall Tor traffic involves hidden services ([1]). As of May 2017, there were about 2 million daily Tor users and around 5 000 hidden services ([2]). It is difficult to estimate what proportion of hidden services on Tor relate to some form of illicit activity; however, one study indicates this to be more than half (Moore and Rid, 2016). The secrecy of these services, however, and the methodological challenges of monitoring this area make it difficult to reach accurate conclusions.

([1]) Recent assessments by the Tor Project gauge hidden-services traffic to constitute 3-6 % of the overall traffic in the Tor network. For a technical breakdown, see 'Some Statistics about Onions', Tor Project, https://blog.torproject.org/blog/33 (accessed on 16 June 2017).

([2]) Recent metrics by the Tor Project, available at https://metrics.torproject.org (accessed on 16 June 2017).

1.4 Dark techniques in the light

Anonymisation services

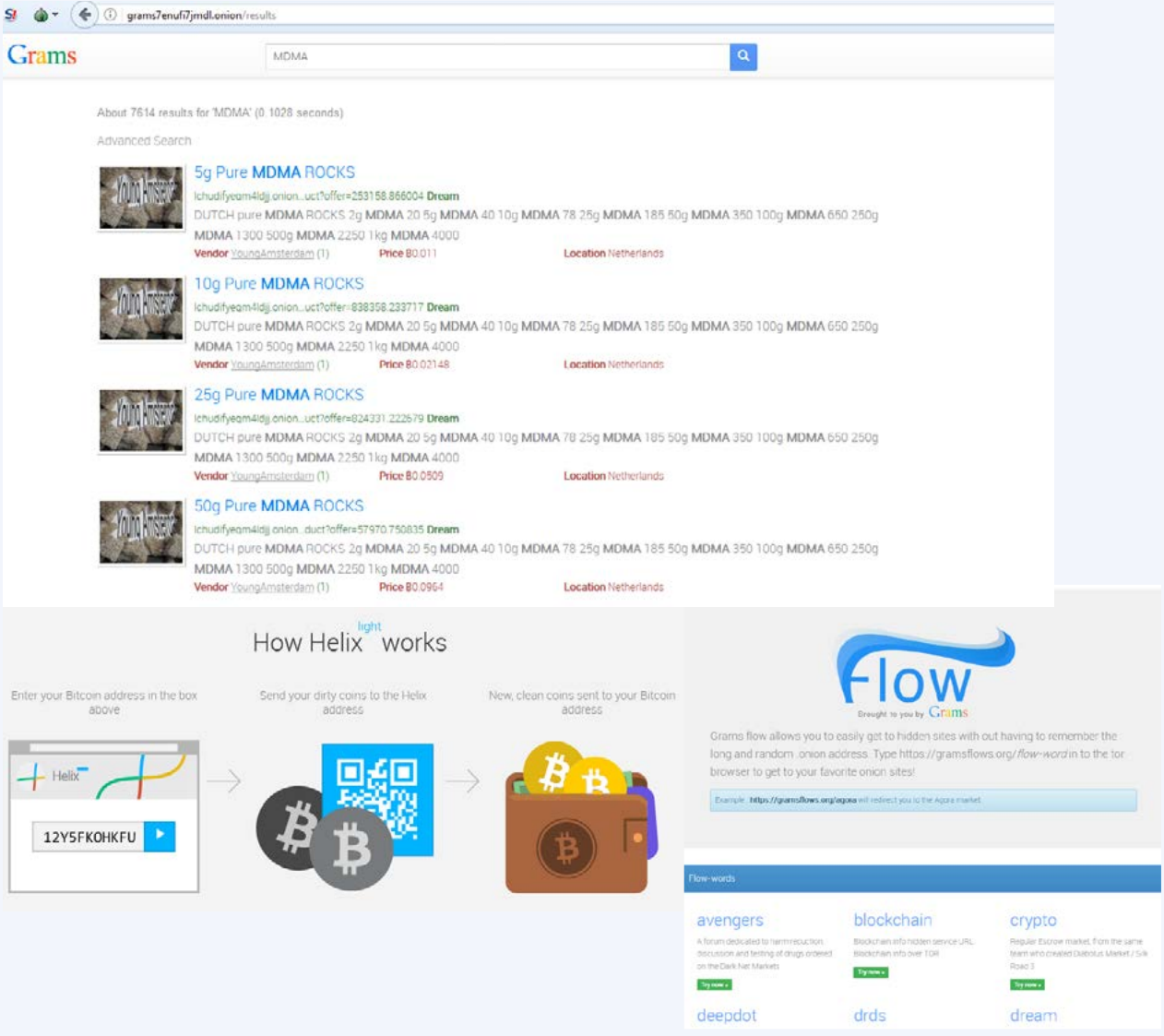
Anonymisation services enable aspects of internet activity to be anonymised, meaning that they allow users to browse the web without revealing their identity or location. They also allow content to be anonymously hosted by disguising where a server is located — a feature known as *hidden services* (Biryukov et al., 2013). Because of these features, darknet marketplaces can sell illicit products in a relatively open fashion, providing an illusion of anonymity to the users. While anonymisation services have to a large degree been misappropriated for illicit, often criminal, activity, this was not their original purpose (see box opposite) and there are many legitimate reasons for which individuals may wish to protect their anonymity online.

Grams website

Launched in April 2014, Grams was one of the first search engines for Tor-based darknet markets, designed to resemble and work in a similar way to surface web search engines.

Since its launch, Grams has been upgraded many times to improve the functionality and user experience. Features have been added to promote specific keyword or key phrase searches, to provide a bitcoin tumbling/mixing service, and to provide easy access to darknet markets through redirection and a network for publishers and advertisers.

Grams may be useful as a point of departure for general research on darknet markets, as it has a convenient and familiar, user-friendly interface, therefore potentially making the darknet more accessible.



Most commonly, darknet markets use Tor's hidden service model (Dingledine et al., 2004). Tor is free software that enables online anonymity using a process known as *onion routing*, which encrypts data and transmits them through a series of network nodes. Tor is, however, not the only software used for this purpose. There are also markets on I2P (the Invisible Internet Project) and other networks, although, currently, these networks are significantly smaller in scope and less popular than Tor (Everett, 2009). It should be noted again here that it is immensely difficult to accurately gauge darknet market sizes for numerous methodological reasons, including the fact that the metrics vary greatly, including traffic, users, relays and other features (Moore and Rid, 2016).

Other unique anonymising software packages, such as Freenet, have been around for a while. More recently, OpenBazaar has attempted to create decentralised markets, with potential support for anonymous communication. These efforts essentially implement anonymous peer-to-peer networks, which can be accessed via free downloadable applications. In this type of network, information is not stored on or transferred via centralised servers, but is encrypted and distributed to every computer on the network. The users do not know what files are stored on their computer, and files shared on the network are duplicated across several computers, ensuring that the content will be accessible if some devices become unavailable. This decentralised model poses further challenges to law enforcement, as there is no single server in a single jurisdiction on which to focus enforcement efforts.

Encrypted communication

Because of the illicit nature of the business conducted on online anonymous markets, many users decide to encrypt their communications. The most common message encryption programme used is PGP (Pretty Good Privacy). Created in 1991, it works with the use of 'pairs of keys', with each pair comprising a public key, used to encrypt messages, and a private key, used to decrypt them.

Essentials for encrypted exchange

To enable transactions to take place between a buyer and a seller without either being vulnerable, there are five crucial conditions that need to be met (based on Moore and Rid, 2016):

1. Privacy: the participants in the transaction need to be able to communicate without the risk of such communication being intercepted. In traditional postal mail, this can be achieved by placing the communication material in a sealed envelope. In virtual communication, participants use cryptographic systems such as public key encryption. This is effectively impossible to decode without access to the private key and this twin-key system eliminates a main vulnerability of encoded communication — the point at which participants agree on the code to be used.

2. Anonymity: as well as the communication being secure from outside observers, the identity of the sender must also be concealed. In the case of traditional postal mail, the equivalent is for the sender to not put their name or address on the letter and envelope. For online communication, Tor allows this through anonymous accounts and onion routing.

3. Authentication: each party needs to be sure that communication is genuinely coming from the other; the equivalent in a traditional, posted letter would be a hand-written signature. Most secure communication systems also feature authentication mechanisms.

4. Hidden exchange: in order to achieve secure transactions, the seller needs to be able to set and run their marketplace without exposure. Outside cyberspace, this is possible for traders who operate without licences or permanent premises. Back-alley deals for drugs, weapons and other illicit goods and services fit these criteria. In darknet environments, hidden services such as those offered on Tor allow the setting up and running of online markets without disclosure.

5. Payment: for a transaction to be secure, it is vital that the payment cannot be traced back to the buyer. In the real world, a buyer can ensure this by paying in cash. In virtual transactions, cryptocurrencies are used.

These five points may be exploited as vulnerabilities when investigating encrypted transactions.

Cryptocurrencies

Anonymisation services allow buyers and sellers to interact without revealing their identities. However, for complete anonymity to be achieved, the financial side of the transaction must also be carried out anonymously. Darknet marketplaces achieve this through the use of *cryptocurrencies*. Probably the most well-known example is bitcoin, introduced in 2008 by an anonymous individual (or group) using the name Satoshi Nakamoto. The aim was to

Features of bitcoin

Digital: bitcoin is based on only electronic records. There is no gold or other tangible asset supporting bitcoin.

Decentralised: the system managing bitcoin is decentralised through the use of a peer-to-peer network. Every member of the network has software that distributes the management of the currency.

Open source: the software needed to acquire and use bitcoin is free and available to anyone.

Public ledger: all bitcoin transactions are recorded in a public ledger called the *blockchain*, stored on the decentralised network. When a transaction is made with bitcoin, this is entered in the ledger, preventing the user from spending the bitcoin twice.

Generated through mining: new bitcoins can be generated through a process called *mining*, which enables the creation of a new blockchain.

How does bitcoin work?

Bitcoin is a decentralised, cryptographically secure digital currency that enables peer-to-peer payments between any two people in the world without relying on government or regulatory oversight. To acquire bitcoin, users first create a wallet. This is represented by a unique identifier that does not reveal the identity of its owner. When someone acquires (a fraction of) bitcoin, either from exchange websites or through a transaction with another party, it is transferred into their wallet and the blockchain is updated to reflect the change of ownership.

When someone wishes to pay for a transaction with bitcoin, they send a message on the bitcoin peer-to-peer network, indicating that bitcoin will be transferred from their wallet to the vendor's wallet. The network will confirm that they control this wallet and that the buyer has not already spent this bitcoin. Once this is verified, the bitcoin will be transferred and the blockchain will reflect that it is now owned by the vendor. The process is identical regardless of the nature of the transaction — licit or illicit.

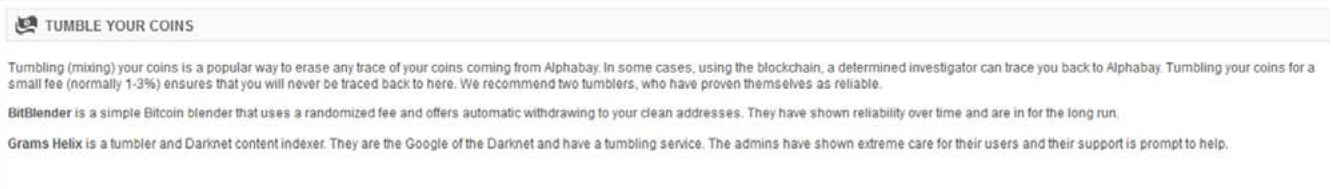
remove the need to trust governments or other political and financial institutions (as is inherent in all *fiat* currencies) and instead base it on a trust in cryptography. Bitcoins are designed to be free from control and interference from outside institutions and to be self-managed by an online community (Nakamoto, 2009).

Cryptocurrencies have been associated with erratic and often dramatic shifts in the currency market, thus presenting opportunities for gains and losses for those reliant on them. However, despite this volatility there also still appears to be a growing interest in the use of these new payment forms, provided that they will in future be seen as a trustworthy and reliable medium for exchange. Greater commercial and public adoption of cryptocurrencies, should it occur, is also likely to have implications for their use for criminal purposes.

All bitcoin transactions dating back to when the currency was first established are recorded in the blockchain, a large, public (unencrypted) database. The blockchain is not in a central location; rather it is stored by thousands of individuals and companies around the globe running bitcoin software. Therefore, a buyer's transaction can be traced back to the point at which the bitcoin was purchased through a process known as *blockchain analysis* (Simonite, 2013). In order to ensure that their identity is concealed, users can employ a number of techniques, and in some cases the markets themselves provide these services. *Tumbling/mixing* is a popular way of obscuring traces of bitcoin coming from a darknet market — two tumblers (BitBlender and Grams Helix) are available to AlphaBay users (Figure 1.3). There are also third-party applications, such as Bitcoin Fog, which conceal the destination of a user's coins to the point at which blockchain analysis becomes exceptionally difficult.

FIGURE 1.3

Example of AlphaBay announcement on tumbling services available to users



While Bitcoin remains the preferred cryptocurrency, alternative ones have been developed that copy some of its features. Some of the most-cited currencies are Litecoin (Vejačka, 2014), Dogecoin (Markus, 2013), Zcash (Ben-Sasson et al., 2014), Ethereum (Wood, 2014), Darkcoin (Greenberg, 2014) and Monero (2017). These seek to solve some of the limitations of Bitcoin, including having concealment features already built in.

Many darknet marketplaces have adopted and offer an extra layer of financial security for their users — an *escrow service*. In a basic escrow system, when a buyer orders an item the fee is held by a third party and provided to the seller only once the buyer has confirmed that they have received the goods. More advanced escrow systems use multisignature, or *multisig*, 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. While markets might offer multisig escrow, it is not always chosen for use. Figure 1.4 shows the guide for multisig transactions on AlphaBay.

FIGURE 1.4
Example of multisig transaction instructions on AlphaBay

Extract from website reads as follows:

> …here is how a multisig works:
> 1) Both the buyer and the seller must have set their public Multisig key in their profile.
> 2) The buyer deposits 4% of the item value in his AlphaBay wallet to cover market fees.
> 3) The buyer purchases the item, then a multisig Bitcoin address is generated using the buyer's key, seller's key, and a market-generated public key (2/3). Both parties can use this publicly-viewable information to verify the authenticity of the address.
> 4) The buyer sends money to this address, and the seller ships the goods.
> 5) If the buyer is happy, he finalizes, and the seller receives the market private key.
> 6) In case of dispute or refund, the buyer receives the private key.
> 7) Whoever got the private key will use it, along with his own private key, to claim the coins.
> To make it simple: buy the product, and you get a BTC address to send the coins to. Seller gets the private key when you finalize. You get the key if you dispute and win. This is a fool-proof method to avoid exit scams. You never give your private key to anyone.

Excerpt from AlphaBay (accessed 12 June 2017)

The alternative, more risky option for the buyer is to *finalise early*, often shown on listings as 'FE' (see Figure 1.5b). This potentially involves paying a reduced price with the incentive of receiving the purchased items without the delay involved in the escrow system.

1.5 Research on darknet markets

There is a growing body of research on various aspects of darknet markets, including attempts to measure the size of these markets, the substances available and whether or not this differs geographically, the characteristics of those using darknet markets, the motivations for using darknet markets, and toxicology testing of the drugs purchased on darknet markets.

In interpreting these findings, it is important to recognise the methodological and practical difficulties of conducting research on and in relation to darknet markets. Sample sizes are often small for example, and formal statistical sampling methods are impractical. Studies may consider only a subset of markets or geographical locations; thus, it cannot be assumed that the results are necessarily representative. In addition, these markets are dynamic, and change occurs rapidly. Despite these limitations, the available data are informative and also highlight areas requiring further investigation and monitoring.

Buyer characteristics

Research has investigated demographic information on those purchasing drugs through darknet markets. Van Hout and Bingham (2013a) reported on a convenience sample of 20 adult Silk Road users. The majority were male, had a history of drug use (ranging from 18 months to 25 years) and were in professional employment or tertiary education. These results are similar to those found in another study of 17 respondents (Barratt et al., 2016a): most (15/17) were male with a median age of 21-25 years. These data are broadly consistent with the demographic characteristics of those that reported buying drugs online in the 2016 Global Drug Survey (GDS) sample. This is an online self-nomination survey — and, while it is not representative in any formal statistical sense, it does benefit from having a large number of participants. Of those completing the online questionnaire who had purchased drugs on the internet, two thirds were male, with a mean age of 28.7 years (47 % were 24 or younger; 23 % were 35 or older). Interestingly, in terms of the total sample of drug users, almost 1 in 10 participants (9.3 %) reported buying drugs from a darknet market at least once (GDS, 2016). It should

be noted, however, that it is possible that, since this was an online drug survey, the sample may have been biased towards those who are more comfortable with an online environment. Similarly, based on an Australian sample of 800 stimulant drug users and data from face-to-face surveys, Van Buskirk et al. (2016) found that 9 % of participants had purchased substances on the darknet in the past year. However, these data are limited to Australian users from urban centres. It would therefore be interesting to further compare these results with results collected through other methods.

Motives for buying and selling online

In terms of users' motives for purchasing drugs on the darknet, existing studies tend to highlight the same issues. Online buyers perceive that higher quality products are available online than are available from alternative sources (Van Hout and Bingham, 2013a; Barratt et al., 2014). Barratt et al. (2014), using data from the GDS, found that those who used Silk Road to purchase drugs had done so because it offered a wider range of drugs, better quality and greater convenience than was usually available offline. It has also been suggested that purchasing from the darknet enables customers to buy from vendors located in the countries where the drug production takes place, in particular MDMA (3,4-methylenedioxy-N-methylamphetamine) from the Netherlands (Van Hout and Bingham, 2013b), presumably reflecting a consumer view that higher quality products may be sourced from known production areas. Décary-Hétu et al. (2016) reported that the majority of vendors on Silk Road were willing to take the risk of shipping drugs internationally, making these drugs much more readily available, at lower costs, to a larger geographical area. This has been suggested to be the case for cocaine shipments to Australia, for example, and MDMA shipments more generally.

Avoiding violence and other risks

Understanding the motivations of those buying drugs online is important for assessing the potential for darknet markets to prosper. Monitoring drug users' attitudes to the relative advantages and disadvantages of purchasing drugs from online and from more traditional sources is informative. It has been suggested that darknet markets might be attractive to buyers, as they are perceived to be safer environments in which to buy drugs because of the removal of face-to-face transactions with dealers, which have the potential to end in violence should things go wrong (Barratt et al., 2016b). However, the extent to which this occurs is likely to vary considerably according to the organisation of drug markets in different locations. Overall, not all drug markets are characterised by the risk of violence (Coomber, 2015). Moreover, many drug users obtain their drugs through peer or friendship networks, so the extent to which obtaining drugs places users at risk of violence or other problems is likely to be highly variable.

While the risks of direct contact with drug sellers may be removed by buying drugs online, there are other risks involved in purchasing from darknet markets. While the seller's location remains anonymous in online drug transactions, a delivery address is required for the buyer. This leaves the recipient open to the risk of *doxing* — the practice of publishing identifying information about an individual. This may result in exposure to the risk of fraud and blackmail (Aldridge and Décary-Hétu, 2016), as well as coming to the attention of law enforcement.

Perceived quality of drugs purchased online

Consumer views about the perceived 'quality' of drugs purchased on the darknet being higher than those brought through street markets has also been suggested as a motivation for using darknet markets. Again, this is an area requiring further research, but some studies, where drugs have been bought on darknet markets and subject to testing in a laboratory, suggest that there is a high probability (greater than 90 %) that what is ordered will subsequently be delivered (Caudevilla et al., 2016; Rhumorbarbe et al., 2016). However, in some cases the purity was overstated; for example, samples of 1 g of cocaine advertised at greater than 95 % purity were determined to contain 33 % and 30 % cocaine when tested. An important caveat here is that this study analysed a very small number of samples, so any conclusions need to made with caution and more data are needed to better judge the extent to which drugs offered on darknet markets match the advertised products. Some commentators have suggested that, by providing a more reliable source of drugs, darknet markets may reduce some of the risks associated with consuming unknown or contaminated products. There are some clear public health risks associated with the misselling of drugs in respect of their composition, purity and possible contaminants. This, however, does not imply that having access to highly pure or potent drugs necessarily reduces risks, as such purity can also represent a hazard in its own right. Data in this area based on user evaluations of product quality — which are often positive with regard to darknet sales — are supportive of the limited forensic information. Assessments of quality based on user evaluations cannot, however, simply be taken at face value, as they will be influenced

by factors including the users' levels of experience, the purpose of using the drugs purchased and the context of use (Bancroft and Reid, 2015). In summary, the limited data that exist would suggest that darknet markets are generally regarded as reliable by those that use them in respect of receiving the substance that was expected. It is possible to postulate that online sales could possibly reduce or elevate some of the health risks associated with purchasing drugs, as compared with those sourced through street markets. While this remains an important topic for further research, it is not possible to draw any firm conclusions on this issue based on the limited information currently available.

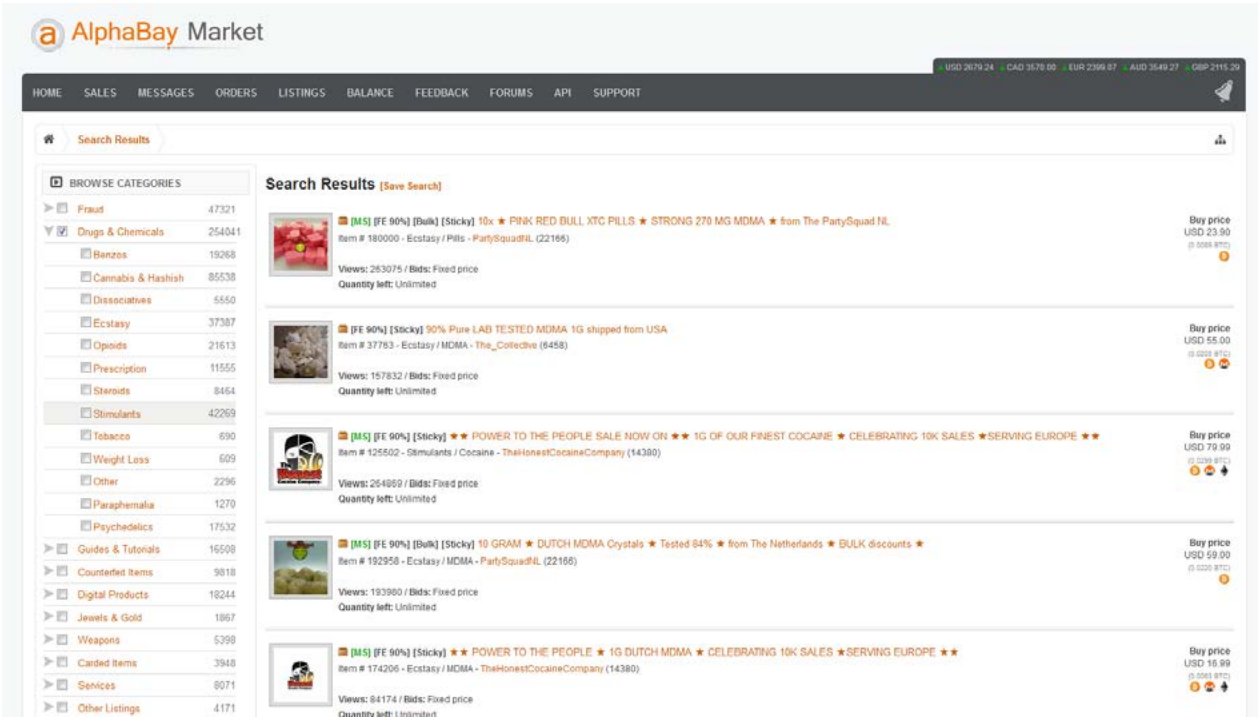
1.6 The user interface

Some research has explored the business models used by darknet drug vendors, and the relationships and interactions that exist between buyers and sellers. Bancroft and Reid (2015), for example, used discussions on a market forum and qualitative interviews to explore how drug quality is assessed by users and how experiences of purity, dosing, effects and vendors are systematically shared.

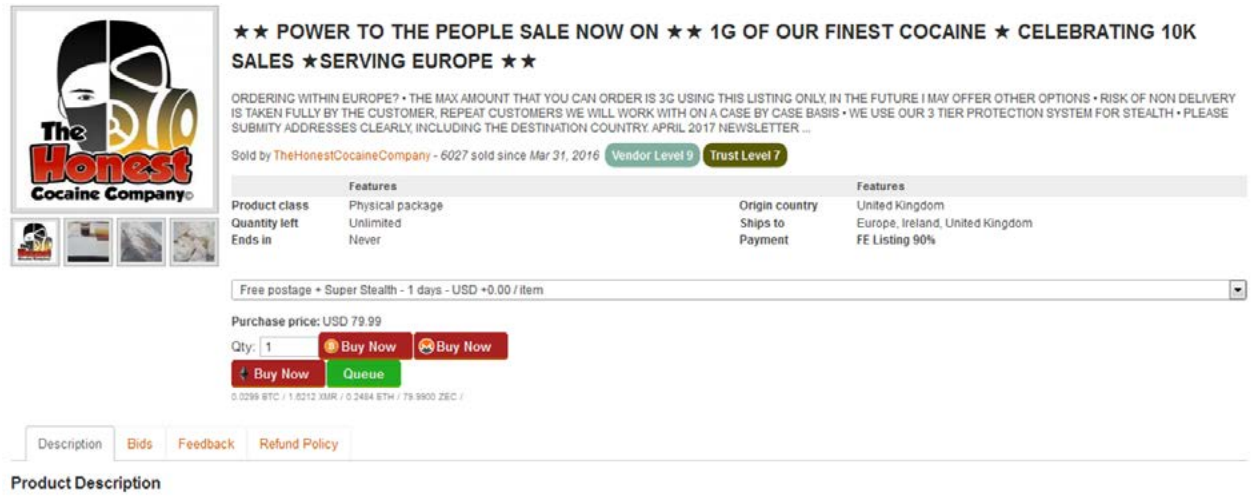
FIGURE 1.5

Example of an online anonymous marketplace: AlphaBay; (a) displays various drug listings and (b) shows a specific item listing

a) Overview of drug listings



b) Specific item listing



Barratt and Maddox (2016) conducted an ethnographic study on the impact of Silk Road on drug use among those using Silk Road to buy drugs. Participants described a peak of drug consumption in the initial months of using Silk Road, with some reporting less hoarding of drugs due to more availability from darknet markets. Van Hout and Bingham (2014) explored vendors' accounts of Silk Road and concluded that sellers often adopted a 'professional' approach or business model to ensure client loyalty and maximise profits over time, meaning attention to providing 'high-quality products', follow-up communication and forum activity. Van Hout and Bingham (2013b), based on a single case study approach, explored the purchasing practices, experiences and motives of users of the initial Silk Road market and reported that the relationship between vendors and customers was often based on mutual trust. These findings highlight the importance of buyer feedback mechanisms to the functioning of darknet markets, as they allow potential buyers to assess the performance of vendors with other customers.

From a user interface standpoint, Figure 1.5 shows, as an example, the AlphaBay marketplace. Information available on AlphaBay is reasonably representative of what can typically be found on an online anonymous marketplace.

The main AlphaBay page, shown in Figure 1.5a, displays various categories of items available for sale, as represented on the left-hand menu, including 'drugs', that is, primarily illicit drugs, and prescription drugs, that is, medicines. As evidenced in the figure, different items may be sold by different vendors. Usually, the marketplace acts as a broker — similar to eBay (see box below) — that ensures that transactions are completed to the satisfaction of both buyers and sellers, while taking a percentage fee for each transaction. For example, information on AlphaBay indicates that the transaction fee is 4 % of the value of the sale. A fixed fee for smaller transactions has also been noted on the Hansa Market. Specific item listings, as shown in Figure 1.5b, contain numerous pieces of information: in the case of AlphaBay, an origin country (the United Kingdom), potential shipping destinations (Europe, the United Kingdom and Ireland), a vendor name (taken out), a description of the item and, crucially, user feedback.

Feedback and ratings mitigate the potential for being tricked by unscrupulous vendors, both on legitimate e-commerce sites and on darknet marketplaces. They provide buyers with a relatively reliable account of a vendor's previous transactions and track record as well as the quality of individual products, and can help buyers to build an impression of whether or not the vendor can be trusted to supply a good-quality product.

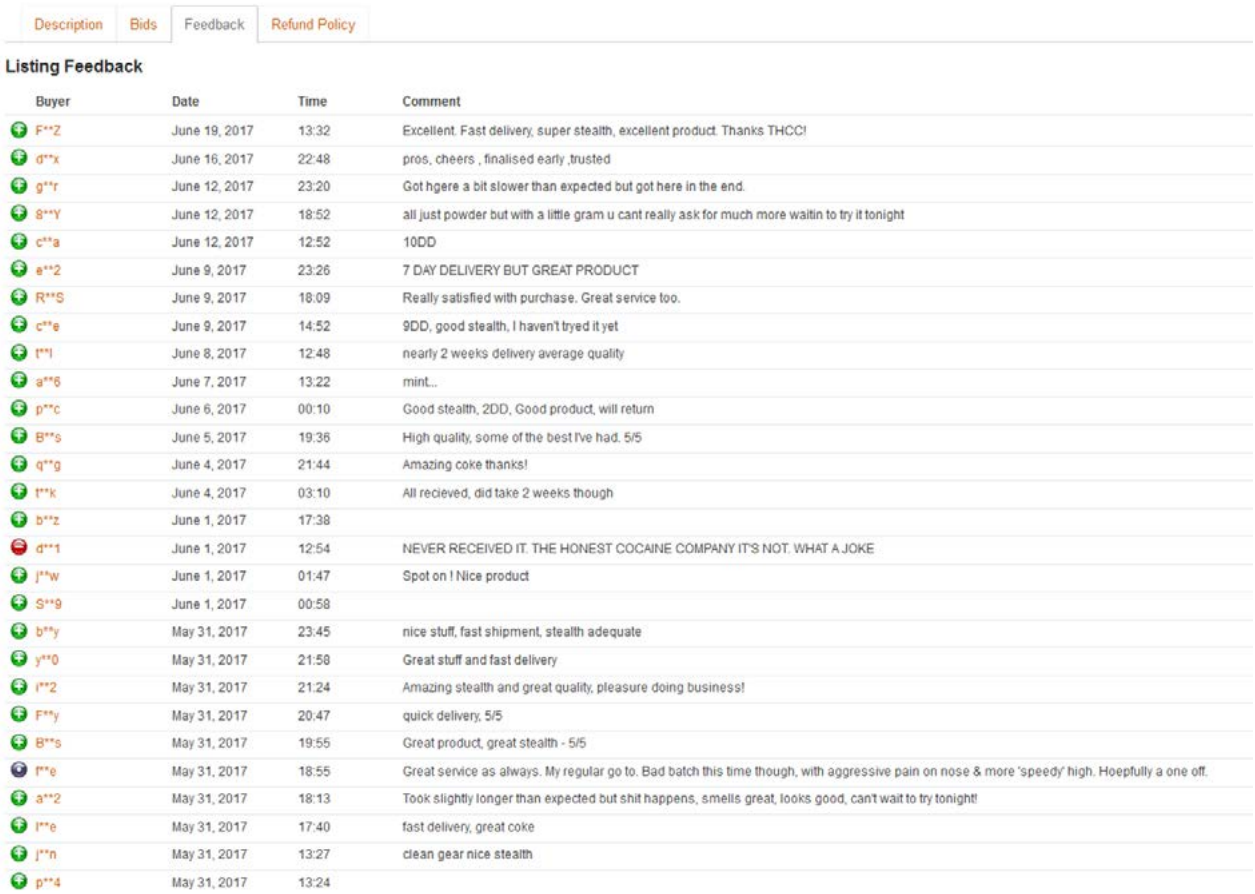
Figure 1.6 gives an example of darknet marketplace feedback fields. On AlphaBay, feedback consists of a timestamp, a short comment, a rating (represented here by the green '+' or red '–' sign) and a four-character string allowing, to some extent, the possibility to differentiate buyers. This last field is not present on most markets. In the comments, several references to 'stealth' can be observed (underlined in Figure 1.6). The term 'stealth' is used to refer to how well the drugs have been concealed by the sender, which is likely to reduce the risk of detection and interception.

Darknet markets: an eBay for drugs?

Some have argued that darknet drug markets cannot be considered the 'eBay for drugs', as eBay is aimed at the retail level (RAND Europe, 2016). This is not strictly correct, however, as there are many examples of wholesale offers and 'job lots' for resellers available on eBay. In the 2016 RAND Europe study, which focused predominantly on the Netherlands, some exceptional wholesale-level transactions were noted (e.g. kilogram quantities of MDMA were listed); however, the vast majority of transactions were at the retail level. Despite this, 25 % of the revenue of Dutch vendors was from wholesale-level sales (those listings having a value of more than USD 1 000), which represented around 2 % of the overall transactions. In addition, the Netherlands was identified as the most active vendor country, per capita, with sales rates 2.4 times that of the United Kingdom and 4.5 times that of the United States. This is an interesting finding that merits further examination and scrutiny.

An important point is that darknet markets may flatten the often multilayered traditional drug-selling networks by providing producers and wholesale distributors with the opportunity to connect directly with consumers, which has been argued to be potentially more profitable from the vendor perspective, as it eliminates the need for intermediaries (Aldridge and Décary-Hétu, 2016). This question requires further investigation because, if it is true, it may represent an opportunity for law enforcement to tackle wholesale distribution.

FIGURE 1.6
AlphaBay offered rich feedback information



Description | Bids | Feedback | Refund Policy

Listing Feedback

Buyer	Date	Time	Comment
F**Z	June 19, 2017	13:32	Excellent. Fast delivery, super stealth, excellent product. Thanks THCC!
d**x	June 16, 2017	22:48	pros, cheers , finalised early ,trusted
g**r	June 12, 2017	23:20	Got hgere a bit slower than expected but got here in the end.
8**Y	June 12, 2017	18:52	all just powder but with a little gram u cant really ask for much more waitin to try it tonight
c**a	June 12, 2017	12:52	10DD
e**2	June 9, 2017	23:26	7 DAY DELIVERY BUT GREAT PRODUCT
R**S	June 9, 2017	18:09	Really satisfied with purchase. Great service too.
c**e	June 9, 2017	14:52	9DD, good stealth, I haven't tryed it yet
t**l	June 8, 2017	12:48	nearly 2 weeks delivery average quality
a**6	June 7, 2017	13:22	mint...
p**c	June 6, 2017	00:10	Good stealth, 2DD, Good product, will return
B**s	June 5, 2017	19:36	High quality, some of the best I've had. 5/5
q**g	June 4, 2017	21:44	Amazing coke thanks!
t**k	June 4, 2017	03:10	All recieved, did take 2 weeks though
b**z	June 1, 2017	17:38	
d**1	June 1, 2017	12:54	NEVER RECEIVED IT. THE HONEST COCAINE COMPANY IT'S NOT. WHAT A JOKE
j**w	June 1, 2017	01:47	Spot on ! Nice product
S**9	June 1, 2017	00:58	
b**y	May 31, 2017	23:45	nice stuff, fast shipment, stealth adequate
y**0	May 31, 2017	21:58	Great stuff and fast delivery
i**2	May 31, 2017	21:24	Amazing stealth and great quality, pleasure doing business!
F**y	May 31, 2017	20:47	quick delivery, 5/5
B**s	May 31, 2017	19:55	Great product, great stealth - 5/5
f**e	May 31, 2017	18:55	Great service as always. My regular go to. Bad batch this time though, with aggressive pain on nose & more 'speedy' high. Hoepfully a one off.
a**2	May 31, 2017	18:13	Took slightly longer than expected but shit happens, smells great, looks good, can't wait to try tonight!
l**e	May 31, 2017	17:40	fast delivery, great coke
j**n	May 31, 2017	13:27	clean gear nice stealth
p**4	May 31, 2017	13:24	

This feedback is particularly important for analysing the activity on darknet markets. As described by Christin (2013), mandatory feedback (which is the case for the majority of marketplaces) is a useful proxy for sales and can be used to explore market operations over time. Thus, data from mandatory feedback can be exploited to provide an idea of the sales volumes through a simple correlation between the feedback timestamps and the item prices (and the quantity, when available). For instance, the product for which feedback is presented in Figure 1.5 is sold for USD 79.99 (EUR 71.31) ([3]) (see Figure 1.5b); three pieces of feedback were deposited on 12 June 2017 (see Figure 1.6). It can then be inferred that the vendor sold USD 79.99 × 3 = USD 239.97 (EUR 213.93) worth of the item on that specific day.

1.7 The impact of law enforcement

Vendors on darknet markets are no different from drug dealers in other marketplaces in their desire to avoid detection and minimise risk (Décary-Hétu et al., 2016; Murray, 2016). These risks include arrest and violence, and threat to profits and reputation. Different law enforcement activities have the potential to have an impact on these risks. Darknet markets provide a place to conduct an illicit business with a low risk of arrest and a low risk of violence. However, the interception of shipments risks reputation and profitability should sales fall because of bad ratings. The closure of darknet marketplaces has been shown to temporarily disrupt market activities (Soska and Christin, 2015; Van Buskirk et al., 2017b). In addition, high-intensity border control of postal deliveries appears to have an impact on the willingness of vendors to ship goods to certain countries. A study of vendor practice also suggests that vendors based in countries where law enforcement is perceived as more effective are less likely to offer

([3]) Currency conversions were carried out using the Currency Converter application at Statistical Data Warehouse, European Central Bank (available at https://sdw.ecb.europa.eu/).

International shipping (Décary-Hétu et al., 2016; Kruithof et al., 2016).

The impact of robust border controls, such as the stringent and frequent control of parcels, has the potential to influence vendor behaviour, with some operational successes noted in several EU Member States (see Chapter 3). An example here is listings on the Hansa market, where some vendors will not ship to Finland, or they will not provide a refund or reship the item if the item is lost. In addition, robust border controls may also be associated with the existence of local darknet markets catering for national demand (see Section 2.2).

The relative magnitude of vendor sales on darknet marketplaces may also indicate another potential vulnerability to the impact of law enforcement interventions. Soska and Christin (2015) estimated that 1 % of vendors across several darknet markets were responsible for about 50 % of transactions. While about half of the vendors sold one or more substances in one market echelon, vendors selling in multiple echelons tended to be 'superstores' carrying more than one drug type and having greater sales volumes. The absolute number of vendors based in the EU reported in this study (see Section 2.1) was 3 305. This suggests that targeting law enforcement efforts on the most active vendors has the potential to significantly reduce the supply of drugs to consumers in the EU and elsewhere.

2

CHAPTER 2

Global phenomenon — EU focus

First, this chapter presents an EU-focused analysis of drug supply on global darknet marketplaces (2011-2015). It then looks into Europe's own national online anonymous markets, identifying their spread and key features. The final section brings into focus the evolution of one of the largest online anonymous darknet markets — AlphaBay — accounting for its activity during (most of) its lifetime (2015-2017).

2.1 An EU-focused analysis of drug supply in the online anonymous marketplace ecosystem

Key methodological points

This section is based on data collected by Soska and Christin (2015). Tables 2.1 and 2.2 outline the data collected (late 2011 to early 2015) and the item categories analysed, respectively. A full report including all technical details can be found in a supporting online report, 'An EU-focused analysis of drug supply on the online anonymous marketplace ecosystem' ([4]), and in Soska and Christin (2015). The aim of the study was to better understand the extent of darknet drug sales originating from Europe. Regular snapshots were collected from 16 major marketplaces during the period 22 November 2011 to 16 February 2015. Based on an extrapolation of data from buyer feedback reports it was possible to estimate the volumes and values of drugs traded over time. Additional information, where it was available, was collected on shipping locations. While not exhaustive, this approach did allow an audit of the main marketplaces trading to European consumers over the study period.

TABLE 2.1

Markets crawled — which markets were crawled, the period the measurements span and the number of snapshots taken

Marketplace	Measurement period	Number of snapshots
Agora ([a])	28.12.13-12.06.15	161
Atlantis	07.02.13-21.09.13	52
Black Flag	19.10.13-28.10.13	9
Black Market Reloaded ([a])	11.10.13-29.11.13	25
Tor Bazaar	02.07.14-15.10.14	27
Cloud 9	02.07.14-28.10.14	27
Deep Bay	19.10.13-29.11.13	24
Evolution ([a])	02.07.14-16.02.15	43
Flo Market	02.12.13-05.01.14	23
Hydra ([a])	01.07.14-28.10.14	29
The Marketplace	08.07.14-08.11.14	90
Pandora ([a])	01.12.13-28.10.14	140
Sheep Marketplace	19.10.13-29.11.13	25
Silk Road ([a])([b])	22.11.11-24.07.12	133
	18.06.13-18.08.13	31
Silk Road 2.0 ([a])	24.11.13-26.10.14	195
Utopia	06.02.14-10.02.14	10

Notes:
([a]) Denotes markets analysed; because of incomplete (feedback) data and/or small volumes, the rest of the markets were excluded from the analysis.
([b]) The November 2011-July 2012 Silk Road data are from a previously reported collection effort, with publicly available data (Christin, 2013).

Source: Soska and Christin (2015).

([4]) See: EU-focused analysis of drug supply on the online anonymous marketplace ecosystem, available at http://www.emcdda.europa.eu/document-library/eu-focused-analysis-drug-supply-online-anonymous-marketplace-ecosystem_en

TABLE 2.2: DATA CATEGORIES

Drug categories of primary interest	Other drugs	Non-drugs
Cannabis: all forms of cannabis products (herb, resin, oil, seeds) Opioids: heroin, opium, analgesics (e.g. oxycodone) Cocaine: all forms of cocaine products Synthetic stimulants: (meth)amphetamine, MDMA, MDA Dissociatives: ketamine, GHB, GBL Hallucinogens: LSD, PCP (excluding psychedelics) NPS: ■ Cannabinoids: synthetic cannabinoids including spice, K2 ■ Opioids: synthetic opioids including fentanils, MT-45 ■ Stimulants: mephedrone, 4-fluoroamphetamine ■ Dissociatives: MXE, DXM ■ Hallucinogens: 25I-NBOMe, 4-AcO-DMT, 2C-B	Prescription drugs: benzodiazepines, barbiturates, sildenafil and related products Psychedelics: mushrooms and other Steroids: steroid products	Drug paraphernalia: bongs, pipes, scales Digital goods: all forms of digital goods including forgeries, credit card numbers, e-books Electronics: electronic items and components Tobacco: tobacco products, including e-cigarettes Weapons: all sorts of illegal firearms Miscellaneous: miscellaneous items not categorised in any other category

Findings

Presented here are (1) an analysis of sales originating from the EU, Turkey and Norway, and a comparison with sales originating outside the region; (2) an analysis of the quantities sold; and (3) an analysis of vendor characteristics.

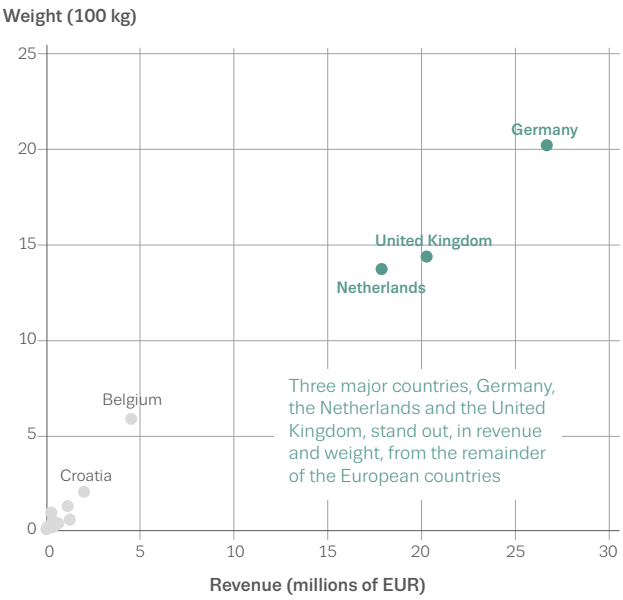
Sales from the European Union

There are 24 EU countries with darknet markets sales in at least one of the seven categories of drugs of primary interest (see Table 2.2). Analysis of the revenue and weight of the drug sales originating from these countries reveals a group of three main countries (see Figure 2.1).

For the seven drug categories, Figures 2.2 and 2.3 present a breakdown of sales originating from the EU, Norway and Turkey by country. Both of these figures are stacked plots. NPS are aggregated into a single category. Figure 2.2 shows the aggregate number of transactions over the entire data collection interval (22 November 2011-16 February 2015). Caution is needed in interpreting these data in respect of the extrapolation of yearly revenues, given the considerable fluctuations in and instability of the whole ecosystem during that period (Soska and Christin, 2015) and the data collection limitations (see online supporting material ([5])).

FIGURE 2.1

Revenue and weight analysis of drug sales originating from the EU, Norway and Turkey by country, 2011-2015

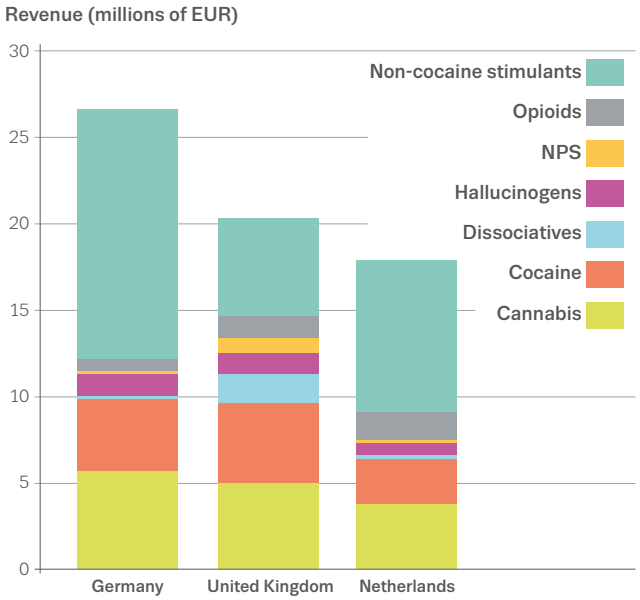


([5]) See: EU-focused analysis of drug supply on the online anonymous marketplace ecosystem, available at http://www.emcdda.europa.eu/document-library/eu-focused-analysis-drug-supply-online-anonymous-marketplace-ecosystem_en

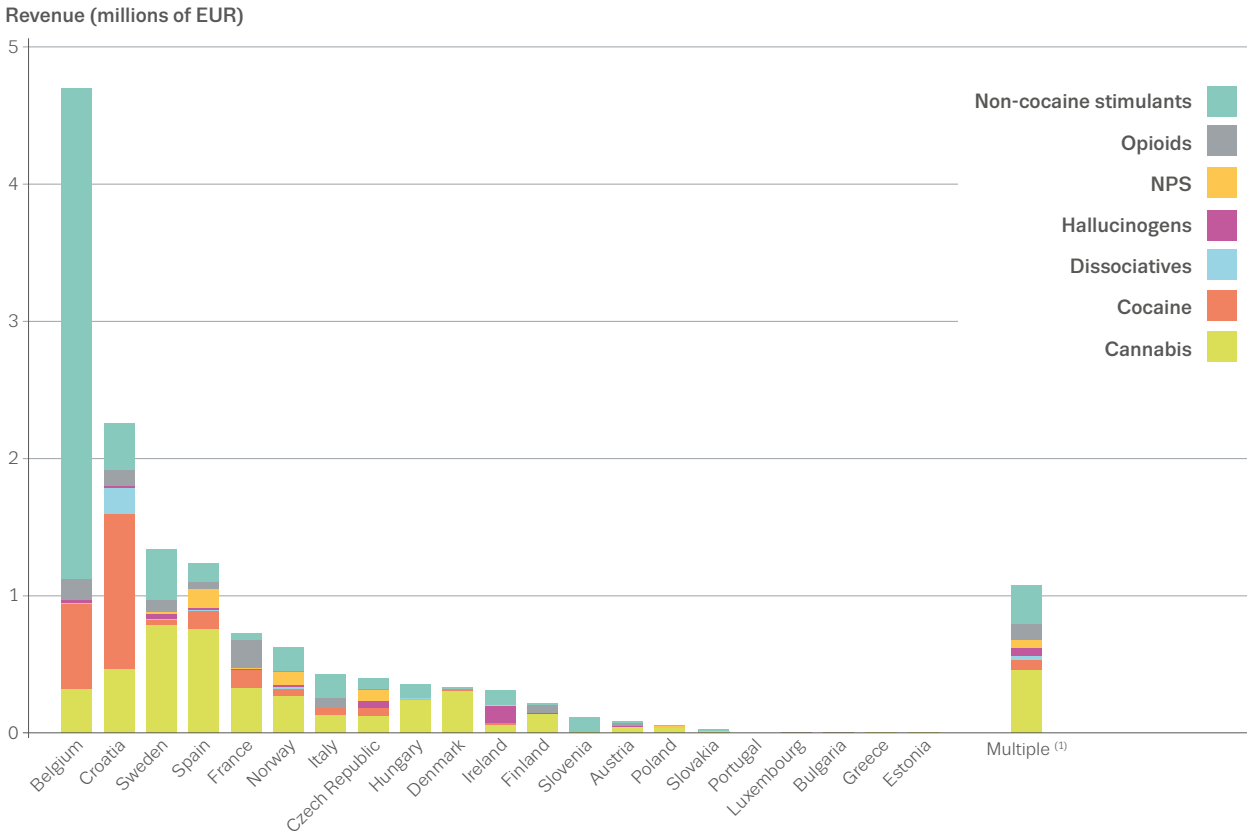
FIGURE 2.2

Breakdown of sales revenues originating from the EU, Norway and Turkey by country, 2011-2015

a) Breakdown by revenue (major countries)



b) Breakdown by revenue (other countries)



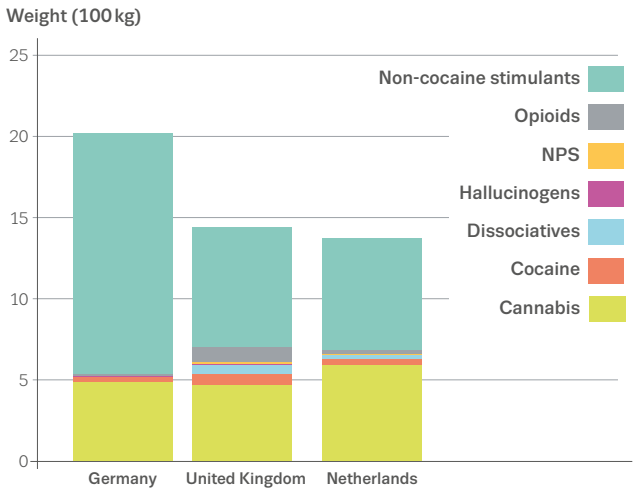
(1) Multiple denotes where several EU countries are mentioned as country of origin.

Note: For readability, the three major countries (Germany, the United Kingdom and the Netherlands) are represented on a different scale.

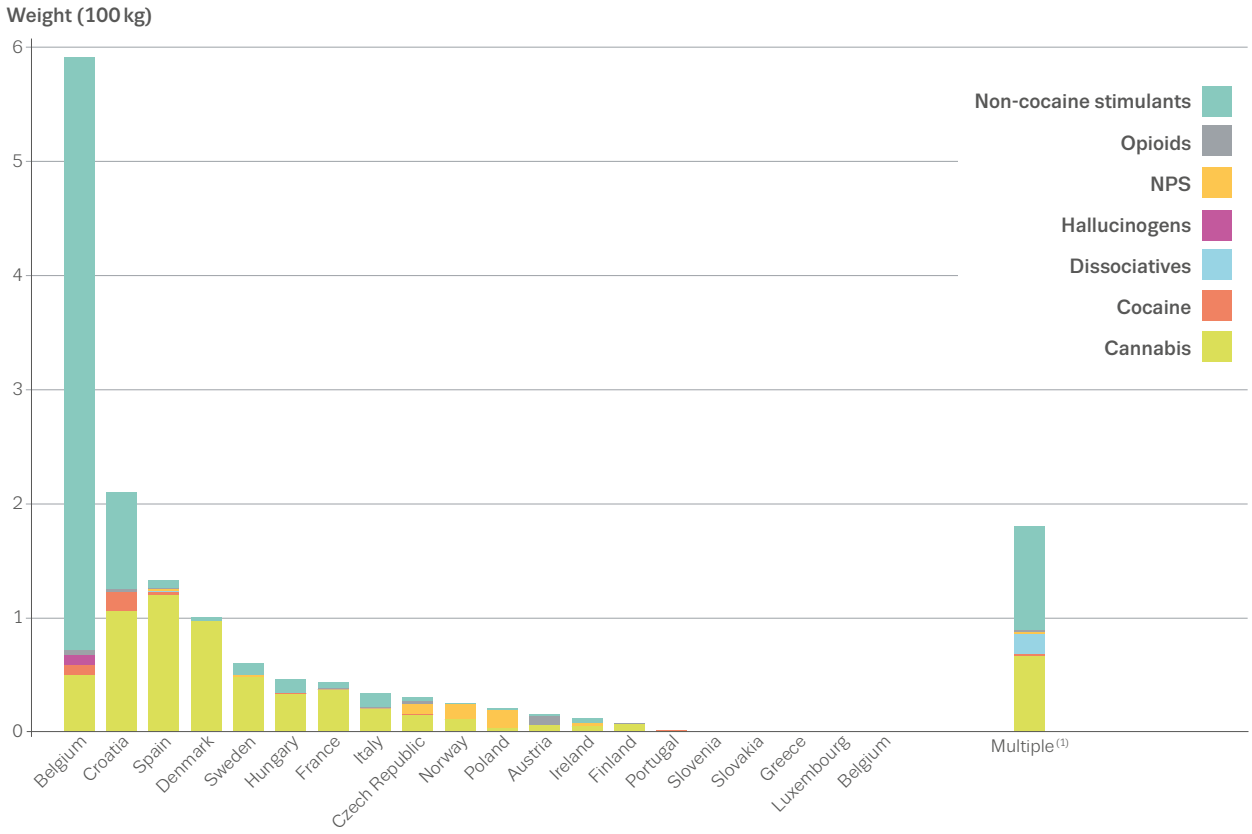
FIGURE 2.3

Breakdown of sales volumes (by weight) originating from the EU, Norway and Turkey by country, 2011-2015

a) Breakdown by volume (major countries)



b) Breakdown by volume (other countries)



(1) Multiple denotes where several EU countries are mentioned as country of origin.

Note : For readability, the three major countries (Germany, the United Kingdom and the Netherlands) are represented on a different scale.

Revenue analysis

The data presented in Figure 2.2 suggest that the vast majority of sales originating from the EU, during the 22 November 2011-16 February 2015 period, originated from three countries: Germany, with about EUR 26.6 million in total sales for the seven drug categories of interest; the United Kingdom, with just over EUR 20.3 million in total sales; and the Netherlands, with just over EUR 17.9 million in total sales. There is a large difference between the value of total sales in these three countries and the next highest sales values for Belgium (EUR 4.7 million), Croatia (EUR 2.3 million), Sweden (EUR 1.3 million), Spain (EUR 1.2 million) and the 'others', that is, those purporting to ship from multiple possible locations (EUR 1.1 million), with the rest all having less than EUR 1 million in total sales.

Among the top four countries, the most common substances sold by markets in Germany (EUR 14.5 million), the Netherlands (EUR 8.8 million) and Belgium (EUR 3.6 million) were non-cocaine stimulants, principally MDMA (ecstasy) and amphetamines. This is hardly surprising, since this region is an important global supplier of these synthetic drugs. In Germany and the Netherlands, cocaine and cannabis sales were also significant (EUR 5.6 million of cannabis sales for Germany and EUR 3.7 million for the Netherlands; EUR 4.2 million of cocaine sales for Germany and EUR 2.6 million for the Netherlands). In the United Kingdom, on the other hand, a more balanced picture can be seen with respect to the drug classes sold, with non-cocaine stimulants representing roughly EUR 5.6 million of all drugs sales, cannabis accounting for EUR 4.9 million and cocaine accounting for EUR 4.6 million. Vendors in the United Kingdom also appear to be far more likely to sell dissociatives (EUR 1.7 million) and NPS (EUR 852 000) than vendors in other countries.

Volume analysis

Figure 2.3 shows a similar breakdown, but this time by weight (in kg). The general trends observed with respect to financial revenue apply here as well: Germany (2 022 kg overall), United Kingdom (1 442 kg overall) and the Netherlands (1 375 kg overall) dominate the ecosystem. These are the only countries where the weights of products shipped exceeded, in aggregate, a metric tonne (i.e. 1 000 kg). Because of the vastly different prices per unit for the different categories of drugs, in this volumetric representation cocaine, opioids and hallucinogens represent a far smaller proportion than in the revenue representation in Figure 2.2; conversely, cannabis accounts for a significantly larger proportion. This is discussed in the section 'Transaction amounts broken down by drug and by quantities sold'.

Comparison with non-EU sales

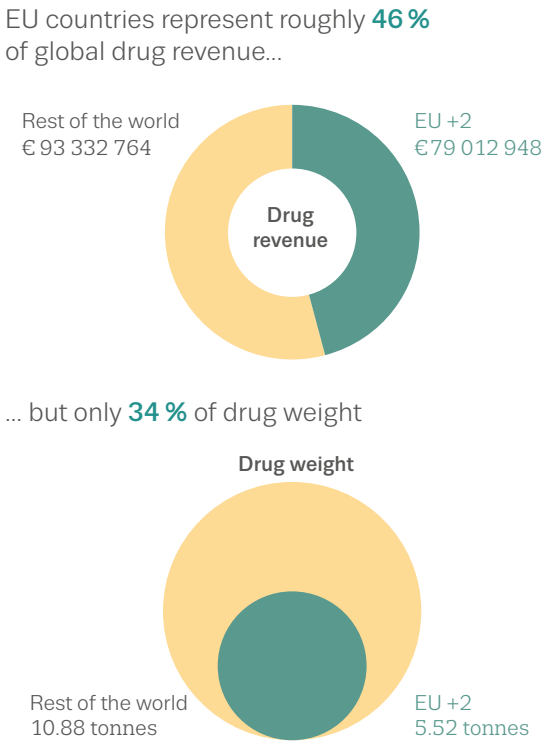
In Figure 2.4, the data presented show sales originating from the EU, Norway and Turkey in comparison with those originating from other countries, both for drugs in the seven categories of interest and for all products. Drug sales represent an overwhelming majority of the revenue of these marketplaces; this is more noticeable in the EU than in the rest of the world. This difference is due to digital goods usually being classified as having no specific origin, and these digital goods representing a non-negligible proportion of overall trade (Soska and Christin, 2015).

In terms of drug sales, EU countries represent roughly 46.0 % of global drug revenue, but only 34.0 % of the weight sold. This is because cannabis, which has a lower unit cost than other substances, is responsible for a greater proportion of sales outside the EU than within the EU (Soska and Christin, 2015).

New psychoactive substances

The analysis indicates that NPS tend to represent only a very small proportion of all trade on online anonymous marketplaces. Where NPS were observed to be sold on

FIGURE 2.4
Comparison of drug sales in the EU and the rest of the world, 2011-2015



Note: Drugs in the seven categories of interest.

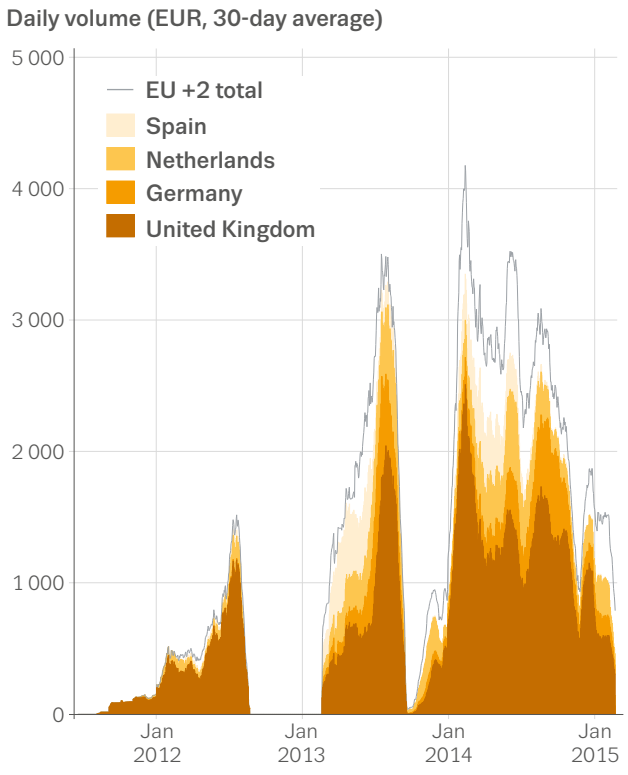
such marketplaces, they were usually despatched from the United Kingdom.

Figure 2.5 provides a finer-grained view of the sales of NPS on online anonymous marketplaces, over time, as a stacked plot. The data are subject to the same limitations as the data described in the original paper (Soska and Christin, 2015). Thus, for example, data collection gaps exist in late 2012 — when most markets were not active — and there are few data available for those that were active, such as Black Market Reloaded and the Sheep marketplace.

To improve clarity, all data points presented here represent averages over 30-day moving windows. Figure 2.5 shows that NPS sales volumes rarely amounted to more than EUR 3 000 per day during the study period. Interestingly, most of the NPS sold on online anonymous marketplaces in the time interval of our study were hallucinogens, whereas sales of synthetic cannabinoids, dissociatives, opioids and stimulants were almost negligible. The reasons for this are unclear, but may tie in with the availability of replacements for LSD (lysergic acid diethylamide) at the time, that is, the NBOMe drugs known as 'N-bombs'. These drugs are particularly dangerous (25I-NBOMe was subject to an EU-level risk assessment in 2014) and gave rise to the 1960s peace campaign slogan 'don't drop bombs, drop acid' among users, to try to discourage the use of such

FIGURE 2.5

Breakdown of daily NPS sales originating from the EU, Norway and Turkey



LSD replacements. Figure 2.4 confirms that the majority of NPS seem to originate from the United Kingdom; Germany, the Netherlands and Spain also contribute to the supply of NPS, albeit to a far lesser extent. The dotted line in Figure 2.5 corresponds to total NPS sales for all countries, including those not represented individually in the plot.

Variations in revenues follow the growth and decline of the overall online anonymous marketplace ecosystem. Caution is needed when interpreting the observed decreases in early 2015: these data represent the ecosystem immediately after Operation Onymous (see Section 3.3) and correspond to the end of the measurement interval. This means that they are statistically less reliable than the earlier data, for reasons related to the incomplete coverage of every single *data scrape* (for more detail, see Soska and Christin, 2015).

Transaction amounts broken down by drug and by quantities sold

This subsection looks at the transaction amounts broken down by drug and by the typical quantities sold.

Regarding cannabis, the majority of deals represent small quantities and only a small number of high-volume sales can be observed. As can be seen from Table 2.3, the most common unit of cannabis product sold is 5 g, with a mean price of EUR 58. The high standard deviation is explained by the fact that various products (oils, edibles, etc.) are also classified as cannabis, so there is quite a large price dispersion. There appears to be a modest volume-discounting effect for cannabis products. The most common unit of cocaine sold is 1 g, with a mean price of EUR 84. The volume-discounting effect is markedly more pronounced for cocaine than it is for cannabis products. Ketamine is the most prominent drug in the 'dissociatives' category. The most common unit sold is 1 g, with a mean price of EUR 40, and there does not appear to be much bulk discounting for ketamine.

It is difficult to provide unit prices for synthetic stimulants, as they include a variety of different types of drugs and the descriptive terms used are not always definitive ('MDMA', 'ecstasy', 'speed', 'meth', etc.). The wide range of substances falling under this category means that there is a corresponding wide range of prices for any given quantity. In addition, difficulties in interpretation are compounded by the fact that a number of sellers offer 'lottery sales', which involve a single item being sold at a heavily discounted price to multiple buyers, only one of whom will actually 'win' it.

TABLE 2.3
Prices of the most common units sold of cannabis products, cocaine and ketamine

Drug	Total number of all items in this drug class	Most common unit sold (g)	Number of items (and percentage) in most common weight category	Mean price (EUR) (standard deviation)
Cannabis products	9 837	5	1 745 (17.7 %)	58 (± 39)
Cocaine	2 295	1	664 (28.9 %)	84 (± 30)
Ketamine	469	1	143 (30.5 %)	40 (± 18)

Despite these difficulties, it is possible to make some observations from the synthetic stimulant data. There appears to be limited bulk discounting for MDMA. As a group, the price for opioids varies considerably and modest volume discounting can be observed. LSD was the most common hallucinogen offered during the study period and there was a large variation in the price of retail doses (250 µg or less) for this drug, partly due to measurement errors at such low levels and partly due to vendors offering samples for (nearly) free or as part of lotteries. As the volume increases, the price increases somewhat linearly. Novel hallucinogens (e.g. NBOMe, DMT) account for the vast majority of NPS sales data in the database. Unsurprisingly, these display the same pattern as that observed for LSD, albeit in relation to considerably larger weights (gram as opposed to microgram quantities).

Vendor diversification

This subsection examines the range of products and the quantities that vendors offer. The analysis explores whether or not vendors sell products within a particular weight range, sell more than one drug type, and sell other products or services.

Diversification in terms of the volumes offered

To examine whether or not vendors who sell large quantities also sell small quantities, a coefficient of diversity was computed (see online supplementary report ([6])). The quantity tiers for each drug category are based on a three-tier distinction based on sales volumes in grams between retail level, middle-market level and wholesale at EU level (EMCDDA, 2016b) (Table 2.4).

An overwhelming (≈90 %) majority of cannabis vendors sell within one market tier, or echelon. A minority sell across two echelons; almost no vendor has significant sales across all three. It also appears quite rare for a vendor to sell both in bulk and small volumes at the same time, but some vendors selling relatively large quantities sometimes also offer 'testing samples' to their customers. Data on cocaine show a similar picture. In contrast, however, more diversity can be seen for hallucinogens, opioids and stimulants in particular, where, although most vendors are selling at the retail level, some vendors also sell across multiple echelons with a number of different drugs in each.

Vendors selling in multiple echelons tend to be what might be regarded as 'superstores', that is, they are more likely to offer more than one type of drug and to have relatively high sales volumes. Conversely, vendors who typically sell at only the retail level tend to specialise in one item and to have relatively low sales volumes.

Diversification in terms of the products offered

With regard to diversity across products, about half of all vendors specialise in one category. This is frequently the case for cannabis (566 vendors) and synthetic stimulants (422 vendors), which is not surprising given that they are frequently sold items. The other half displays more diversity. Typically, such vendors sell drugs from a couple of categories and a very small number of those vendors sell multiple substances. Those vendors usually sell at the retail level.

Of the 2 062 vendors reportedly shipping drugs in one of the seven categories of interest from the EU, 346 (16.8 %) also sell other types of drugs (e.g. prescription drugs) and, perhaps surprisingly, 897 (43.5 %) also sell non-drug products (mostly digital goods). Over a third (35.5 %) of those 897 vendors who also sell non-drug products sell drugs from only one category (primarily cannabis or synthetic stimulants); and just under a quarter (23.9 %) sell a range of drugs. Only five of the vendors selling non-drugs are 'bulk' vendors — three sell large amounts of hallucinogens, one sells opioids and one sells synthetic stimulants.

([6]) See: EU-focused analysis of drug supply on the online anonymous marketplace ecosystem, available at http://www.emcdda.europa.eu/document-library/eu-focused-analysis-drug-supply-online-anonymous-marketplace-ecosystem_en

TABLE 2.4
Quantity tiers for selected drugs of interest

Drug type/ market level	Cannabis (g)	Opioids (g)	Stimulants (MDMA tablets) (g)	Hallucinogens (g)
Retail	< 100	< 1	< 10 (< 50)	< 8
Middle-market	100-999	1-999	10-999 (> 50-999)	8-159
Wholesale	≥ 1 000	≥ 1 000	≥ 1 000	≥ 160

Vendors selling under multiple aliases or on multiple marketplaces

The discussion of the analysis presented above assumes that every vendor account denotes a unique vendor. However, it is to be expected that a vendor would sell on more than one marketplace (Soska and Christin, 2015). From the 3 305 vendor accounts identified in Chapter 1, we attempted to identify which ones belong to the same person(s). These 3 305 vendor accounts in the EU are estimated to map to 2 180 unique entities, 1 271 of which sell drugs; 226 (17.8 %) of those sell at least two different types of drugs and 683 (53.7 %) sell drugs and also other products (e.g. digital goods).

2.2 National non-English-language darknet markets

The above analysis of the stated origin countries shows the dominant position of English-speaking countries (the United Kingdom) and western European countries (Germany and the Netherlands) in darknet marketplaces. This is in line with other studies of darknet marketplaces (Kruithof et al., 2016; Broséus et al., 2017). This may reflect the central position of English-speaking parties in online darknet drug trade, which could deter non-English vendors (Kruithof et al., 2016). However, it may also be because less attention has been given to non-English-language or national sites. Currently, studies of non-English-speaking countries are very limited, but include a study of the Finnish version of Silk Road, *Silkittie* (Nurmi et al., 2017). Despite this, since 2013 several non-English-language markets have appeared ([7]). As noted previously, as many vendors appear to be reluctant to ship to countries with strict law enforcement and border controls, such as Finland (Kruithof et al., 2016); this may be one incentive for national markets to become established. To date, little is known about the extent to which national-based, non-English-language markets exist and what operational models they use.

There is therefore a need to invest in work to better identify and describe darknet markets in order to target specific countries or languages. A preliminary analysis of this topic is provided here.

Key methodological points

This section of the report is based on data collected by the EMCDDA on a subcategory of darknet marketplaces — those with limited geographical scope of operation, catering for the non-English-speaking buyers in a particular place. Data were sourced in May 2017 through a short survey distributed among the 28 EU Member States, Turkey, Norway and the neighbouring countries (IPA: n = 6; ENP: n = 7) ([8]) (see Annex 1 for the questions in this survey and instructions for completion). In addition, in June 2017, two surface websites ([9]) were searched for non-English darknet markets, and information was gathered from the darknet markets identified.

The prices of a range of drug types sold on national darknet markets were collected from a number of platforms, with mean prices based on several samples (between two and eight) taken in June 2017.

Findings

Two thirds (n = 29) of the countries approached responded to the data request. Of these, four countries reported a total of nine national darknet marketplaces — France (n = 5), Finland (n = 2), Sweden (n = 1) and Norway (n = 1). Additional searching identified a further four French-, three Italian- and four Russian-language (selling exclusively to the Russian market) darknet marketplaces — thus bringing the total to 20 national marketplaces across six countries.

([7]) Though not discussed here, it has been noted that machine-translated versions of several global marketplaces have also appeared, e.g. Wall Street Market and T•chka.

([8]) IPA (Instrument for Pre-accession Assistance) countries: Albania, Bosnia and Herzegovina, the former Yugoslav Republic of Macedonia, Kosovo*, Montenegro and Serbia; ENP (European Neighbourhood Policy) partner countries: Armenia, Azerbaijan, Georgia, Israel, Moldova, Morocco and Ukraine.

* This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo declaration of independence.

([9]) https://darknetmarkets.org/markets/; https://www.deepdotweb.com/marketplace-directory/categories/non-english/

TABLE 2.5
Excluded national marketplaces — overview

Country/language	Platform name	Source	Reason for exclusion
France/French	The French connection	Survey	(Temporarily) closed (2 June 2017)
France/French	French Deep Web	Survey; Deepdotweb.com	(Temporarily) closed (2 June 2017)
France/French	French Freedom Zone	Survey; Deepdotweb.com	(Temporarily) closed (2 June 2017)
France/French	THC Market	Deepdotweb.com	Unavailable (20 June 2017)
France/French	French Darknet	Deepdotweb.com	Unavailable (20 June 2017); possibly hacked
France/French	French Market Place	darknetmarkets.org	Unavailable (20 June 2017)
France/French	French Dark Place 2.0	darknetmarkets.org	Unavailable (20 June 2017)
Italy/Italian	Babylon	darknetmarkets.org	Unavailable (20 June 2017)
Italy/Italian	Italian darknet Community	Deepdotweb.com; darknetmarkets.org	Forum
Norway/Norwegian	Fluesopp	Survey	Never had actual sales (as of 2 June 2017)
Russia/Russian	Wayaway	Deepdotweb.com	Unavailable (20 June 2017)
Russia/Russian	Rutor	Deepdotweb.com	Forum
Russia/Russian	Ramp	Deepdotweb.com	Forum

Of these, seven French, one Italian and one Russian marketplace appeared, at least temporarily, to be closed or unavailable when accessed. The Norwegian market never actualised any sales and a further three sites were noted to be forums rather than marketplaces (Table 2.5).

At the time of writing, there appeared to be seven active national darknet marketplaces, as outlined in Table 2.6).

All seven darknet marketplaces catering for specific countries, or run in a language other than English for the global market, appear to sell drugs over Tor, with the majority offering open registration (with the exception of La main noire, which is accessible by invitation only) and some form of escrow functionality (except Sipulikanava and Flugsvamp 2.0). In just two instances, the creation date of the reported platform was known (Flugsvamp 2.0: April 2015; Silkkitie: January 2014).

While different factors may contribute to the emergence and endurance of these national/local platforms, it would appear that law enforcement activity may play a significant role. As noted above, some vendors will not (re)ship to Finland (see Figure 2.6a) and some Finnish vendors will ship only nationally (see Figure 2.6b).

In terms of geographical scope, while in most cases it was made apparent that the marketplace served the needs of a national drug market (e.g. Russian Hydra sellers all appeared to be Russia based, shipping to over 100 locations across the country), there were instances where the marketplace was run in a non-English language, for example the Italian IDC 2.0 market, even though sellers were not necessarily based in Italy and were reportedly shipping 'worldwide' (see Figure 2.7).

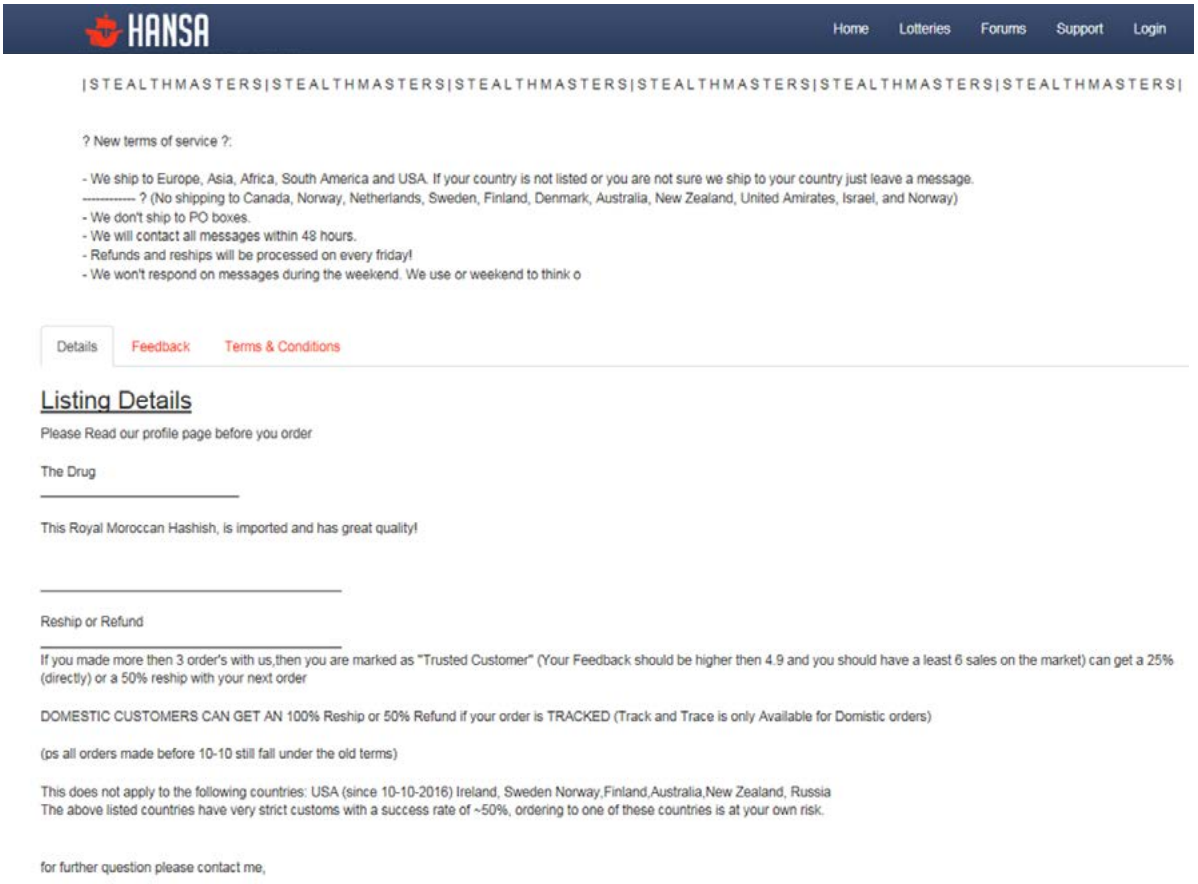
TABLE 2.6
Active darknet marketplaces for specific countries/languages

Country/language	Platform name and URL	Source
France/French	La main noire	Survey
France/French	Le bon coin	Survey; Deepdotweb.com
Finland/Finnish	Sipulikanava	Survey
Finland/Finnish	Silkkitie	Survey; deepdotweb.com; darknetmarkets.org
Sweden/Swedish	Flugsvamp 2.0	Survey
Italy/Italian	IDC 2.0 market	Deepdotweb.com
Russia/Russian	Hydra	Deepdotweb.com

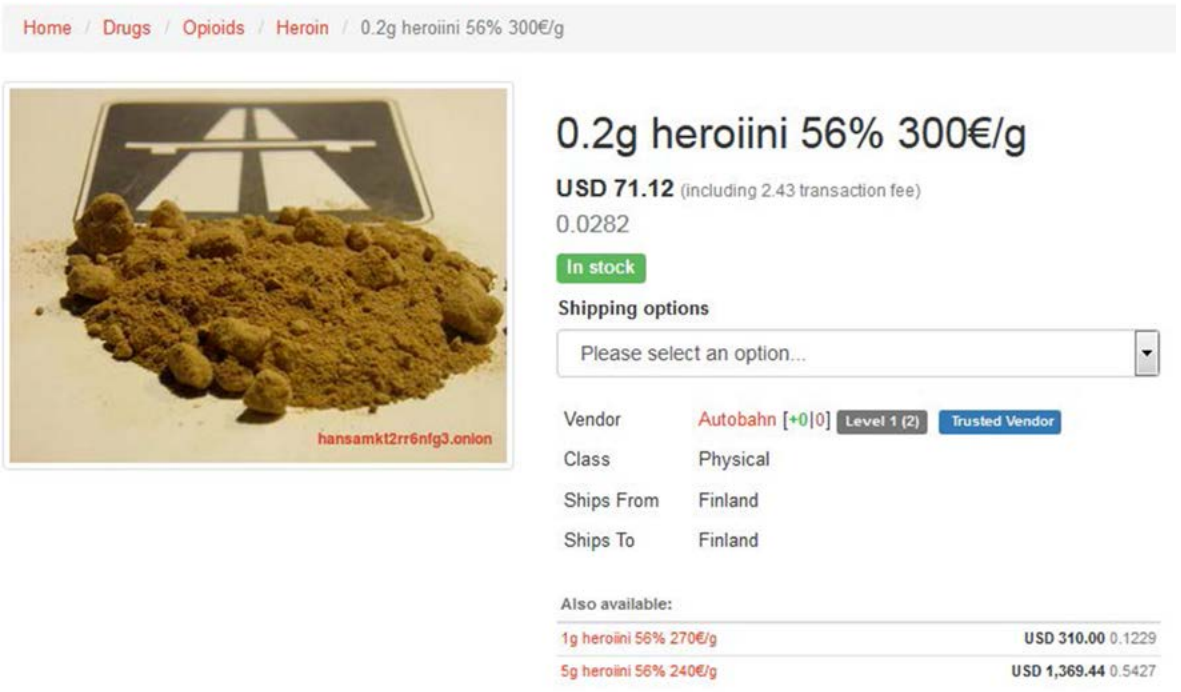
FIGURE 2.6

Examples from the Hansa market of Finland-related vendors' activity

a) Vendors state, in their terms of service, 'no (re)shipping to. . . Finland' among other countries



b) Finland-based vendor declares shipping to Finland only



At the time of reporting, all seven darknet marketplaces had limited commercial activity. For example, only 30 drug products were displayed on the French marketplace Le bon coin and a comparable number of illicit drugs and medicinal products across 10 drug categories were available on the Russian marketplace Hydra.

The average retail prices of cannabis resin, MDMA and LSD were lowest on the Italian IDC 2.0 market and highest on the Russian Hydra market. Herbal cannabis and cocaine appeared cheapest on the Swedish Flugsvamp 2.0 market (herbal cannabis, EUR 10/g; cocaine, around EUR 70/g) and most expensive on the Finnish darknet markets (herbal cannabis, EUR 20/g) and the Russian Hydra market (cocaine, EUR 180/g) (Table 2.7).

When trying to compare darknet market prices with conventional 'street' market prices reported to EMCDDA, no meaningful pattern emerged; a larger dataset would need to be compiled to permit such comparative analysis.

Since drug prices were not collected systematically, the values in Table 2.7 should be seen as a rough guide to what some of the main drug types cost on national darknet platforms. At the time of data gathering, key drugs such as heroin were unavailable on some markets, limiting the analysis. Nonetheless, an important observation is that drug prices on the Russian darknet market are consistently higher than on European darknet markets, particularly the Italian IDC 2.0 market, possibly reflecting the greater distance of Russia-based vendors from countries perceived to be associated with the production of drugs.

2.3 Case study: AlphaBay

Key methodological points

In the previous sections of this report, a market-level analysis of darknet activities has been provided based on a review of the major markets that were known to exist during the study period. Here we complement this with a more detailed case study of one of the most important marketplaces (in terms of lifespan, sales volume and customer database), AlphaBay. This section reviews in detail the activities of the AlphaBay darknet marketplace throughout most of its existence (from March 2015 to May 2017; AlphaBay was shut down in July 2017 by law

FIGURE 2.7
The Italian IDC 2.0 market's Spain-based vendor ships 'worldwide'

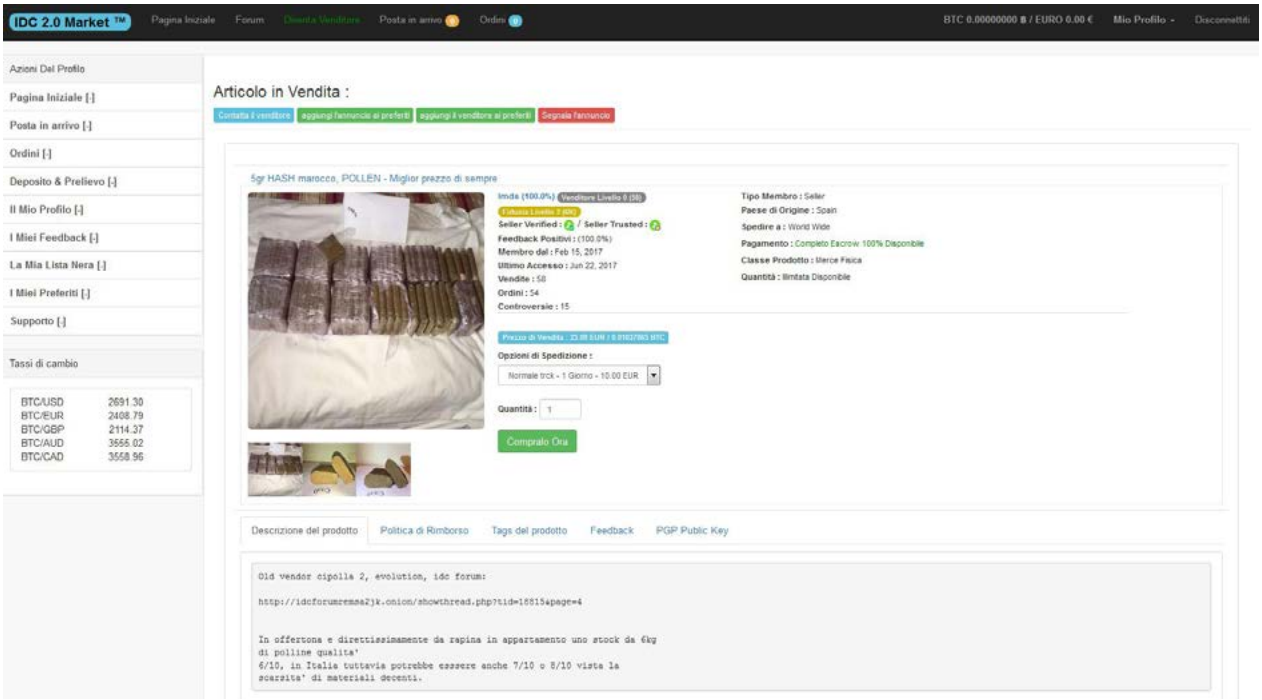


TABLE 2.7

Average prices (EUR) per drug unit (g/tablet/blotter); examples from five national darknet markets

Drug type/ market (country)	IDC 2.0 (Italy)	Flugsvamp 2.0 (Sweden)	Sipulikanava (Finland)	Silkkitie (Finland)	Hydra (Russia)
	Price (EUR) (± SD) per drug unit (g/tablet/blotter)				
Herbal cannabis	11.7 (± 2.3)	10.3	20.0	20.0	17.2 (± 4.7)
Cannabis resin	7.7 (± 3.3)	8.2	NA	NA	13.6 (± 3.4)
Heroin	NA	102.8	NA	NA	64.5 (± 18.6)
Cocaine	85.8 (± 9.7)	72.0	140.0	150.0	180.0 (± 28.0)
Amphetamine	9.3 (± 5.5)	10.3	40.0	30.0	11.8 (± 3.8)
MDMA	5.2 (± 0.2)	6.2	NA	12.0	13.2 (± 4.0)
LSD	11.0 (± 4.7)	17.1	NA	NA	23.4 (± 4.5)

NA, not available, i.e. no listings at the time; SD, standard deviation (not available for prices reported for the Swedish and Finnish markets).

enforcement) and applies the same methodology used for the EU-focused analysis of the whole online anonymous marketplace ecosystem (see Section 2.1 and online supporting report ([10])).

The AlphaBay marketplace

The AlphaBay marketplace was reportedly designed in mid-2014 ([11]). It went online on 26 December 2014, shortly after Operation Onymous took place (see Figure 1.2). Similar to the Evolution marketplace, AlphaBay was reportedly started by 'carders', that is, people who had been trading stolen credit card numbers and other banking credentials. However, AlphaBay quickly began offering illicit drugs as well. Initially, it existed as a fairly small marketplace, overshadowed by Evolution and Agora. By mid-2015, however, following the closure of Evolution, AlphaBay started to gain exposure and reportedly became one of the leading markets later that year and, by 2016, it was almost certainly the most prominent operator in the cryptomarket space. Below is a historical analysis of how this progression happened.

Findings

Evolution of sales on AlphaBay

The evolution of sales on AlphaBay over time is shown in Figure 2.8 for most of its operating history. Each (stacked) curve represents a specific country or set of countries.

Figure 2.8a represents the evolution of sales in absolute value, over time, presented in euros, as a 28-day moving average. The discrepancy between the total value of sales and the sum of all sales from countries that could be identified is due partially to incomplete coverage.

Overall, it appears that AlphaBay gained considerable popularity towards the end of 2015, and then more or less continued its steady climb until its demise. The apparent decline, at the end of the collection interval, is likely to be an artefact due to imperfect coverage. For earlier scrapes, incomplete data could be recovered in subsequent scrapes. After the closure of the market, such data recovery was not possible, resulting in a likely underestimate for the final data collection period. It can be seen that by early 2017 AlphaBay had reached a peak of over EUR 600 000 per day — this is about twice as much as the value of the original Silk Road sales during its peak in the summer of 2013 (Soska and Christin, 2015). Figure 2.8b shows the same information, expressed as a fraction of total sales. It can be seen that all EU trade is roughly a quarter of all the total trade that could be identified, and that this remained fairly constant over time.

Categories over time

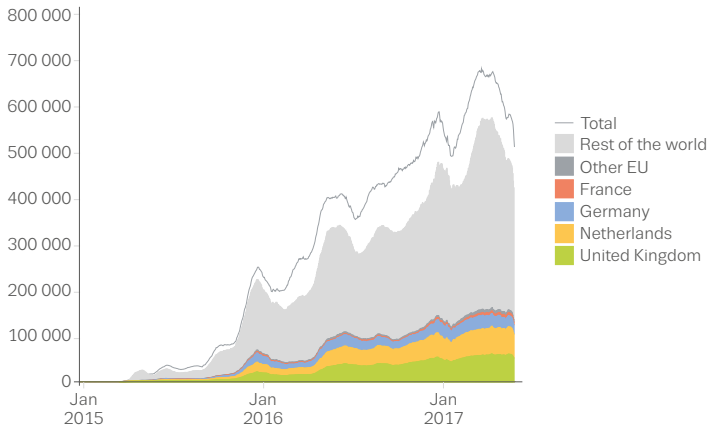
In terms of overall sales volumes, broken down by product categories, Figure 2.9 shows that AlphaBay started as a primarily digital goods business, but then gradually began to trade more and more in illicit drugs when the (then-leading) Evolution marketplace went down in March 2015. Following the Agora marketplace shutdown in August 2015, the increase in transactions on AlphaBay became even more pronounced. By mid-2017, cannabis and stimulants (cocaine and synthetic substances) represented approximately two thirds of all trade on this marketplace.

([10]) See: EU-focused analysis of drug supply on the AlphaBay darknet market for the full duration of its operation, available at http://www.emcdda.europa.eu/document-library/eu-focused-analysis-drug-supply-alphabay-marketplace_en

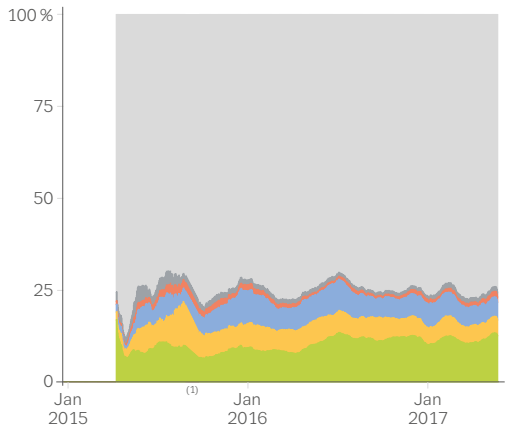
([11]) United States of America vs. Alexandre Cazes, June 2017. United States District Court, Eastern District of (California. Indictment 1:17CR-0144-LJO-SKO.

FIGURE 2.8
Evolution of sales on AlphaBay over time by country, 2015-2017

a) Total sales over time EUR (per country breakdown)



b) Relative sales over time (per country breakdown)



Notes: The left-hand plot (a) represents a breakdown per country. The grey line shows the total value of sales. The white area represents sales for which there is a record, but for which no corresponding item listing could be recovered, thus preventing country inference. The grey area shows non-EU sales. The right-hand plot (b) presents the same information, on a relative scale, excluding items for which the corresponding listing is missing.

(1) There were no sales identifiable from feedback occurring on 31 August 2015, as AlphaBay was down for significant parts of the day. There was evidence that some sales had taken place; however, no country or category could be identified because there was no direct feedback attached to them. As a result, Figure 2.8a displays no data for 31 August 2015. For Figure 2.8b the missing data points were removed before computing the moving 28-day averages, resulting in a continuous plot.

Sales from the European Union

This part of the analysis looks solely at drugs (in the seven categories of primary interest; see Section 3.2, Table 2.2) originating from the EU, Norway and Turkey.

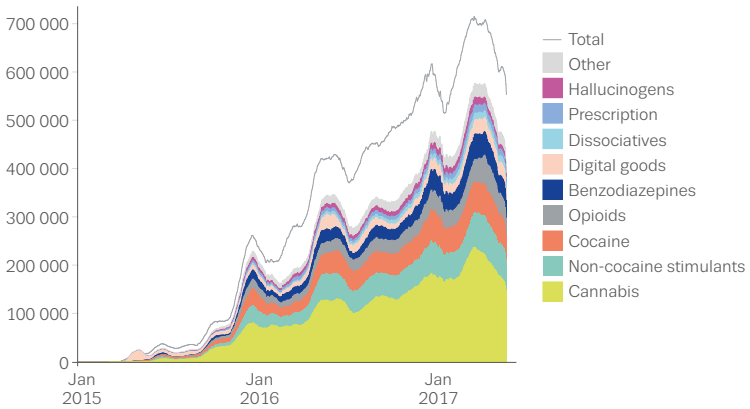
There were 24 EU countries with AlphaBay sales in at least one of the seven categories of drugs of primary interest (see Table 2.2). Analysis of the revenue and weight of the drug sales originating from these countries revealed a group of three main countries (see Figure 2.10).

Revenue analysis

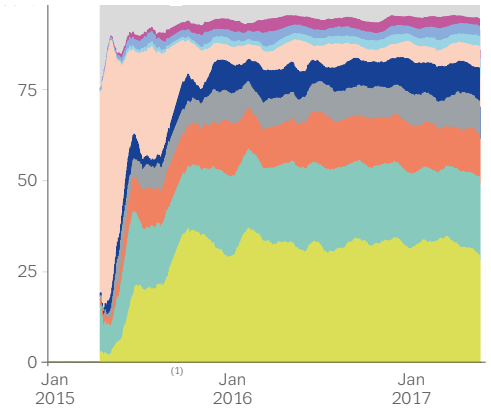
As was the case for the marketplace ecosystem as a whole between 2011 and 2015 (Section 2.1), Figure 2.11 shows that the vast majority of sales originating from the EU come from the same three countries: the United Kingdom, with approximately EUR 19.7 million of total sales for the seven drug categories of interest between March 2015 and May 2017; Germany, with sales of EUR 12.1 million; and the Netherlands, with sales of EUR 10.6 million. France, with sales of EUR 2.0 million, is the only other country that had

FIGURE 2.9
Evolution of sales on AlphaBay over time by category, 2015-2017

a) Total sales over time EUR (per category breakdown)



b) Relative sales over time (per category breakdown)

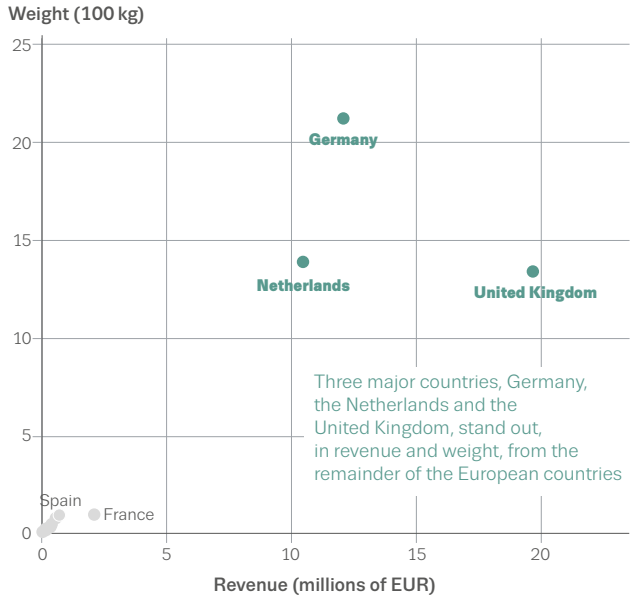


Notes: The grey line in (a) is the total value of sales. The white area represents sales for which there is a record, but the corresponding item listing could not be recovered, thus preventing category inference. The right-hand plot (b) presents the same information, but on a relative scale (excluding items for which the corresponding listing is missing).

(1) There were no sales identifiable from feedback occurring on 31 August 2015, as AlphaBay was down for significant parts of the day. There was evidence that some sales had taken place; however, no country or category could be identified because there was no direct feedback attached to them. As a result, Figure 2.9a displays no data for 31 August 2015. For Figure 2.9b the missing data points were removed before computing the moving 28-day averages, resulting in a continuous plot.

FIGURE 2.10

Revenue and weight analysis of AlphaBay drug sales originating from the EU, Norway and Turkey by country, 2015-2017



a gross revenue of more than EUR 1 million between 2015 and 2017.

The analysis of the whole darknet ecosystem identified that the top three countries primarily sold stimulants other than cocaine (Section 2.1, Figures 2.2 and 2.3). The situation with regard to AlphaBay appears slightly different, with revenues more evenly distributed between cannabis, cocaine and other stimulants; and with a second tier (opioids, hallucinogens and dissociatives) also fairly evenly distributed. The Netherlands appears to sell significantly less cannabis than other countries and, proportionally, more cocaine and stimulants. France, the fourth country on the list, seems to generate a relatively high amount of revenue from opioids. Overall, the value of NPS sales remains quite small (in the order of EUR 100 000-EUR 300 000 for the leading countries); however, it is possible that some novel opioids that could be classified as NPS are instead classified under the general term opioids.

Volume analysis

Figure 2.12 shows a breakdown by weight (kg) of drugs sold. The results are generally consistent with those of Figure 2.10: Germany (2 130 kg overall), the Netherlands (1 392 kg overall) and the United Kingdom (1 352 kg overall) dominate; these are the only countries where the weight of products shipped exceeds, in aggregate, a metric tonne. Interestingly, the United Kingdom generates more revenue per volume of drug sold than other countries. In particular, the volume of stimulants from the United Kingdom is much smaller than the volume from Germany and the Netherlands, yet the revenue is only slightly less. A manual inspection of results reveals that, while Germany and the Netherlands primarily focus on sales of MDMA/ecstasy tablets, the United Kingdom tends to sell more stimulants such as methylphenidate, amphetamine and dextroamphetamine, the individual unit sizes sold of which are much smaller than those of MDMA and ecstasy, but are a similar price.

Comparison with non-EU sales

Figure 2.13 compares sales originating from the EU (plus Norway and Turkey) with those originating from other countries, both for the drugs in the seven categories of interest and for all products. The first observation is that drug sales on AlphaBay constituted an overwhelming majority (> 90.0 %) of all sales originating from the EU during this period. This is less so for sales originating from the rest of the world (76.0 %), which makes sense for reasons related to the origin of digital goods, as noted in Section 2.1.

EU countries accounted for 28.4 % of all revenue and 24.4 % of all volumes sold on AlphaBay between 2015 and 2017.

New psychoactive substances

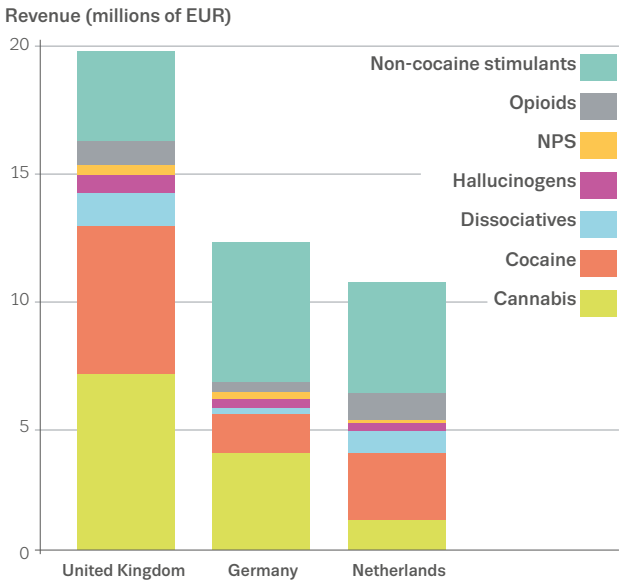
In an effort to compare data from AlphaBay with those from older marketplaces, this section focuses on NPS. The data presented in Figure 2.5 (Section 2.1) show that NPS accounted for a very small fraction of all drug traffic on online anonymous marketplaces — probably less than EUR 3 000/day — during the period examined (2011-2015).

Figure 2.14 provides a finer-grained view of the sales of NPS specifically on AlphaBay, over time, as a stacked plot. It can be seen that NPS sales have remained modest, and are in line with that observed for the 2011-2015 interval (Figure 2.5, Section 2.1). Most NPS originate primarily from the United Kingdom and Germany, with the Netherlands a distant third. It is emphasised again that many NPS opioids (e.g. fentanyl derivatives) may in fact be labelled as opioids by the classifier, rather than as NPS, which could result in an underestimation of NPS sales. Most NPS sold on AlphaBay (and classified as such) appeared to be hallucinogens.

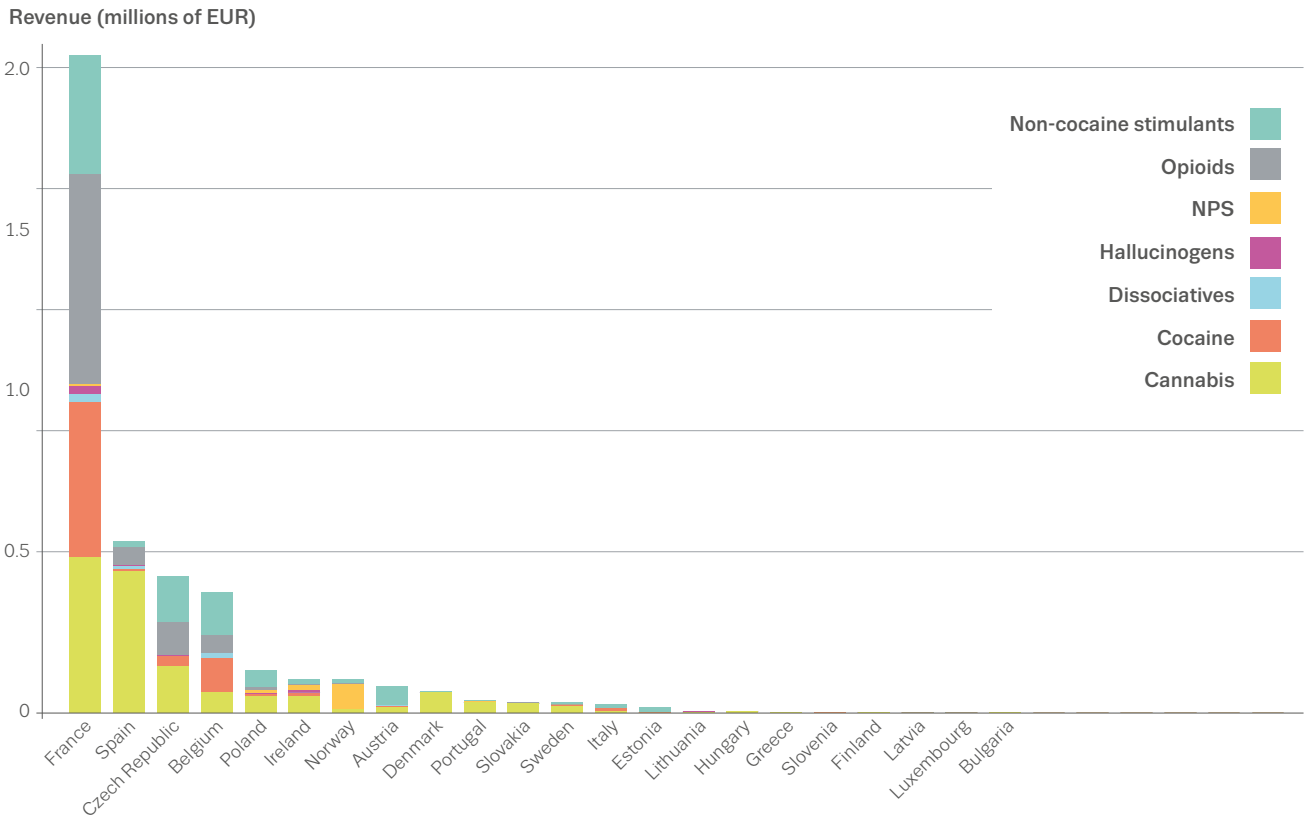
FIGURE 2.11

Breakdown of AlphaBay sales revenue originating from the EU, Norway and Turkey by country, 2015-2017

a) Breakdown by revenue (major countries)



b) Breakdown by revenue (other countries)

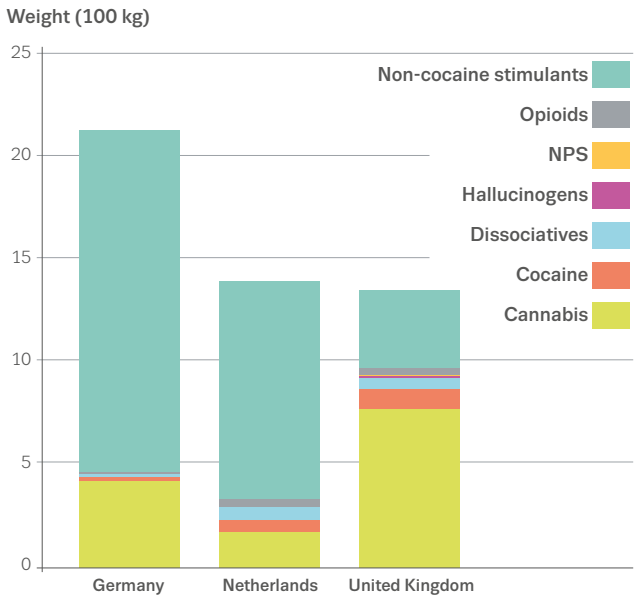


Note: For readability, the three major countries (the United Kingdom, Germany and the Netherlands) are represented on a different scale.

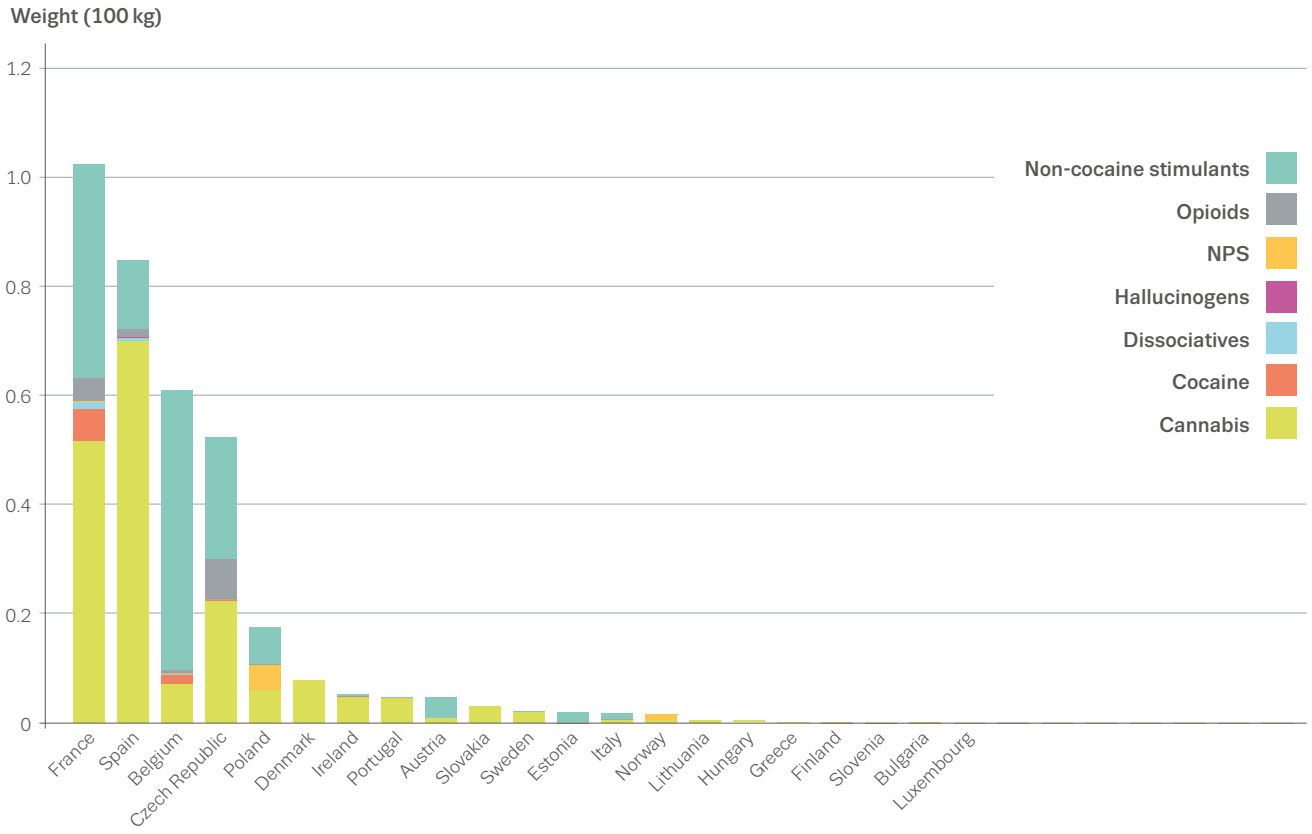
FIGURE 2.12

Breakdown of AlphaBay sales volumes originating from the EU, Norway and Turkey by country, 2015-2017

a) Breakdown by volume (major countries)



b) Breakdown by volume (other countries)



Note: For readability, the three major countries (Germany, the Netherlands and the United Kingdom) are represented on a different scale.

FIGURE 2.13
Comparison of drug sales and other AlphaBay sales in the EU and the rest of the world, 2015-2017

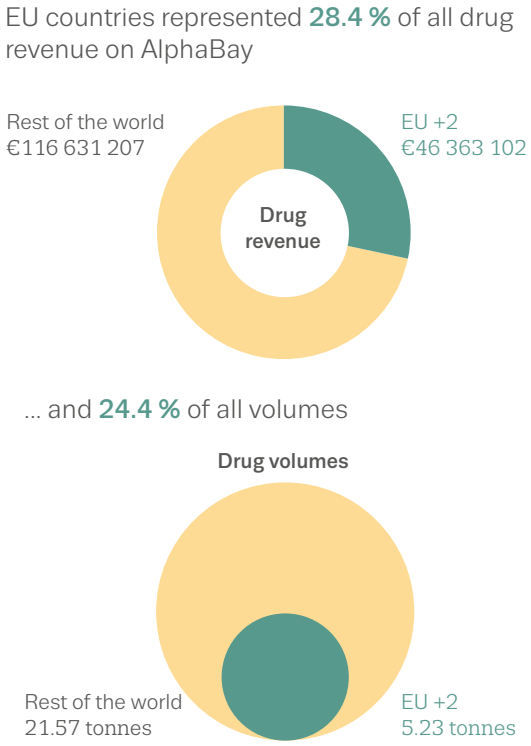
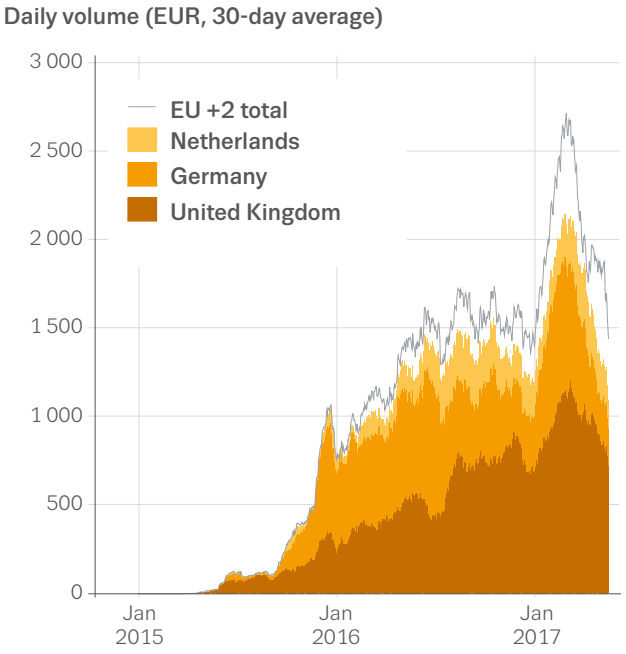


FIGURE 2.14
Breakdown of AlphaBay NPS sales originating from the EU, Norway and Turkey



Transaction amounts broken down by drug and by quantities sold

This section looks at the transaction amounts broken down by drug and by typical quantities sold, along with an indication of how things compare with the findings on the darknet ecosystem as a whole over the 2011-2015 period.

With regard to cannabis, the majority of sales were of small quantities, with only a small number of high-volume sales observed. Table 2.8 provides information about the most common units of cannabis product, cocaine and ketamine. For all these drugs, the most common unit sold is 1 g. There appears to be a modest volume-discounting effect.

The results closely mirror those of the findings reported in Section 2.1. The high standard deviations can be explained by the large dispersion due to a range of different products (oils, edibles, etc.) being classified as cannabis.

Drug sales across the different market levels

Figure 2.15 shows that, for cannabis and cocaine, most transactions occur at the retail level, and retail-level transactions account for the greatest proportion of all revenue. In contrast, for opioids and MDMA a greater proportion of transactions occur at the middle-market level. Importantly, for these two drugs the revenues generated at the middle-market level are higher than those generated as a result of retail transactions. For MDMA and opioids, therefore, darknet sales appear to be associated with supply for secondary distribution more than is the case for

TABLE 2.8
Prices of the most common units sold on AlphaBay: cannabis products, cocaine and ketamine

Drug	Total number of all items for this drug class	Most common unit sold (g)	Number of items and percentage of items in this weight category	Mean price (EUR) (standard deviation)
Cannabis products	8 244	1	1 239 (15.0 %)	12 (± 20)
		5	976 (11.8 %)	49 (± 28)
		10	910 (11.0 %)	86 (± 204)
Cocaine	2 546	1	626 (24.6 %)	68 (± 22)
Ketamine	709	1	158 (22.3 %)	30 (± 13)

cannabis and cocaine. This assumes however that high-volume purchases are more likely to be sold on rather than stored for personal use over time. Middle-market purchases of MDMA were defined, for the purposes of this study, as purchases of between 10 g and 1 kg (or 50-1 000 tablets). While it is possible that purchases of this magnitude would be for personal use, it is likely that a significant proportion of these purchases will be intended for secondary supply or could represent a group-purchasing approach. This finding requires further investigation, as it may be associated with a number of factors. Europe is a major producer of MDMA, and this may be important here. Alternatively the MDMA supply market may be structured in ways that make online sales more attractive. With respect to average drug prices across the different market levels, these data show that any discounting that may occur is likely to be for sales at the middle-wholesale level. The figures for opioids are more difficult to interpret because of the different substances included in this category and the relatively low cut-off volume used to define middle-level sales (1 g). No wholesale opioid transactions were detected; however, two large-volume sales of opioid cutting agents are apparent.

Vendor diversification

Diversification in terms of the volumes offered

The results for the diversification of vendors in terms of the volumes offered are nearly identical to those reported in Section 2.1. That is, an overwhelming (≈90 %) majority of cannabis vendors sell within only one volume tier (for drug-quantity tier definitions, see Section 2.1, Table 2.4). The rest of the vendors' sales are more spread out across the volume tiers, but, in general, sales by a single vendor appear to be confined to no more than two tiers. In other words, most vendors stay within a single volume tier, a minority of vendors sell across two tiers, and almost no vendor has meaningful sales across three tiers. It is quite rare for a vendor to sell both bulk-sized quantities and small volumes at the same time, but some vendors selling larger quantities sometimes also offer 'testing samples' to their customers. More diversity among opioid and cocaine vendors is apparent in this analysis than was apparent in the entire ecosystem analysis for 2011-2015 (Section 2.1). In particular, a number of sellers sell across more than one tier, some giving out free (or cheap) samples, and some also sell in much larger quantities. As in the earlier analysis (Section 2.1), most diversity is apparent for stimulants other than cocaine, with most vendors sticking to the retail tier, but some vendors selling across multiple tiers with a number of items in each tier. This can be explained by the ease of stealthily shipping fairly large quantities of stimulant tablets. Likewise, the diversification of hallucinogen sales in terms of the volumes offered by vendors is almost the same as that reported in Section 2.1.

Vendors selling in multiple echelons tend to be 'superstores' — they carry more than one type of drug and are also are more likely to sell higher volumes. In contrast, vendors who stick to one echelon (typically the lowest one) tend to specialise in one item, and to have relatively low sales volumes. In other words, vendor behaviour on AlphaBay during the 2015-2017 period, overall, was not much different from vendor behaviour in 2011-2015, based on previous measurements of the entire ecosystem (see Section 2.1).

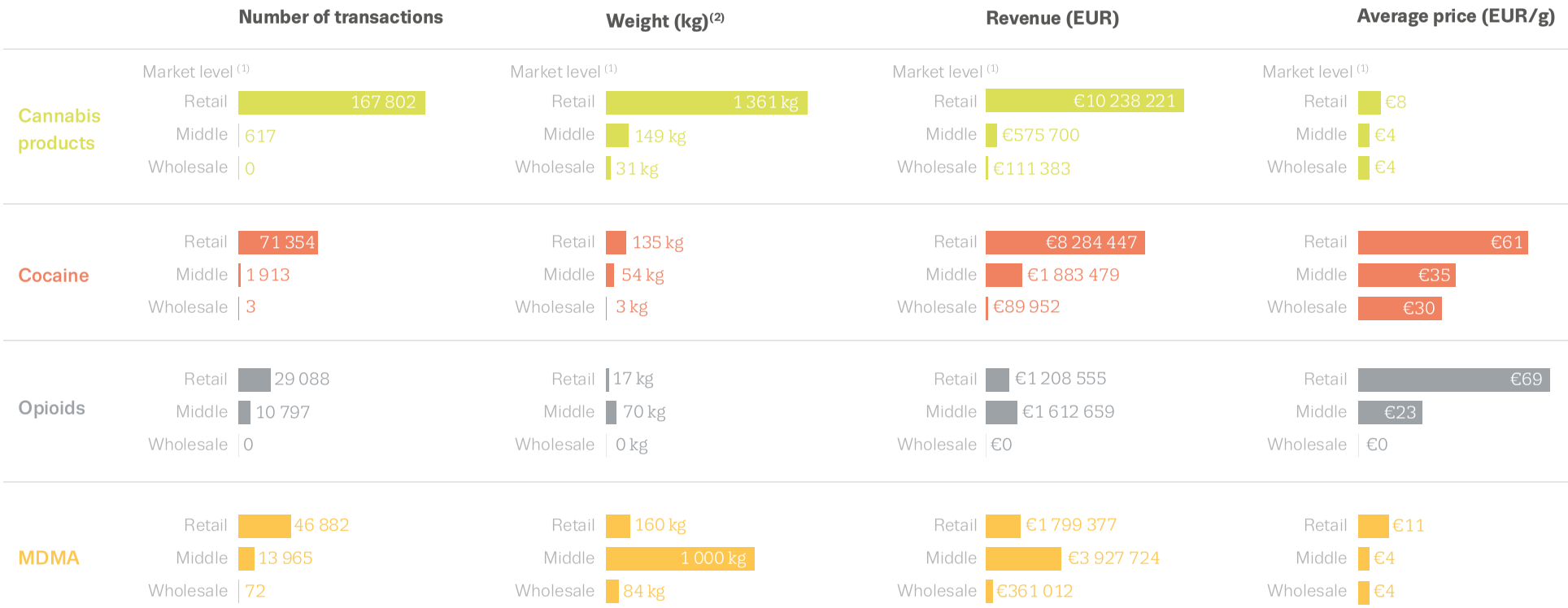
Diversification in terms of the products offered

In all, 1 956 AlphaBay vendors reportedly shipped from the EU. With regard to the diversity of the products being sold, approximately half of these vendors specialise in one category only — this is frequently the case for cannabis (329 vendors) and stimulants other than cocaine (225 vendors), which is unsurprising given that those are very frequently sold items. On the other hand, only 59 vendors specialise in opioids only. The other half of vendors are far more diverse, and typically those vendors sell drugs from a couple of categories. For instance, vendors selling dissociatives, hallucinogens or NPS rarely sell from only these categories. A very small number of vendors sell drugs from all categories, typically individual or small doses only.

Of the 1 956 EU vendors, 1 321 sell drugs from one of the seven categories of interest. Of those, 171 (13.0 %) also sell other types of drugs (e.g. prescription drugs); and 464 (35.1 %) also sell non-drug products (e.g. digital goods). This diversity is consistent and comparable to previous findings (see Section 2.1). Of the 464 vendors selling drug and non-drug items, 133 (28.7 %) are confined to one drug category (primarily cannabis and stimulants other than cocaine); and 93 (20.0 %), on the other hand, are more diverse with regard to the types of products sold, selling multiple drugs along with non-drug products.

FIGURE 2.15

Breakdown of AlphaBay sales by market level



Notes:

(1) For market-level definitions, see Section 2.1, Table 2.4.

(2) The weight is defined as the product of the unit weight and the number of units; for example, a sale of 1 000 tablets of 200 mg MDMA would be considered as 200 g of MDMA; the information presented here is based on a subset of all transactions between March 2015 and May 2017 — those for which the weight could be identified; while outliers were removed, parsing errors may have introduced some error in the weight computations; the figures are inclusive of items sold for USD 10 000 or more.

3

CHAPTER 3
Law enforcement perspectives

This chapter reviews online anonymous markets from an operational law enforcement perspective, elaborating on the challenges but also successful recent action — thus informing the discussion on future interventions in this area.

3.1 The threat

The darknet has emerged as a key platform to offer all types of illicit goods and services. Difficult to police yet easy to access, the darknet provides an ideal environment for the distribution of all types of illicit commodities including drugs, firearms, counterfeit goods and fraudulent documents. The number of goods on offer and the frequency with which new products become available indicates that the darknet trade in illicit goods is thriving and highly dynamic. Europol's 2017 Serious and Organised Crime Threat Assessment (SOCTA) identified the online trade in illicit goods and services as one of the engines of organised crime, which continues to drive organised crime forward (Europol, 2017a). The online trade in illicit goods and services increasingly shapes business models and dictates the way in which successful OCGs operate.

The trade in illicit drugs is the mainstay of most major darknet markets. The majority of activity on darknet markets is drug related (see Figures 1.1 and 2.9). Research suggests that the total monthly illicit drugs revenue of the top eight darknet markets ranges between EUR 10.6 million and EUR 18.7 million (RAND Europe, 2016). It is estimated that the top 1 % most successful vendors are responsible for 51.5 % of all transactions on darknet markets (Soska and Christin, 2015). While it is assessed that the majority of vendors are lone offenders, dealing in small amounts, it is assessed that many of the 'top sellers' are likely to be OCGs earning significant profits. Law enforcement authorities across the EU have noted a significant increase in the number of cases involving the trade in illicit drugs on darknet markets over the last four years. The proportion of illicit drugs traded online remains small compared with the proportion traded through traditional distribution and trafficking networks, and it remains to be seen whether this new channel of supply will supplement or otherwise affect drug demand. Law enforcement authorities expect this phenomenon to continue and online markets to expand and, in some case, possibly even replace the use of traditional distribution networks by some user demographics.

While it is recognised that the scope of drug trade on the darknet is expanding and that darknet markets have the potential to displace (segments of) existing traditional drug markets in the EU, the overall interplay and relationship between the drugs trade via darknet markets and the traditional 'offline' drugs trade is still poorly understood by law enforcement authorities.

Finnish customs uncover major online drug network

In August 2016, the Finnish Customs Board dismantled a network involved in the trafficking and distribution of illicit drugs on the darknet. The network had emerged as the largest darknet vendor on the Nordic market. Finnish customs suspects that this network may have imported up to 40 000 ecstasy tablets, 30 000 LSD blotters and 40 kg of other drugs including amphetamine, methamphetamine, heroin, cocaine, MDMA, alpha-PVP and MDPV into the country.

The vendor profile had been in operation since 2014 on the Silk Road market on the darknet.

Source: Yle Uutiset (2016).

A polydrug trade paradise

All types of illicit drugs consumed in the EU are traded on darknet markets. The drugs trade, online and offline, is highly polycriminal. In terms of traditional drug trafficking, more than 75 % of the OCGs involved in the trafficking of one drug also traffic and distribute other types of drugs. Around 65 % of the OCGs involved in the drug trade are simultaneously involved in other criminal activities such as the trade in counterfeit goods, trafficking in human beings (THB) and migrant smuggling.

Darknet markets are tailor-made polycriminal environments. While some markets specialise in specific or niche commodities, the largest and most successful darknet markets either offer all types of illicit commodities or restrict themselves to distributing all types of illicit drugs.

The variety of illicit drugs on offer on darknet markets significant and greatly exceeds that available to individual users through street distribution.

Darknet drugs and arms vendor arrested by Slovak authorities

In May 2017, Europol supported Slovak law enforcement authorities in their investigation into a Slovak national who had been trading firearms, ammunition and drugs on the darknet.

In one of the locations searched, Slovak authorities discovered and seized five firearms and approximately 600 rounds of ammunition of different calibres. The investigators also found a sophisticated indoor cannabis plantation, 58 cannabis plants and a bitcoin wallet containing bitcoin worth EUR 203 000, which is thought to have been obtained from illicit online activities.

In addition, Slovak authorities and Europol dismantled an online drugs marketplace that was hidden on the darknet and which the individual arrested had been running as an administrator and operator since 2015. At least 10 kg of cannabis had been purchased through this channel.

In addition to darknet trading in both firearms and drugs, firearms are sometimes used by those involved in the drug market and, unsurprisingly, there are reports of drugs and firearms being smuggled together (Europol, 2017b).

Investigations into vendors operating on darknet markets have revealed a significant polycriminal element to the trade in illicit commodities on the darknet. Some vendors dealing in drugs have also been found to be involved in the trade in illegal firearms, payment fraud and cyber-dependent crimes (offences that can be committed only using a computer, computer networks or other forms of information and communications technology) such as selling malware solutions or other toolkits. Many of these criminals or criminal groups operate using a crime-as-a-service business model. This model mirrors the business-to-business approach in the licit economy. Criminals primarily, or in some cases exclusively, provide criminal services, such as toolkits used for fraud or cyber-dependent crimes, to other, less sophisticated criminals. This model has also seen the proliferation of subscription-based models, which allow criminals to 'rent' cybercrime tools for a limited period, making these tools more affordable.

Many vendors offering illicit drugs on darknet markets operate polydrug businesses. While vendors of cannabis products largely confine themselves to distributing cannabis products, vendors selling other substances, such as cocaine or opioids, frequently offer different types of illicit drugs. This is particularly highlighted by the AlphaBay case study (Chapter 2, Section 2.3).

Perhaps like no other substances, despite the comparatively low volumes traded, NPS in particular have been associated with the expanding variety of substances offered on darknet markets. In some Member States, NPS are now almost exclusively distributed online. Prior to their prohibition, NPS are distributed on platforms on the surface web. However, once an NPS becomes a controlled substance under EU legislation, their distribution moves to darknet markets. The trade in NPS on darknet markets is expected to further expand, increasing the availability of all types of NPS over the coming years.

Law enforcement authorities have noted an increase in the availability of cannabis, both resin and herbal, on darknet markets over the last four years. In addition to their availability on surface web platforms, cannabis seeds are also offered widely on darknet marketplaces.

Wholesale distribution?

The analysis of data from darknet markets taken down by law enforcement authorities, such as Silk Road 2.0 and others, reveals the extent of trading activity, including information on the geographical location of vendors, if provided, and the number of transactions, the nature of the goods sold and the amounts paid. However, some trading,

Substantial profits

The revenues and profits of vendors on darknet marketplaces can be substantial.

In 2016, German law enforcement authorities arrested four suspects accused of distributing illicit drugs via darknet marketplaces between 2013 and 2016. The group had distributed illicit drugs exceeding a value of EUR 1.27 million to customers in 62 countries using post and parcel services (Focus Online, 2016).

Other successful vendors on darknet marketplaces are able to sell relatively large amounts of illicit drugs, generating even more substantial profits.

especially the trading of wholesale quantities, is believed to be conducted via private messages after initial contact has been established between vendors and customers in response to darknet market listings. These messages are typically encrypted and require significant effort to decrypt. Even in the cases where encryption can be overcome, law enforcement authorities face additional challenges in the analysis of the communications data.

As already noted in Section 2.3, the wholesale of different drugs on darknet markets via listings appears to be limited; most transactions involve smaller quantities for individual use by consumers. However, repeated sales by individual vendors suggests that they have access to larger quantities of illicit drugs to sustain their businesses and meet customer demands. In many cases, it is unclear where these vendors obtain their supply, although they probably interact and trade with established OCGs involved in the traditional wholesale trafficking of illicit drugs. The nature of the links and the engagement between vendors on the darknet and 'traditional' drug traffickers remains a significant knowledge gap.

Vendors: individual criminals and organised crime groups

Darknet markets are dynamic environments with a significant number of vendors entering and leaving markets based on the availability of their stock and profit opportunities. Initially, most vendors on darknet markets were individual sellers, distributing limited amounts of different substances based on their availability. In addition to a high number of lone offenders, who deal in relatively small quantities of drugs, there are so-called 'top sellers', some of whom use organised structures and earn sizeable profits.

Darknet markets offer a convenient and safe distribution platform to individual criminals and OCGs alike. Trading on darknet markets allows distributors to reduce the risk of detection while being able to advertise to a large number of potential clients. Vendors can sell significant quantities of drugs as part of high-frequency, low-quantity transactions. For example, the most commonly sold unit of cocaine on the AlphaBay darknet market in 2011-2015 was 1 g (see Section 2.3, Table 2.8).

Organised crime involvement

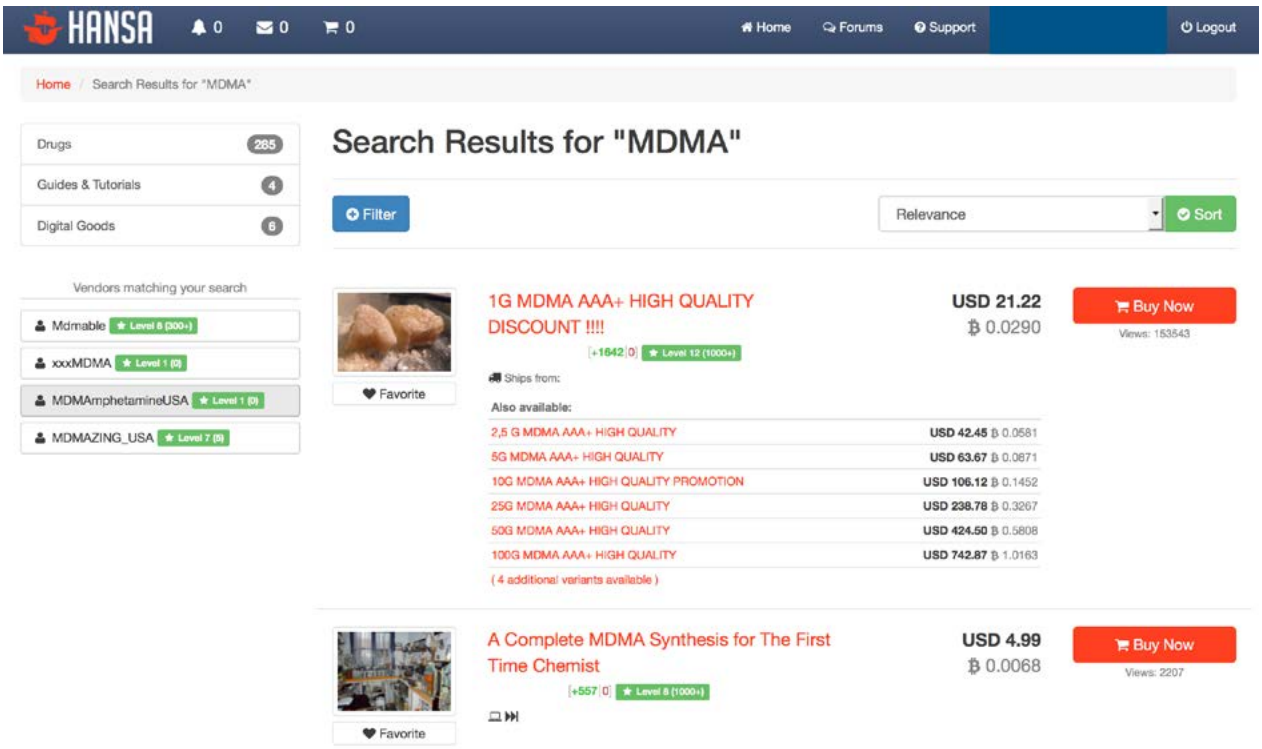
There has been a substantial increase in the number of transactions involving drugs over the past years, and the number and quantities of individual sales is set to continue to grow. While the quantities of individual sales on darknet marketplaces remain relatively small, the overall volume of drugs traded online points to the involvement of OCGs, which are able to procure larger quantities of drugs and distribute them to individual buyers. Nonetheless, there are notable examples of vendors who do not fit the traditional profile of organised crime.

Some Member States have observed an increase in the level of professionalism displayed by vendors, which is indicative of the involvement of established OCGs. It is believed that some OCGs involved in the 'traditional' distribution of drugs via street dealers are increasingly using darknet market trading as an additional distribution channel and revenue stream. This professionalisation is also driven by the competitive nature of trading on darknet markets, which forces vendors to innovate and deliver a customer-focused service offering.

Recent investigations highlight the move of OCGs involved in the large-scale production of herbal cannabis in the EU to darknet markets for the distribution of their production output. In addition to the obvious benefits of mitigating the risk of law enforcement detection and reducing costs, this additional distribution platform allows OCGs to gain access to an additional client base, while maintaining their established distribution networks.

Small and medium-sized OCGs based outside the EU are believed to rely on darknet markets to supply them with synthetic drugs produced in the EU. It is, however, unclear whether the vendors offering these drugs are acting as mid-level suppliers and middle men, or are more closely associated with the OCGs involved in the large-scale production of these substances in the EU. The EU remains a key region for the production of synthetic drugs such as MDMA and amphetamine trafficked to destinations across

FIGURE 3.1
A range of MDMA quantities offered on Hansa



the world. EU-based OCGs dominate the global production of MDMA and amphetamine (EMCDDA and Europol, 2016).

New business opportunities

The diminishing reliance on access to street networks of consumers of illicit commodities may challenge the established business models in many criminal markets. While most illicit trade is still carried out by OCGs, individual criminal entrepreneurs without access to networks of criminal contacts are able to directly enter criminal markets via online trade platforms (see Figure 3.1).

The proportion of drug trade conducted via darknet markets is still limited and has not diminished the role of established OCGs in the large-scale trafficking and production of drugs in the EU, and is unlikely to challenge them in their function as primary wholesale suppliers. However, polydrug-trafficking OCGs involved in the street-level distribution of illicit drugs tied to specific territories or regions may find themselves competing with smaller OCGs focusing on the online distribution of illicit drugs directly to consumers. OCGs operating on darknet markets are not tied to a specific territory and can operate using a much leaner infrastructure.

Resilience

The darknet has proven to be a very resilient environment, able to quickly absorb law enforcement actions such as the takedown of major marketplaces. Following the takedown of a darknet market, trading activities are reduced for a short time. However, vendors and customers alike will quickly migrate to alternative existing or newly emerging darknet markets. The most recent example is the rapid growth of several darknet markets, such as TradeRoute and Dream, following the takedown of AlphaBay and Hansa.

Online vendors have quickly developed countermeasures to protect against the monitoring of online marketplaces and investigations carried out by law enforcement authorities. Such monitoring includes technical investigations of the platforms and trading activity, as well as financial investigations into the money flows associated with the drugs trade on the darknet. For instance, previously, communication between vendors and customers was unencrypted. However, following the major takedowns of Silk Road and Silk Road 2.0, most communication on these platforms is now carried out using multilayered encryption. Similarly, whereas transactions did not previously require multisignature, multisignature transactions are now common to many of the most frequently used darknet markets. In some cases, surface web vendors redirect their customers to mirror sites on the darknet or advertise their products using false product designations or descriptions.

Converting the proceeds of crime

The use of cryptocurrencies is an in-built feature for most darknet markets. Vendors receive payment for their goods in cryptocurrencies such as bitcoin. These funds can be used to directly purchase other goods on darknet platforms or, increasingly, for legitimate purchases. Funds generated from the trade in illicit drugs on darknet markets are generally used to purchase other products, sourcing additional drugs for further distribution, or are converted to traditional currencies as profit.

The cryptocurrencies used for payment on darknet markets are and can be exchanged for fiat currency. The conversion of cryptocurrencies into major currencies such as euros or US dollars allows vendors to use the proceeds of their sales outside the darknet ecosystem.

Virtual currency exchanges act as brokers and allow users to buy or sell virtual money for a variable fee. An exchange works like any other currency exchange: the user converts a fiat currency into a virtual one or vice versa. Alternatively, users can also convert one form of virtual currency to another.

In order to use a virtual currency exchange, users register for an account with the exchange. The majority of popular exchanges require users to provide identification to open an account. Criminals are able to circumvent the pre-set verification processes of exchanges that require identity verification by relying on fraudulent identity documents, which are widely available on darknet markets. Some exchanges now require customers to verify their identity via Skype (or a similar telecommunication software application) or by producing pictures of themselves with their identification documents.

Some exchanges require no verification of identity and have made the protection of the client's identity part of their mission statement. This allows criminals to use the profits generated by trading in illicit drugs on the darknet to anonymously buy and sell cryptocurrencies, converting digital proceeds into analogue profits.

Exchange services accept different payment methods, predominantly bank transfers and credit or debit card payments, for the purchase and sale of cryptocurrencies. Some also offer the use of money service businesses, such as Western Union and MoneyGram, PayPal and bank cheques, and some even dispense cash via cash deposits or cash in mail. Cash, in particular, remains the medium of choice for money launderers and criminals seeking to make purchases or reinvest their criminal proceeds.

Digital money laundering as a service

In July 2017, Greek law enforcement authorities arrested a Russian national wanted in the United States for allegedly leading a substantial money-laundering operation. The suspect is accused of laundering more than EUR 3.5 billion (USD 4 billion) through bitcoin transactions.

Greek law enforcement authorities described the suspect as the leader of a sophisticated criminal organisation that owns, operates and manages 'one of the largest cybercrime websites in the world'.

US authorities allege that the suspect facilitated crimes including hacking, fraud, identity theft, tax refund fraud, public corruption and drug trafficking during his time in the digital currency market.

Source: The Guardian (2017).

Cash continues to play an important role when it comes to realising criminal gains; there are well-established methodologies for laundering cash, and it is as readily exchangeable, untraceable and anonymous as the cryptocurrencies favoured in the digital underground. As a result, virtual currencies have yet to be adopted to any large degree by established money launderers, who are likely to favour long-established methodologies.

Cryptocurrencies are likely to become more attractive, however, both online and offline, with several new currencies already establishing themselves on the criminal markets. Whether or not any of these cryptocurrencies will grow to challenge the role of bitcoin in terms of criminal use will remain to be seen, but some of these alternative cryptocurrencies appear to offer greater anonymity to criminals (see Chapter 1).

While knowledge and experience of how to investigate, trace and seize virtual currencies continues to grow in the law enforcement community, enhanced by various private sector tools for attribution, this is often limited to bitcoin and not the other cryptocurrencies emerging on the criminal markets. Successful law enforcement activity related to bitcoin-using criminals may further lead to more criminals using alternative cryptocurrencies.

Crypto-vulnerabilities

The use of cryptocurrencies is no guarantee of complete anonymity and immunity from prosecution if funds are used for criminal purposes on the darknet.

In February 2017, the Danish National Police Cyber Crime Center (NC3) announced a breakthrough in using new methods to track and identify darknet users. This new technique, which relies on bitcoin transaction analysis, has already been used in practice to identify individuals and help prosecute darknet traders.

Source: Anklagemyndigheden (Danish Prosecutor's Office) (2017).

Take-downs generate intelligence

Early takedowns such as the closure of the original Silk Road have provided law enforcement authorities with much-needed insight into the functioning of the darknet market environment.

Based on analysis of the data obtained from the Silk Road takedown, US law enforcement authorities were able to identify and prosecute one of the platform's top vendors based in the EU. The Dutch national was sentenced to 10 years in prison after pleading guilty to selling 104 kg of MDMA and 566 000 MDMA tablets, 4 kg of cocaine, 3 kg of benzodiazepines, and substantial quantities of amphetamine, LSD and cannabis to customers in the United States.

Source: The Register (2014).

Knowledge gaps

There are significant knowledge gaps around the darknet trade in drugs. While vendor and customer interactions are well researched and understood, there is limited knowledge regarding the actors and mechanisms involved in this trade beyond the distribution/sales phase in the drug-trafficking chain (see Figure 3.2).

The takedown of darknet marketplaces, such as the original Silk Road, Silk Road 2.0, and, most recently, the AlphaBay and Hansa markets, has provided law enforcement authorities with significant insight into the functioning and interactions on darknet marketplaces. Successful follow-up investigations have been able to identify several high-profile vendors, which operated profitable vendor profiles and darknet trading business ventures.

However, some knowledge gaps remain, particularly in relation to the extent of the involvement of traditional OCGs in the darknet trade in illicit drugs and in the financial flows associated with the profits generated on darknet market platforms.

Additional law enforcement actions and follow-up investigations of successful takedowns will probably provide law enforcement authorities with additional insight into this aspect of trade on darknet markets. Law enforcement authorities will need to enhance their intelligence picture and gain a better understanding of the role of the darknet trade in illicit drugs in order to effectively combat this phenomenon.

3.2 Challenges

Law enforcement authorities and prosecution services encounter various challenges in combating cybercrime and especially in pursuing investigations on the darknet.

Eurojust and Europol have jointly identified a number of challenges, which include loss of data, loss of location, legal frameworks, public–private partnerships, international

FIGURE 3.2
Intelligence picture



cooperation and the rapidly developing threat landscape and resulting expertise gap.

Loss of data

Data retention

The overturning of the Data Retention Directive (DRD) by the European Court of Justice (ECJ) in its ruling of 8 April 2014 ([12]) has left law enforcement and prosecutors uncertain about the possibilities of obtaining data from private parties. In some Member States there is legislation in place to ensure that internet service providers (ISPs) retain data for law enforcement purposes, whereas in other Member States national legislation has been annulled in the wake of the ECJ judgment. In those Member States, ISPs retain some data for commercial or accounting purposes, but have no data available to support law enforcement investigations. Such discrepancies impede the work of law enforcement authorities and may result in the loss of investigative leads and ultimately reduce the ability to effectively prosecute online criminal activity.

In its Tele2 Sverige and Watson ruling of 21 December 2016 ([13]), the Court did not go so far as to deem data retention per se unlawful. In interpreting the e-Privacy Directive, the Court highlighted that a Member State is not prevented from introducing legislation that would facilitate the targeted retention of traffic and location data for the preventive purpose of fighting serious crime. It is also very important to acknowledge that the use of retained communications data may help to clear persons suspected of serious crimes without resorting to other more intrusive means of surveillance, such as the interception of communications or house searches.

As described in Europol's 2017 Internet Organised Crime Threat Assessment (IOCTA) report (Europol, 2017c), operational experiences have shown that electronic communication data are key to the successful investigation and prosecution of serious crimes including criminal activity on darknet marketplaces. The lack of the unified retention of electronic communication data across the EU has proven a key obstacle to investigating cross-border cybercrime. Recent developments and case-law with an impact on data retention regulations have presented law enforcement authorities with significant obstacles in their operational work, particularly when it comes to identifying and investigating high-value targets.

Carrier-grade network address translation

This loss-of-data challenge also affects the widespread implementation of carrier-grade network address translation (often called carrier-grade NAT (CGN)) by ISPs. Carrier-grade NAT allows a single IP (internet protocol) address to be shared by, potentially, thousands of subscribers/end users on the same network simultaneously. CGN is used by 95 % of mobile providers (network operators and mobile virtual network operators) and almost 50 % of traditional ISPs worldwide. CGN prevents ISPs and electronic content providers from logging certain types of information, such as source port numbers and destination IP addresses that would otherwise allow law enforcement to associate criminal activity with an end user. Investigators may be confronted with long lists of potentially hundreds or thousands of end users associated with a particular public IP address, the investigation of which requires many resources, incurs large delays, and generates privacy and data protection issues for many innocent customers.

Encryption

A growing number of electronic service providers implement default encryption for their services. At the same time, tools that enable personal encryption of communications and other data are widely available and promoted. While this counts as a positive development towards increasing cybersecurity in general, the possibilities for digital forensic analysis are negatively affected as a result of the increased implementation of encryption. This leads to a situation where criminals are able to effectively and indefinitely hide critical evidence and activities from law enforcement. More than three quarters of cybercrime investigations in the EU involve the use of some form of encryption to protect data. Almost half of the Member States also noted the increased use of encrypted email. The growing use of encryption by criminals to protect their communications or stored data can lead to the loss of critical intelligence and evidence. The increase of operational security measures, such as the use of multi-layered encryption among criminals, creates serious challenges for investigators.

([12]) ECLI (2014), European Case Law Identifier, Judgment of 8 April 2014, ECLI:EU:C:2014:238 (case C-2A93/12).
([13]) ECLI (2016), European Case Law Identifier, Judgment of 21 December 2016, ECLI:EU:C:2016:970 (cases C-203/15 and C-698/15).

Virtual currencies

The widening use of decentralised virtual currencies by criminals and the increased use of tumbling/mixing services effectively prevent law enforcement agencies from 'following the money' and significantly hinder asset recovery and the prevention of fraudulent transactions. The lack of (minimum) standards of due diligence and know-your-customer ([14]) processes for such services and the non-application of existing regulations compound the problem. A growing number of investigations involving cryptocurrencies and blockchain analytics highlights the need for expertise, tools and legislative and regulatory means to 'follow the money' to be at the disposal of law enforcement and judicial authorities.

Loss of location

Recent trends such as the increasing use of encryption, anonymisation tools, virtual currencies and the darknet by criminals have led to a situation where law enforcement may no longer be able to (reliably) establish the physical location of the perpetrator, the criminal infrastructure or the electronic evidence. This loss of location is a substantial barrier to effective investigations and prosecutions. In such situations, it is often unclear which country has jurisdiction and what legal framework regulates the collection of evidence or the use of special investigative powers, such as the monitoring of online criminal activities and various undercover measures. The growing use of cloud-based storage and services means that data can be located in physically different jurisdictions.

In addition to jurisdictional issues, loss of location also presents significant challenges during the investigative phase. It is increasingly difficult to establish the physical location of the servers hosting darknet markets and to map a market's infrastructure.

Legal framework

Differences in legislation

Despite the existence of international legislative instruments, differences between domestic legal frameworks in the EU Member States and international instruments often prove to be a serious impediment to international criminal investigation and the prosecution of crimes with an online dimension, such as the trade in illicit drugs on darknet markets.

([14]) As an example, see the recommendations proposed by the Financial Action Task Force (available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf).

The main differences relate to the criminalisation of conduct and the provisions to investigate cybercrime and gather electronic evidence. The adaptation and alignment of these legal frameworks is often time-consuming and difficult because of the rapid evolution of the online threat landscape. Existing operational processes could be harmonised and streamlined, and forensic-technical standards for the collection and transfer of electronic evidence could be developed.

The proliferation of the internet, its impact on traditional types of criminality such as the trade in illicit drugs and the growing sophistication of cybercrime require dedicated legislation that regulates law enforcement presence and action in an online environment more specifically.

Online investigations

Similarly, there is a growing need for a harmonised legal framework at EU level for conducting online investigations (Council of the European Union, 2016a), which would allow more effective joint operational actions such as large-scale botnet and/or underground criminal forum takedowns. The lack of the harmonisation of efforts to monitor online criminal activities and to lawfully collect critical evidence on darknet markets hinders effective operational activities and complicates the subsequent presentation of evidence in judicial proceedings. In response to these challenges, the European Commission will put forward a new legal instrument to regulate the use of electronic evidence in early 2018.

In some cases, investigators may be deterred from carrying out investigations on the darknet because of a lack of awareness of the tools available to them. In many jurisdictions, the monitoring of darknet marketplaces requires no special covert activity on the part of the investigator beyond the use of an anonymous account.

International cooperation

The collection of electronic evidence is often a time-sensitive issue. The current process of mutual legal assistance (MLA) is perceived by practitioners as being too slow and cumbersome to gather and share evidence effectively. MLA is a method of between-state cooperation, used to obtain assistance in the investigation or prosecution of criminal offences. MLA is generally used to obtain material that cannot be obtained on a police-cooperation basis, particularly material that must be obtained by coercive means. Because of the differences in legal systems and frameworks, the early coordination and involvement of

the judicial authorities is necessary. There is a clear need to streamline the MLA process wherever possible, for instance by aligning and using existing model requests and using a common taxonomy of cybercrime terminology. The implementation of the European Investigation Order (EIO) Directive may go some way towards addressing these issues for the majority of Member States. However, the EIO framework may not accommodate the speed that is required to capture electronic evidence. The EIO Directive also does not contain provisions that specifically facilitate the collection of common types of electronic evidence, meaning that additional tools need to be developed to facilitate the collection of electronic evidence under the EIO framework.

The various existing legal tools and mechanisms could be better promoted at international level. There is also a clear need for a better mechanism for cross-border communication and the exchange of information for the purpose of investigation, prevention and protection, but also to ensure that any ensuing MLA request conforms with all the relevant legal requirements of the country in question.

The current differences in legal frameworks and the existing challenges to effective international cooperation may lead to the emergence of virtual safe havens in the online environment, where criminal investigation and prosecution as well as evidence collection are challenging. By design, the darknet is an environment that, while not impenetrable by law enforcement authorities, does function to hinder monitoring and investigative efforts.

Skills gap

Cybercrime and online criminality are evolving rapidly, at a scale and speed never before seen, making it difficult for law enforcement and prosecutors to keep pace. Current and expected trends require an increasing level of practitioner expertise. Currently no EU-wide standards for the training and certification of such practitioners exist. Nonetheless, existing initiatives at EU level, such as the European Cybercrime Training and Education Group (ECTEG), the Training of Trainers (TOT) Project and the training activities under the EMPACT (European Multidisciplinary Platform Against Criminal Threats) policy framework carried out in cooperation with CEPOL (the European Union Agency for Law Enforcement Training), are already paving the way towards addressing the expertise gap at EU level. Still, the alignment of existing programmes within Member States and the implementation of current EU-wide initiatives is necessary. Other training and capacity-building initiatives also exist at international level, supported by organisations such as Interpol and the United Nations Office on Drugs and Crime (UNODC).

3.3 Responses

Criminality on the darknet is rapidly evolving, and law enforcement authorities are confronted with an increasing number of cases and incidents related to criminal activity taking place on the darknet and darknet markets. Criminality on the darknet is truly global in scope and affects all EU Member States. Despite growing recognition that darknet markets are emerging as key distribution platforms for illicit drugs, the level of response and the capacities deployed to fight this phenomenon vary considerably across the EU.

Illicit drugs are the main commodity sold on the darknet. However, in most cases drug units investigating the trafficking and distribution of drugs still focus on traditional drug-trafficking activities and distribution. While this arguably reflects the relatively small proportion of illicit drugs traded on the darknet, it is clear that this and similar platforms provide convenient, new and innovative opportunities for the drugs trade and that there has been a noticeable increase in the number of these cases.

Law enforcement authorities in the EU have followed a number of strategies to counter the trade in illicit drugs via darknet markets (RAND Europe, 2016), as discussed below.

Traditional investigative techniques

Investigations into the trade in illicit drugs on the darknet have presented law enforcement authorities with challenges. Traditional investigative techniques typically applied for investigating the drugs trade focus on targeting OCGs and individuals using interception of communication, surveillance and other techniques. While these 'traditional' drug-trafficking organisations increasingly rely on online technologies to communicate more securely, much of their business still concerns the moving of physical commodities. Drugs investigators often seem to be ill-equipped to deal with the trade in drugs on the darknet, which requires investigative techniques and expertise more typically found within units combating cybercrime.

While additional cyber-related expertise is required to identify vendors operating on darknet marketplaces, these traditional investigative techniques remain valuable and essential for follow-up investigations and to build strong cases against darknet market vendors.

Postal detection and interception

The trade in illicit drugs on darknet markets is intimately linked with an increase in the distribution of illicit drugs via post and parcel services. The possible detection of drug shipments bought on darknet markets is a key vulnerability of the darknet trade in drugs. While online purchases can be anonymised to a large degree and represent significant, but not insurmountable, obstacles for the identification of vendors and customers, the physical parcels need to be submitted and received at specific locations (Figure 3.3).

Vendors have developed various countermeasures to prevent the detection of parcels containing drugs. These involve the concealment of the substances in parcels and their incorporation into parcels with other goods, as well as the use of distraction packages containing small amounts of illicit drugs to divert the attention of law enforcement authorities from the 'real' shipment. These techniques largely mirror those employed by OCGs in the traditional trafficking of illicit drugs.

The overall volume of legitimate parcel traffic has increased significantly over recent years and prohibits the use of systematic and effective control measures by law enforcement authorities to identify and intercept all but a few suspicious parcels. So far, the risk profiling of parcels, akin to the methodologies used to identify suspect cargo shipments, has proven difficult because of the volume of regular parcel traffic.

Law enforcement authorities closely monitor developments in this area and cooperate with the private sector, including major transportation and logistics service providers, in order to identify and intercept potential drug shipments. The use of traditional forensic investigation techniques, such as the fingerprinting of parcels, first requires the successful identification of drug shipments. Increasing the rate of detections in combination with the efficient use of information exchange systems by law enforcement authorities to share forensic data could aid investigations into the darknet trade in illicit drugs. Enhanced cooperation between police and customs authorities in carrying out controlled deliveries and implementing other mitigation strategies will also strengthen the law enforcement responses to the online trade in illicit drugs.

Some new approaches to the shipping of parcels with complete anonymity potentially offer an opportunity for vendors and buyers of illicit goods on darknet markets to overcome the vulnerability of trafficking physical goods using parcels. The first proofs of concept of blockchain-based anonymous physical package delivery systems have been developed by academia (AlTawy et al., 2017). The implementation of such systems would probably further hinder the efforts of law enforcement authorities to intercept drug shipments and identify the vendors of illicit drugs on darknet markets.

FIGURE 3.3

Envelope with Amsterdam postmark containing MDMA purchased online and delivered to a customer in Austria



Source: Bundeskriminalamt, Austria.

Operation Porto

In May 2017, Austrian and German law enforcement authorities concluded Operation Porto, which targeted vendors and customers purchasing illicit drugs on darknet markets.

The operation resulted in the initiation of 697 investigations into individual suspects, as well as the seizure of 35 kg of various types of drugs in Austria.

The operation also highlights the close link between the darknet trade in drugs and parcel trafficking. Control actions carried out as part of the operation in Germany resulted in the seizure of 6 000 parcels containing more than 175 kg of drugs. The recipients of the parcels were based in 60 countries worldwide.

Source: Der Standard (2017).

Monitoring darknet markets

Law enforcement authorities in the EU actively monitor online marketplaces to identify trends, such as the most popular darknet markets, the substances traded, the most prolific vendors active on specific darknet markets, price

developments, the flow of virtual currencies and other innovations in this area.

The regular monitoring of darknet markets yields intelligence on top vendors, prices, available substances and other trends. However, an efficient law enforcement response requires a multidisciplinary approach and multi-agency cooperation including follow-up investigations to convert intelligence gathered online into concrete investigative leads such as the identity of vendors.

Cyberpatrol actions bring together experienced investigators and experts in an intelligence-gathering exercise to map out criminality on the darknet. The objective of these exercises is to identify actors and targets active on darknet markets, as well as to support investigators in prioritising targets and deconflicting investigations. A good intelligence picture allows law enforcement authorities to focus resources and activities on investigating the most active and prolific vendors. The deconfliction of investigations is essential to prevent interference from different investigations.

Cyberpatrol actions allow law enforcement authorities to gather intelligence and identify high-value vendors and targets and their criminal activities, with the objective of initiating follow-up investigations and operations. Overall, these actions contribute to the development of a common law enforcement approach as well as innovative tools, techniques and tactics to combat criminality on the darknet and to deter criminals from becoming active on darknet markets.

These actions significantly improve the cooperation between investigators targeting different types of criminality, including drug trafficking, firearm trafficking, the distribution of counterfeit documents and the trade of any other illicit commodities on the darknet.

Operation Hyperion

In October 2016, law enforcement authorities from across the world came together to carry out Operation Hyperion. The operation targeted buyers and sellers of illicit drugs, weapons and fake and stolen identities, and other illicit activities using darknet marketplaces.

As a result of Operation Hyperion, Swedish law enforcement authorities arrested Sweden's largest suspected darknet marketplace vendor, suspected of making millions of Swedish kronor in profit by distributing illicit drugs in the country and to customers outside Sweden (DeepDotWeb, 2016).

As part of Operation Hyperion, the National Prosecution Service of the Netherlands launched a hidden service to showcase the detection and prosecution of many large vendors on darknet markets.

Operation Hyperion was carried out by law enforcement authorities in Australia, Canada, Finland, France, Ireland, the Netherlands, New Zealand, Spain, Sweden, the United Kingdom and the United States, and was supported by Europol.

The takedown of a darknet market provides investigators with a rich data source. Exploring and analysing the accumulated data gained from several takedowns in a central database generates investigative leads. The planning and execution of Operation Hyperion was made possible by analysis of data obtained through Operation Onymous and other investigations into darknet trading activity.

Disrupting darknet trade

The disruption of darknet markets is a key area of activity for law enforcement authorities in the fight against the online trade in illicit goods. In many cases, these actions have targeted the largest darknet markets in terms of the number of vendors, sales and products on offer.

Overall, these actions have disrupted the online trade in illicit drugs and reduced overall trade activity. They have also generated intelligence and investigative leads, allowing investigators to focus on the most successful vendors and the most active buyers. Disrupting darknet trade also undermines customer confidence in the reliability and availability of darknet markets.

While this approach has delivered the desired short-term objective of disrupting online trading activity, it has also revealed the resilience of darknet market trading. Once a major marketplace has been taken down, vendors and customers quickly migrate to alternative platforms.

Recent high-profile international operations, such as Operations Onymous, Bayonet and GraveSac, have generated substantial intelligence and awareness of the quickly expanding scope of the trade in illicit drugs on the darknet.

The exploitation of the anonymity provided by the darknet in combination with other encrypted means of communication and payment systems, such as cryptocurrencies, poses a challenge for law enforcement authorities in terms of detection, attribution and disruption. Although the exact

Operation Onymous

On 6 November 2014, law enforcement and judicial agencies around the globe undertook a joint action against darknet markets running as hidden services on the Tor network. Sixteen European countries, alongside counterparts from the United States, brought down several marketplaces as part of a unified international action from Europol's operational coordination centre in The Hague.

The action aimed to stop the sale, distribution and promotion of illicit and harmful items, including weapons and drugs, which were being sold on darknet markets. Operation Onymous, coordinated by Europol's European Cybercrime Centre (EC3), the FBI, US Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) and Eurojust, resulted in 17 arrests of the vendors and administrators running these online marketplaces and more than 600 onion addresses being taken down. In addition, bitcoin worth approximately USD 1 million and EUR 180 000 in cash, drugs, gold and silver were seized. The darknet market Silk Road 2.0 was taken down by the FBI and the US ICE HSI.

Operation Onymous had a significant short-term impact on the darknet environment by removing key marketplaces and displacing trading activity to existing smaller marketplaces or newly emerging marketplaces. Following the closure of major marketplaces, such as a Silk Road 2.0, the prices of illicit goods on surviving marketplaces increased in the immediate aftermath of the takedown. However, longer term studies indicate that price levels quickly returned to their pre-takedown levels, as vendors and customers migrated to alternative darknet markets (Décary-Hétu and Giommoni, 2016).

Despite its success in closing down some of the most threatening darknet markets in terms of turnover and trading activity, Operation Onymous also demonstrated the resilience of the darknet market environment: as one major marketplace closes down,the next most credible markets absorb the displaced business of that market.

Operation Onymous's operational outcomes are impressive and also highlight the effectiveness of international law enforcement cooperation at tackling online criminality, including on the darknet. However, they also reveal that takedowns of darknet markets alone result in only short-term gains for law enforcement and that effective disruption strategies require a broader and more integrated approach to monitoring, intervention and investigation.

Source: Europol (2014).

scale of the criminality on the darknet cannot yet be fully determined, the darknet is clearly an established criminal environment hosting an increasing number of platforms, including darknet markets and other hidden services.

A new integrated approach — darknet investigations teams

Law enforcement authorities tackle the distribution of illicit commodities on darknet markets as part of international operations and investigations at national level. Many of these actions focus on disrupting the trade in illicit drugs online by removing or taking down platforms and identifying vendors for further investigations and prosecution. The majority of law enforcement investigations on the darknet focus on markets selling illicit drugs — or at least the vendors and buyers thereon.

However, so far most Member State law enforcement authorities have not created dedicated units to specifically tackle trade on darknet markets. The combination of a lack of coordination, the deconfliction of cases, and operations on national and international levels results in an overall knowledge gap in relation to darknet-related crime.

Responding to the need for a more coherent approach to fighting criminality on the darknet, Europol is promoting the concept of darknet investigations teams, which could be implemented by coordinating and executive agencies at national and international levels.

These teams, one of which is being established at Europol, will analyse intelligence on a daily basis and assist in the prioritisation and coordination of darknet-related cases. Darknet investigations teams will need to rely upon available secure communication channels and databases, as well as robust data protection and confidentiality arrangements.

Darknet investigations teams will coordinate the fight against the criminality on the darknet by gathering intelligence, providing operational support, engaging in the coordination of joint technical and investigative actions, and ensuring deconfliction between ongoing investigative efforts. These teams will also support the prioritisation of top targets and threats, driving technical development, centralising expertise, carrying out training and building capacities.

Darknet investigations teams will bring together key capabilities such as analytical support, specialised expertise to support case development, technical expertise and practical cooperation with law enforcement and non-law enforcement stakeholders. It is envisaged that this

capacity will also include the comprehensive involvement of digital forensic teams, access to experts on the different commodities traded on the darknet including illicit drugs, and outreach through networks and to the private sector.

A joint operational international taskforce

A second and complementary approach to fighting the distribution of illicit goods on darknet markets closely follows the highly successful concept of joint operational international taskforces. This mature and well-tested model of operational and concrete law enforcement cooperation has been successfully deployed to fight other types of cyber-dependent crime.

A joint operational international taskforce focusing on darknet markets will enhance the coordination and deconfliction of operations and investigations on an international level, and will further develop knowledge and expertise that can be shared across borders.

This taskforce would formulate and implement a European strategy against threats posed by the darknet including the trade in illicit drugs. The core elements of such a strategy are the creation of a deconfliction model, priority setting and the formulation of a joint operational action plan.

A joint operational international darknet taskforce will allow a coordinated approach to fighting the trade in drugs on the darknet and a more tactical and coordinated response to criminality on the darknet generally. Emulating existing successful ventures in other areas, this taskforce approach should be based on partnerships between law enforcement authorities, industry and academia.

3.6 Outlook

The trade in illicit drugs on the darknet has emerged as a common feature of European drugs markets and is a key challenge for law enforcement authorities seeking to disrupt the online trade in illicit goods and services. Law enforcement authorities expect the emergence of new darknet markets in response to successful takedowns and, without an effective approach to disrupt this distribution channel, an increase in darknet trading in illicit drugs over the coming years.

Darknet markets have the potential to partially displace existing traditional drug markets and make illicit drugs available to an even wider customer base than is already the case.

Unless effective action is taken, the profitability and reduced risk of detection and prosecution associated with the darknet trade in illicit drugs will increasingly attract organised groups seeking to exploit this environment.

Law enforcement authorities face a number of challenges in confronting this threat. Technical obstacles that form part of the design of darknet markets can be overcome, but they require concerted action and the availability of a range of expertise, which is so far lacking in many law enforcement authorities.

Current legislation is not fully equipped to provide law enforcement authorities with the tools needed to ensure that takedowns and other disruptive activities designed to deter darknet trading in illicit drugs and degrade trust in darknet market platforms have maximum effect. Legislative challenges such as the lack of online investigative powers and the absence of a harmonised framework for handling electronic evidence are impediments to the pursuit of effective investigations into darknet market trading. Existing legislation should be adapted to reflect the needs of practitioners and to equip law enforcement authorities and the judiciary with the tools they need to respond to criminality on the darknet.

However, an integrated approach reliant on international cooperation has the potential to more effectively make a sustainable impact on such criminal activity. Coordinated actions, such as those used to take down the AlphaBay and Hansa markets, and an improved common information position, resulting from shared law enforcement patrolling, have reduced the use of the darknet market environment as a platform for the trade in illicit drugs.

In the past, law enforcement responses to emerging threats have been reactive rather than proactive. Today, EU law enforcement authorities have mature capabilities to fight cybercrime, as well as a partnership network that provides an innovative and collaborative response to this challenge. However, arguably, the response to cybercrime as an emerging crime threat was only fully realised after cybercrime had already made a significant impact on the security and safety of citizens, businesses and public authorities.

There is now a window of opportunity to address and disrupt the growing threat from the online trade in drugs and other illicit commodities on the darknet before such markets fully emerge as prominent distribution mechanisms for illicit drugs in the EU.

Major international law enforcement operations shut down AlphaBay and Hansa

Two major law enforcement operations, led by the FBI, the US Drug Enforcement Agency (DEA) and the Dutch National Police, with the support of Europol, shut down the infrastructure of an underground criminal economy responsible for the trading of over 350 000 illicit commodities including drugs, firearms and cybercrime malware. The coordinated law enforcement action in Europe and the United States ranks as one of the most sophisticated takedown operations ever seen in the fight against online criminal activities.

AlphaBay was the largest criminal marketplace on the darknet, utilising a hidden service on the Tor network to effectively mask user identities and server locations. Prior to its takedown, AlphaBay reached over 200 000 users and 40 000 vendors. A conservative estimation of USD 1 billion has been transacted in this market since its creation in 2014. Transactions were paid in bitcoin and other cryptocurrencies. Hansa was the third largest criminal marketplace on the darknet, trading in similarly high volumes of illicit drugs and other commodities. Both markets were created to facilitate the expansion of a major underground criminal economy, which affected the lives of thousands of people around the world and was expressly designed to hinder the ability of law enforcement to bring offenders to justice.

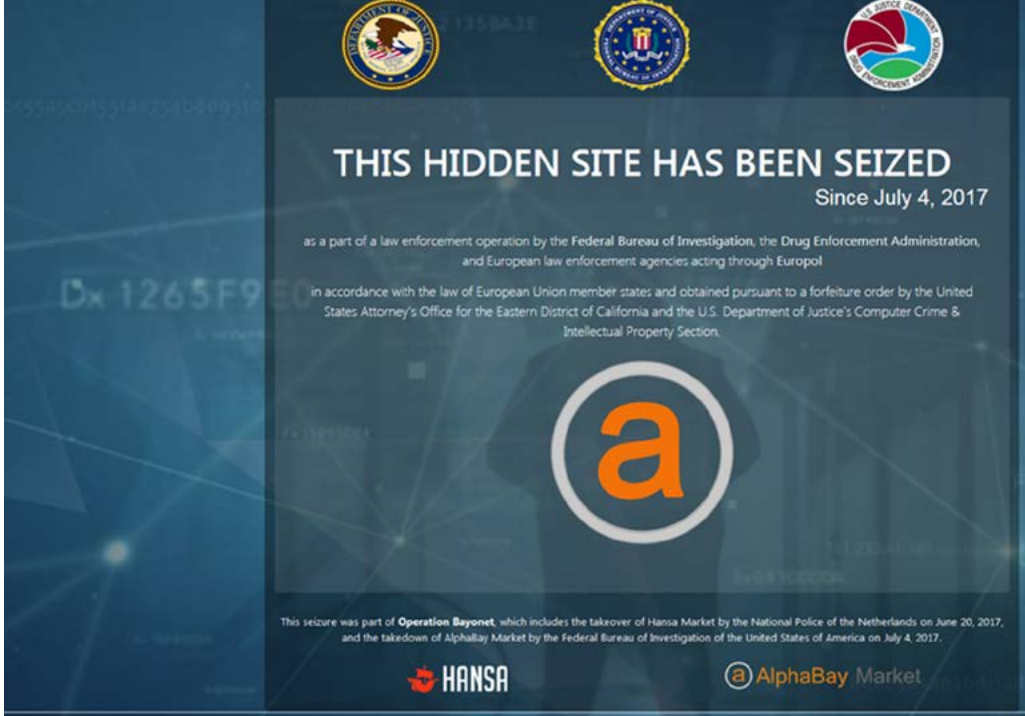
The investigations

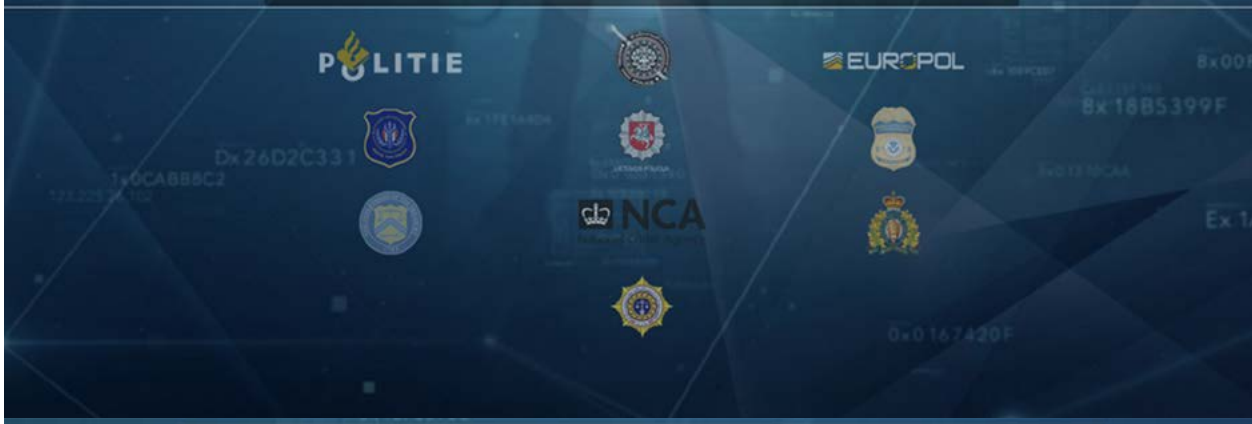
Europol has supported the investigation of criminal marketplaces on the darknet for a number of years. With the help of Bitdefender, an internet security company advising EC3, Europol provided Dutch authorities with an investigation lead into Hansa in 2016. Subsequent enquiries located the Hansa market infrastructure in the Netherlands, with follow-up investigations by the Dutch police leading to the arrest of its two administrators in Germany and the seizure of servers in the Netherlands, Germany and Lithuania. Europol and partner agencies in those countries supported the Dutch National Police with the take over of Hansa on 20 June 2017 under Dutch judicial authorisation, facilitating the covert monitoring of criminal activities on the platform until it was shut down on 20 July 2017. Since its take-down, the Dutch Police have collected valuable information on high-value targets and delivery addresses for a large number of orders. Some 10 000 foreign addresses of Hansa market buyers were passed on to Europol for analysis.

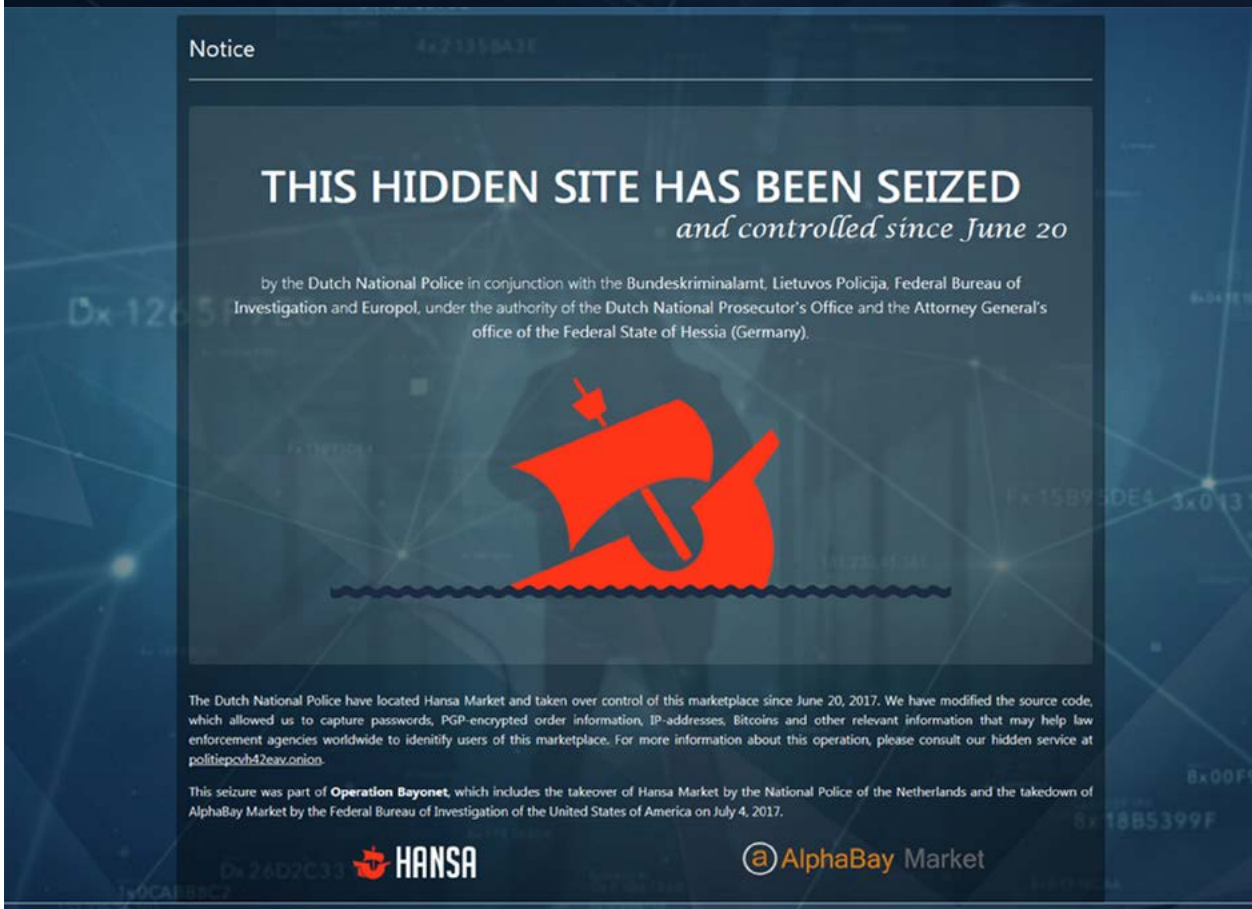
In the meantime, an FBI- and DEA-led operation, called Bayonet, was able to identify the creator and administrator of AlphaBay, a Canadian citizen living a luxurious life in Thailand. On 5 July 2017, the main suspect was arrested in Thailand and the site taken down. Millions of dollars' worth of cryptocurrencies were frozen and seized. Servers were also seized in Canada and the Netherlands.

Law enforcement strategy

In shutting down two of the three largest criminal marketplaces on the darknet, a major element of the infrastructure of the underground criminal economy has been taken offline. It has severely disrupted criminal enterprises around the world, led to the arrest of key figures involved in online criminal activity and yielded huge amounts of intelligence that will lead to further investigations. But what made this operation really special was the strategy developed by the FBI, the DEA, the Dutch police and Europol to magnify the disruptive impact of the joint action to take out AlphaBay and Hansa. This involved taking covert control of Hansa under Dutch judicial authority one month before Hansa's take-down, which allowed Dutch police to monitor the activity of users without their knowledge, and shutting down AlphaBay during the same period. This meant that the Dutch police could identify and disrupt the regular criminal activity on Hansa and also identify new users displaced from AlphaBay who were looking for a new trading platform. This is apparent from the eight-fold increase in the number of new members of Hansa recorded immediately following the shutdown of AlphaBay. As a law enforcement strategy, leveraging the combined operational and technical strengths of multiple agencies in the United States and Europe, it has been an extraordinary success and provides an illustration of the collective power that the global law enforcement community can bring to disrupting major criminal activities.


THIS HIDDEN SITE HAS BEEN SEIZED
Since July 4, 2017
as a part of a law enforcement operation by the Federal Bureau of Investigation, the Drug Enforcement Administration, and European law enforcement agencies acting through Europol
in accordance with the law of European Union member states and obtained pursuant to a forfeiture order by the United States Attorney's Office for the Eastern District of California and the U.S. Department of Justice's Computer Crime & Intellectual Property Section.
This seizure was part of Operation Bayonet, which includes the takeover of Hansa Market by the National Police of the Netherlands on June 20, 2017, and the takedown of Alphabay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.
HANSA
AlphaBay Market


POLITIE
EUROPOL
NCA


Notice
THIS HIDDEN SITE HAS BEEN SEIZED
and controlled since June 20
by the Dutch National Police in conjunction with the Bundeskriminalamt, Lietuvos Policija, Federal Bureau of Investigation and Europol, under the authority of the Dutch National Prosecutor's Office and the Attorney General's office of the Federal State of Hessia (Germany).
The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to idenitify users of this marketplace. For more information about this operation, please consult our hidden service at politiepcvh42eav.onion.
This seizure was part of Operation Bayonet, which includes the takeover of Hansa Market by the National Police of the Netherlands and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.
HANSA
AlphaBay Market


OPENBAAR MINISTERIE
POLITIE
EUROPOL
HESSEN
Bundeskriminalamt

4

CHAPTER 4

Conclusions and recommendations

This chapter provides key points and considerations stemming from the analysis presented in the previous chapters of this report.

4.1 Putting the darknet into context

Developments in information technology are transforming virtually all aspects of modern life, and this now includes the way that illicit goods are traded and the modus operandi used by OCGs. Online anonymous drug marketplaces can therefore be seen as part of a more general development for which addressing cybercrime and the use of information technology platforms for criminal purposes has become a more important policing priority across the EU. Innovation in criminal practices in this area represents a recognised challenge to established law enforcement practice and, if operational capacity is to keep pace, such innovation requires responses that are equally innovative and technologically informed. This report contributes to this objective by providing the conceptual framework necessary for understanding developments in this area, accompanied by an EU-focused analysis of darknet operations and a review of both the challenges to and the possible opportunities for law enforcement.

The analysis reported here supports the conclusion that drug transactions are a significant and important element of darknet market activities (although modest in value compared to the overall estimated retail drug trade in the EU), accounting for around two thirds of all offers made on the cryptomarkets reviewed. This report has also detailed how law enforcement interventions can disrupt darknet markets. That said, overall, this new online ecosystem appears relatively resilient to disruption, with new marketplaces becoming established and vendors and buyers quickly migrating to new platforms. This resilience, as well as the relatively large scale and diversity of drug market activity, means that current operational models that are considered appropriate for addressing some other forms of hidden online criminality, such as the marketing of illegal firearms or the facilitating of crimes against children, may not be directly transferable to, or sufficient in isolation for, tackling the online drug trade. Experience to date would suggest that, to increase the effectiveness of law enforcement activities, market disruption needs to form part of a broader, more integrated set of measures implemented as part of an overall strategy to address the drug market. This implies that the identification and targeting of major vendors, in addition to market administrators, is needed to prevent simply displacing activities from the targeted marketplaces to other marketplaces. It also implies that it is equally important to target the other key elements of the supply chain, such as production, precursor sourcing and bulk trafficking, without which the online market cannot function. To some extent this means recognising that established intelligence-led policing approaches must be brought together, but conducted in a technologically-informed, coordinated and collaborative manner, if law enforcement activities are to have a sustained impact on the online drug trade.

4.2 National coordination and international collaboration are key to an effective response

Despite the need to consider activities from a more holistic, strategic perspective, darknet markets do present particular challenges that require specific responses. Darknet drug sales have been driven by the exploitation of the opportunities presented by new technologies, and this

remains a dynamic and developing area. To be effective, responses must have sufficient technical capacities and specialist, dedicated resources, configured to keep pace with new threats as they emerge. In practical terms, this presents both human-resource and investment challenges for already hard-pressed criminal investigation and prosecution services. Experience to date provides a strong argument for pooling national resources to create, multiply and share expert capacity, for example by creating darknet investigations units. In this context, a clear recommendation from the findings of this report is the need for capacity building and increased investment to support specialist investigation capacities. Currently, Member States are often faced with significant skills gaps for conducting investigations on the darknet, and many authorities lack experts who have both a technical understanding of cybercrime investigation and practical expertise in combating drug-related crime. Therefore, there is a need to map existing expertise and competencies and to invest in appropriate training and capacity-building exercises.

Pooling resources is also important at the European level, to create synergies, maximise the available resources and facilitate knowledge transfer. In addition, such European-level pooling of resources is appropriate, and necessary, because darknet markets rarely exist solely within one national jurisdiction and their physical location is also often uncertain. This problem is likely to increase, as developments in decentralised software will allow marketplaces to exist without residing on any individual server. This is a potential 'dark cloud' on the horizon for investigations and prosecutions in what is already a challenging judicial landscape. There are many practical advantages, at the European and International levels, to creating joint operational taskforces and coordinated actions, such as cyberpatrolling. Such coordination is likely to improve operational efficiency and support a shared understanding of the role of the darknet drugs trade in the overall understanding of the changing operational models used by OCGs. Thus, in summary, given the significant resource and technical demands of investigations on the darknet, this represents an area in which the sharing of intelligence, as well as operational best practice, is clearly essential. Effective international cooperation is important for effective resource management in an area in which activities need to be coordinated across jurisdictions.

It therefore follows that addressing jurisdiction issues and location uncertainties associated with online activities is a task that is likely to be successfully accomplished only through increased coordination between legal, technical and law enforcement professions in different Member States. In this context, it is important to note that, in the EU, the Council conclusions (Council of the European Union, 2016a) on improving criminal justice in cyberspace have set out a framework for structuring future work and concrete action in three main areas: streamlining MLA proceedings, improving cooperation with service providers and launching a reflection process on possible connecting factors for enforcement jurisdiction in cyberspace. The Council took note in December 2016 of the progress made so far by the Commission on the implementation of these conclusions (Council of the European Union, 2016b).

4.3 Understanding the darknet from a European perspective

One of the purposes of this report was to document what is currently known about darknet drug market operations within an EU context. In any analysis of this topic, the considerable difficulties of collecting data on an area of activity that is, by definition, seeking to remain hidden needs to be borne in mind. Caution is therefore needed in respect of the interpretation of the findings. Nonetheless, it is possible to comment on the current situation from an EU perspective and this is helpful for anticipating threats in this area. The trade in illicit drugs on darknet markets is a dynamic area subject to rapid change as marketplaces appear and disappear, in part through the actions of law enforcement but also often through other forms of disruption, such as exit scams. While quantification is difficult, overall the importance of this area, in respect of illicit drug supply, appears to be increasing, even though darknet markets still account for only a relatively modest proportion of overall drug sales. That said, revenues from drug sales derived from online sales are considerable, and thus the potential profits to be made by those who can develop successful online 'businesses' are likely to be an incentive for both new groups entering the market and established OCGs involved in drug production, trafficking or supply. The online trade also now appears to affect most EU Member States to some extent, through either access to global marketplaces or nationally targeted platforms. The EU appears to be an important base for suppliers providing drugs online, particularly stimulants. In the analysis of marketplaces conducted for this report, just under half of all sellers appeared to be located in EU countries, with Germany, the United Kingdom and the Netherlands being most commonly identified. The availability of NPS on darknet marketplaces is currently relatively low, probably reflecting the significant role played by surface web sales in this sector. This may change, however, as these substances are increasingly being placed under control measures and other strategies are being developed to inhibit their open sale, such as engagement with producer countries.

4.4 Knowledge gaps

This report highlights that we now know far more about the operations of darknet markets than was previously the case, and this can be seen from the number of recent, high-profile interventions targeting specific marketplaces. Despite this progress, it is important to recognise that significant knowledge gaps still exist, especially with respect to the role of traditional OCGs in this area. Importantly, to understand the growth potential of darknet markets and how to better disrupt them, it is necessary to understand better the origin, production and wholesale practices relevant to their sourcing. Currently, most of the activity observed appears to be vendor–client level or at the middle-market or retail level. A better understanding of what makes darknet markets attractive or unattractive to potential vendors and customers is also important. The rationale underpinning the operation of darknet markets (providing anonymity for both buyers and sellers) would suggest that darknet drug markets are most likely to be used for mid-volume or low-volume individual sales. This is simply because the financial risks of loss are likely to grow with large-value single anonymous transactions. This means not that bulk supply is not being facilitated by new technologies, but rather that it is less likely to take place on an anonymous basis. In addition, major suppliers may try to reduce risk by using intermediaries to manage low-volume sales. Currently, very little is known about the source of drugs supplied on darknet markets or how the supply chain is organised; clearly, this is an area requiring further consideration. It is also possible that buyers and sellers will move 'off market' once a successful relationship has been established. This would mirror behaviour patterns seen in other, more established drug markets where, once trust has been established between a buyer and seller, a more exclusive relationship may be established.

It is also important to gain a better understanding of how the relative attractiveness or unattractiveness of darknet marketplaces, to both buyers and sellers, is influenced by the wider, existing drug market and the factors that affect it. This is also likely to be important for explaining the national and regional differences observed in the use of online marketplaces. For example, the rigorous control of parcels by customs appears to inhibit international sales, but may drive the development of national marketplaces as we have seen in Finland and has also been observed elsewhere. The accessibility of drugs through other sources is also likely to be an important factor in influencing the extent to which consumers will be attracted to darknet markets. For example, for drug users living in remote geographical locations or where policing or other factors mean that drug availability is poor there may be more incentive to explore online options for drug supply. Currently, the motives and rationale for using online drug markets remain poorly understood, and this is an area that merits further research. Some studies suggest that avoiding the possible violence associated with the street drug market and obtaining what are considered 'high-quality' products have been cited as reasons for using online marketplaces. These findings are interesting and suggest that, potentially, virtual markets are associated with fewer harms than traditional drug markets. However, further research is necessary in this area before any conclusions can be made. Not all physical drug markets are directly linked with violent crime, for example. Furthermore, understanding the relationship between purity and potency, chemical composition, possible contamination, and the relative availability of different types of substances and their relationship to harm at both the individual and population levels is a complex topic.

4.5 Engagement with industry

Engagement with key industries, such as the information technology, social media, payment services, and commercial product distribution and collection industries, is likely to be increasingly important for both identifying new threats and the development of effective responses. Public–private cooperation is also likely to play an important role: the success of law enforcement operations against cyber-enabled crime often depends on the cooperation of private technological companies. In this context, there is a need for standardised rules of engagement with private industries.

4.6 Threat assessment: understanding the potential for development of online drug markets

The dynamic nature of online markets, their ability to evolve to counter threats and exploit new opportunities, and the introduction or adoption of new technologies mean that enhanced monitoring capacity in this area is crucial to ensure that responses keep pace with developments. In this context, there are a number possible developments that may pose additional threats with respect to the technologically assisted distribution and sale of drugs. Developments in the darknet market are among these, but may evolve in tandem with the exploitation of other technological platforms in ways that may bring about additional regulatory and law enforcement challenges.

The potential threats already identified that may increase the challenges in responding to cyber-enabled drug supply include the development of decentralised software and new encryption technologies; new forms of parcel delivery and collection services; the greater integration of darknet markets with existing local drug markets; nationally based darknet markets; and the growing use of instant messaging applications. These are briefly discussed below, but require ongoing consideration.

There are barriers associated with accessing darknet markets in some key areas, but further technological developments or other innovative developments could potentially reduce these. Currently, law enforcement efforts often target the servers on which the marketplaces are hosted. Current software options allow servers to be partially hidden, but future software options may mean that a market need not be located on any individual server. Currently, some degree of technological sophistication is required to successfully access darknet drug markets. Although this is not an obstacle to many young people, it may be that developments in encryption and other software may increase the ease with which more technologically naive individuals may be able to access darknet marketplaces. The need to make traceable payments and the need to ship drugs to a fixed address are also potential barriers associated with using online platforms to buy drugs. Attention should therefore be given to assessing whether or not developments in remote payment technologies, including but not restricted to cryptocurrencies, and options for more convenient pick-up points for goods ordered online may increase the attractiveness of online platforms to potential drug buyers.

The need to keep pace with changes in this area is illustrated by the fact that evidence is beginning to emerge for the use of instant messaging and social media apps, together with global positioning system (GPS) technologies, for drug distribution in some European cities. These applications, if combined with existing darknet markets and distributed software to create a darkcloud-based drug distribution platform linked to numerous low-volume local supplies, have the potential to disrupt existing organised-crime drug-trafficking models and pose even greater challenges to existing regulatory and law enforcement approaches. Currently, this risk is largely speculative, but it does, however, underline the urgent need for the systematic monitoring and assessment of the anonymous online ecosystem, conducted in the context of understanding the operation of the overall drug market. This is necessary to support the comprehensive and strategic analysis required to inform future policy and operational responses in this area, and to reduce both the health threats and the security threats that developments in the technologically-assisted marketing and sale of drugs and other illicit commodities now present.

All markets, including illicit ones, function to facilitate the exchange of goods or services. Therefore, markets will prosper if they confer advantages to both buyers and sellers. Considerations for consumers can include the level of choice, ease of availability, convenience, perceived quality and price. For illicit drug markets, the level of risk is also an important factor, as vendors and consumers will be attracted to markets that are associated with relatively low risks of detection, experiencing market-related violence and 'rip offs'. Darknet markets provide a convenient sales channel for technologically-savvy drug users, and appear to have the potential to grow in the longer-term. It is possible that they will disrupt traditional drug markets in the same way as online markets have disrupted the traditional markets for some legitimate commodities, especially if they become more accessible to consumers (see Griffiths and Mounteney, 2016). However, changes in this area are currently difficult to predict. Importantly, they will not occur in isolation from broader developments in the illicit drug market as a whole, including the use of other technologies and platforms; the impact of law enforcement and regulatory efforts; and broader social and policy developments that may shape the supply of and demand for drugs more generally. For this reason, the systematic monitoring and assessment of the anonymous online ecosystem in the context of the overall drug market is necessary to support the comprehensive and strategic analysis needed to inform future policy and operational responses and to reduce the health and security threats that developments in this area now present.

Finally, changes are occurring rapidly in this area, and considerable challenges still exist with respect to our capacity to monitor these developments. This report summarises the current state of our understanding of the operation of darknet markets and how they can be successfully countered. It also highlights that greater investment and innovation are needed if we are to keep pace with the likely challenges in this area.

References

Aldridge, J. and Décary-Hétu, D. (2016), 'Hidden wholesale: the drug diffusing capacity of online drug cryptomarkets', *International Journal of Drug Policy* 35, pp. 7-15.

AlTawy, R., ElSheikhy, M., Youssefy, A. and Gong, G. (2017), 'Lelantos: a blockchain-based anonymous physical delivery system', *Cryptology ePrint Archive* (available at https://eprint.iacr.org/2017/465.pdf; accessed on 21 June 2017).

Anklagemyndigheden (Danish Prosecutor's Office) (2017), *Gennembrud: Nye beviser ophæver kriminelles anonymitet på mørkenettet*, http://www.anklagemyndigheden.dk/nyheder/Sider/gennembrud-nye-beviser-ophaever-kriminelles-anonymitet-paa-moerkenettet.aspx (accessed on 24 February 2017).

Bancroft, A. and Reid, P. (2015), 'Concepts of illicit drug quality among darknet market users: purity, embodied experience, craft and chemical knowledge', *International Journal of Drug Policy* 35, pp. 42-49.

Barratt, M. and Maddox. A. (2016), 'Active engagement with stigmatised communities through digital ethnography', *Qualitative Research* 35, pp. 24-31.

Barratt, M., Ferris, J. and Winstock, A. (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., Ferris, J. and Winstock, A. (2016a), 'Safer scoring? Cryptomarkets, social supply and drug market violence', *International Journal of Drug Policy* 35, pp. 24-31.

Barratt, M., Lenton, S., Maddox, A. and Allen, M. (2016b), '"What if you live on top of a bakery and you like cakes?" Drug use and harm trajectories before, during and after the emergence of Silk Road', *International Journal of Drug Policy* 35, pp. 50-57.

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E. and Virza, M. (2014), 'Zerocash: decentralized anonymous payments from bitcoin', in *2014 IEEE Symposium on Security and Privacy*, San Jose, CA, 18-21 May 2014, pp. 459-474.

Biryukov, A., Pustogarov, I. and Weinmann, R.-P. (2013), 'Trawling for Tor hidden services: detection, measurement, deanonymization', in *2013 IEEE Symposium on Security and Privacy*, San Francisco, CA, 19-22 May 2013, pp. 80-94.

Broséus, J., Rhumorbarbe, D., Morelato, M., Staehli, L. and Rossy, Q. (2017), 'A geographical analysis of trafficking on a popular darknet market', *Forensic Science International* 277, pp. 88-102.

Caudevilla, F., Ventura, M., Fornís, I., Barratt., Vidal, C., Lladanosa, C.G., Quintana, P., et al. (2016), 'Results of an international drug testing service for cryptomarket users', *International Journal of Drug Policy* 35, pp. 38-41.

Christin, N. (2013), 'Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace', in *Proceedings of the 22nd World Wide Web Conference (WWW'13)*, Rio de Janeiro, Brazil, 13-17 May 2013, pp. 213-224.

Coomber, R. (2015), 'A tale of two cities: understanding differences in levels of heroin/crack market-related violence — a two city comparison', *Criminal Justice Review* 40, pp. 7-31.

Council of the European Union (2016a), *Council conclusions on improving criminal justice in cyberspace of 9 June 2016*, doc. 10007/16 (www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf/; accessed on 19 July 2017).

Council of the European Union (2016b), Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace of 7 December 2016 (available at http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf; accessed on 13 October 2017).

DarkNet Stats (2017), https://dnstats.net/ (last accessed on 22 July 2017).

DarkWebNews (2017), https://darkwebnews.com/category/darknet-markets/ (last accessed on 22 July 2017).

DEA (United States Drug Enforcement Administration) (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*, http://www.dea.gov/divisions/nyc/2013/nyc102513.shtml (accessed on 21 June 2017).

Décary-Hétu, D. and Giommoni, L. (2016), 'Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous', *Crime, Law and Social Change* 67, pp. 55-75.

Décary-Hétu, D., Paquet-Clouston, M. and Aldridge, J. (2016), 'Going international? Risk-taking by cryptomarket drug vendors', *International Journal of Drug Policy* 35, pp. 69-76.

DeepDotWeb (2016), *Dutch National Prosecution Service and police launch Hidden Service in global darknet enforcement operation*, https://www.deepdotweb.com/2016/10/31/dutch-national-prosecution-service-police-launch-hidden-service-global-darknet-enforcement-operation/ (accessed on 21 July 2017).

DeepDotWeb (2017), https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/ (last accessed on 22 July 2017).

Dingledine, R., Mathewson, N. and Syverson, P. (2004), 'Tor: the second-generation onion router', in *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA, 9-13 August 2004.

Dolliver, D.S. and Kuhns, J.B. (2016), 'The presence of new psychoactive substances in a Tor network marketplace environment', *Journal of Psychoactive Drugs* 48, pp. 321-329.

Duxbury, S. and Haynie, D. (2017), 'The network structure of opioid distribution on a darknet cryptomarket', *Journal of Quantitative Criminology*, https://doi.org/10.1007/s10940-017-9359-4.

EMCDDA (2016a), *The internet and drug markets*, EMCDDA Insights 21, Publications Office of the European Union, Luxembourg.

EMCDDA (2016b), 'EMCDDA drug seizures indicator, guidelines for reporting data on drug seizures' (unpublished).

EMCDDA and Europol (2016), *EU Drug Markets Report: in-depth analysis 2016*, Publications Office of the European Union, Luxembourg (available at http://www.emcdda.europa.eu/system/files/publications/2373/TD0216072ENN.PDF).

Europol (2014), *Global action against dark markets on Tor network*, https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network (accessed on 7 August 2017).

Europol (2017a), *European Union Serious and Organised Crime Threat Assessment (SOCTA): Crime in the Age of Technology*, Europol, The Hague (available at https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017; accessed on 5 July 2017).

Europol (2017b), *Darknet dealer of drugs and arms arrested by Slovak authorities*, https://www.europol.europa.eu/newsroom/news/darknet-dealer-of-drugs-and-arms-arrested-slovak-authorities (accessed on 4 May 2017).

Europol (2017c), *Internet Organised Crime Threat Assessment (IOCTA) 2017*, Europol, The Hague (available at https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017).

Everett, C. (2009), 'Moving across to the dark side', *Network Security* 9, pp. 10-12.

Focus Online (2016), *Gemeinsame Presseerklärung der Staatsanwaltschaft Göttingen und der Polizeidirektion Göttingen: Illegaler weltweiter Rauschgifthandel im Internet*, http://www.focus.de/regional/goettingen/goettingen-polizei-gemeinsame-presseerklaerung-der-staatsanwaltschaft-goettingen-und-der-polizeidirektion-goettingen-illegaler-weltweiter-rauschgifthandel-im-internet_id_5635749.html (accessed on 15 June 2016).

Global Drug Survey (GDS) (2016), *The Global Drug Survey findings: key findings from the Global Drug Survey 2016 (data collected Nov 15-Jan 16)*, https://www.globaldrugsurvey.com/past-findings/the-global-drug-survey-2016-findings/ (accessed on 19 July 2017).

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/ (accessed on 27 July 2017).

Griffiths, P. and Mounteney, J. (2016), 'Disruptive potential of the internet to transform illicit drug markets and impact on future patterns of drug consumption', *Clinical Pharmacology & Theraputics* 101, pp. 176-178.

The Guardian (2017), *'Criminal mastermind' of $4bn bitcoin laundering scheme arrested*, https://www.theguardian.com/technology/2017/jul/27/russian-criminal-mastermind-4bn-bitcoin-laundering-scheme-arrested-mt-gox-exchange-alexander-vinnik (accessed on 27 July 2017).

Gwern Archives (2017), https://www.gwern.net/DNM-archives (accessed on 22 July 2017).

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E. and Hoorens, S. (2016), *Internet-facilitated drugs trade: an analysis of the size, scope and the role of the Netherlands*, RAND Europe, Cambridge.

Markoff, J. (2005), *What the dormouse said: how the sixties counterculture shaped the personal computer industry*, Penguin, London.

Markus, B. (2013), *Dogecoin*, http://dogecoin.com/ (accessed on 8 June 2017).

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

Monero (2017), *Monero: private digital currency*, https://getmonero.org/home (accessed on 18 September 2017).

Moore, D. and Rid, T. (2016), 'Cryptopolitik and the darknet', *Survival: Global Politics and Strategy* 58, pp. 7-38.

Murray, K. (2016), *The value of understanding organised crime business structures and processes: background paper commissioned by the EMCDDA for the 2016 EU Drug Markets Report*, European Monitoring Centre for Drugs and Drug Addiction, Lisbon.

Nakamoto, S. (2009), *Bitcoin: a peer-to-peer electronic cash system*, Bitcoin (available at https://bitcoin.org/bitcoin.pdf; accessed on 5 May 2017).

Nurmi, J., Kaskela, T., Perälä, J. and Oksanen, A. (2017), 'Seller's reputation and capacity on the illicit drug markets: 11-month study on the Finnish version of the Silk Road', *Drug and Alcohol Dependence* 178, pp. 201-207.

Owen, G. and Savage, N. (2016), 'Empirical analysis of Tor hidden services', *IET Information Security* 10, pp. 113-118.

RAND Europe (2016), *The role of the 'dark web' in the trade of illicit drugs*, RAND Europe, Cambridge (available at https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9900/RB9925/RAND_RB9925.pdf; accessed on 16 June 2017).

Reddit (2017), https://www.reddit.com/r/DarkNetMarkets/ (last accessed on 22 July 2017).

The Register (2014), *Silk Road dealer 'SuperTrips' faces 40 years for DVD drug imports: customs catch 22-year-old Dutch bloke on the brink of his big payday*, https://www.theregister.co.uk/2014/04/25/supertrips_silk_road_dealer_facing_40year_term_for_dvd_drug_imports/ (accessed on 16 June 2017).

Rhumorbarbe, D., Staehli, L., Broséus, J., Rossy, Q. and Esseiva, P. (2016), 'Buying drugs on a darknet market: a better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data', *Forensic Science International* 267, pp. 173-182.

Roxburgh, A., Van Buskirk, J., Burns, L., and Bruno, R. (2017), *Drugs and the internet*, Issue 8, May 2017, National Drug and Alcohol Research Centre, University of New South Wales, Sydney.

Schwartz, M. (2012), *Feds bust 'farmer's market' for online drugs*, https://www.darkreading.com/attacks-and-breaches/feds-bust-farmers-market-for-online-drugs/d/d-id/1103901 (accessed on 19 September 2017).

Simonite, T. (2013), *Mapping of the bitcoin economy could reveal users' identities*, https://www.technologyreview.com/s/518816/mapping-the-bitcoin-economy-could-reveal-users-identities/ (accessed on 16 June 2017).

Soska, K. and Christin, N. (2015), 'Measuring the longitudinal evolution of the online anonymous marketplace ecosystem', in *Proceedings of the 24th USENIX Security Symposium*, Washington, DC, 12-14 August 2015, pp. 33-48.

Der Standard (2017), *Operation 'Porto': 159 Dealer im Darknet ausgeforscht*, http://derstandard.at/2000058084813/Operation-Porto-159-Dealer-im-darknet-ausgeforscht (accessed on 22 May 2017).

Van Buskirk, J., Roxburgh, A., Bruno, R., Naicker, S., Lenton, S., Sutherland, R., Whittaker, E. et al. (2016), 'Characterising dark net marketplace purchasers in a sample of regular psychostimulant users', *International Journal of Drug Policy* 35, pp. 32-37.

Van Buskirk, J., Griffiths, P., Farrell, M. and Degenhart, L. (2017a), 'Trends in new psychoactive substances from surface and "dark" net monitoring', *Lancet Psychiatry* 4, pp. 16-18.

Van Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S. and Roxburgh, A. (2017b), 'The recovery of online drug markets following law enforcement and other disruptions', *Drug and Alcohol Dependence* 173, pp. 159-162.

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

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

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

Van Hout, M. and Hearne, E. (2017), 'New psychoactive substances (NPS) on cryptomarket fora: an exploratory study of characteristics of forum activity between NPS buyers and vendors', *International Journal of Drug Policy* 40, pp. 102-110.

Vejačka, M. (2014), 'Cryptocurrencies and their influencing factors', *Proceedings in GV : Global Virtual Conference* 2.

Wadsworth, E., Drummond, C., Kimergård, A. and Deluca, P. (2017), 'A market on both "sides" of the law: the use of the hidden web for the sale of new psychoactive substances', *Human Psychopharmacology: Clinical and Experimental* 32, doi:10.1002/hup.2596.

Wood, G. (2014), *Ethereum: a secure decentralised generalised transaction ledger,* http://gavwood.com/paper.pdf (accessed on 8 June 2017).

Yle Uutiset (2016), *Customs uncover huge online drug seller*, https://yle.fi/uutiset/osasto/news/customs_uncover_huge_online_drug_seller/9122125 (accessed on 8 July 2017).

Glossary

Bitcoin: One of the most popular cryptocurrencies in use today. As of 22 August 2017, 1 bitcoin = EUR 3 325.5 ([1]).

Bitcoin wallet: Also referred to as a 'digital wallet'. Establishing such a wallet is an important step in the process of obtaining bitcoins. Just as bitcoins are the digital equivalent of cash, a bitcoin wallet is analogous to a physical wallet but, instead of storing bitcoins literally, what is stored is relevant information such as the secure private key used to access bitcoin addresses and carry out transactions. The four main types of wallet are the desktop, mobile, web and hardware wallets.

Blockchain: Essentially a distributed database. Information within a blockchain is publicly shared across all participating users or machines. The bitcoin blockchain is a public record of all bitcoin transactions, which helps to verify transactions and prevent double spending.

Cryptocurrency: Virtual currency that employs cryptography for security purposes.

Cryptomarket: Anonymous digital platform that uses anonymising software (e.g. Tor) and cryptocurrencies (e.g. bitcoin) to facilitate the peer-to-peer trade of goods (including illicit drugs and new psychoactive substances) and services.

Customer feedback: When making a purchase, it is mandatory (or strongly encouraged, depending on the darknet market's policy) for customers to leave feedback. The feedback is posted underneath a listing and can be used as a proxy to estimate transactions.

Dark web or darknet: A network, built on top of the internet, that is purposefully hidden; it has been designed specifically for anonymity. Unlike the deep web, the darknet is accessible only with special tools and software — browsers and other protocol beyond direct links or credentials.

Darknet market: Also known as a 'cryptomarket' (see definition above).

Deep web: 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 amounts of deep-web data.

Doxing: 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. a 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.

Encryption: The process of converting data to an unrecognisable or 'encrypted' form. It is commonly used to protect sensitive information, including files, storage devices and data transfers, so that only authorised parties can view it.

Escrow: 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.

([1]) https://bitcoincharts.com/markets/currencies/

Exit scam: A scam in which a darknet market administrator or a vendor shuts down operations while stealing as much money as possible from users and/or buyers in the process.

Fiat currency: A 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 from the value of the material that the money is made of.

Finalise early: A circumvent escrow that ensures direct payment without funds first being held in escrow as a backup measure in terms of high levels of concern over exit scams or law enforcement seizure, reducing the risk that vendors and buyers lose the funds held in escrow.

Freenet: A peer-to-peer platform, using a decentralised distributed data store, to keep and deliver information. The distributed data store of Freenet is used by many third-party programmes and plug-ins to provide microblogging and media sharing, anonymous and decentralised tracking, blogging, etc.

Garlic routing: 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.

Grams: A service that offers a way to search for products across different darknet markets.

Hidden services: 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 (discussion) forum: A web-based environment where ideas and topics can be discussed freely among users. Forum members generally log in with a screen name or alias to post and comment on content. Forums differ from real-time internet messaging and chat rooms in that the topics and information are not intended to be discussed in real time, but instead are posted for all users to see over an extended period.

The Invisible Internet Project (I2P): 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.

Mining: A process for generating new bitcoins by creating new blockchains.

Multisignature ('multisig') escrow: This payment method is the most secure, as multiple keys are generated for the bitcoin transaction and the payment release process. The multisignature allows 2-of-2 or 2-of-3 escrow services, where a 2-of-3 service provides the most security for three keys: the market's key, the vendor's key and the buyer's key.

Onion routing: 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 the location of only the immediately preceding and following nodes.

OpenBazaar: 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 sites could be possible with this model, to further protect the identity and privacy of users involved in the marketplace.

Pretty Good Privacy (PGP): A data encryption and decryption computer program 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.

Protocol: The scheme in which internet content is retrieved and displayed to a browser. Tor and the darknet use a 'non-standard communication protocol', which refers to the complex set of onion proxy methods used to obscure the identity of the requestor and the content server. 'Protocol' can also refer to the currency used for the financial transaction, e.g. bitcoin.

Relay (or node): A device that switches internet traffic from one computer to another before it reaches its destination. The Tor network comprises around 7 000 relays.

Router: The hardware used to forward packets of information along a network, performing the traffic-directing functions of the internet.

Scrape (as a verb): In the context of web-content scraping, this term describes the process of harvesting large sets of data from websites and storing the content in a database on a local computer or server.

Scrape (as a noun): A copy of the entire content of a darknet market for further analysis.

Surface web (or clear web): The 'regular' internet, which can be found by the link-crawling techniques used by typical search engines such as Google, Bing and Yahoo. It is the unencrypted non-dark, non-Tor internet. In this report, the term 'surface web' is used.

Tor (The Onion Router): A free web browser designed for anonymous internet browsing and hosting; the most commonly used tool for accessing and browsing the darknet.

Tumbling: A method of mixing/scrambling or anonymising the source of bitcoin.

Annex 1

Local darknet drug markets survey

The EMCDDA and Europol are preparing a joint analysis on drugs and darknet markets to be published in the last quarter of 2017. Part of the analysis will focus on a subcategory of darknet marketplaces — those with limited geographical scope of operation, catering for national (and/or local) markets. To help us gauge the extent and key features of these markets, you are invited to complete this short survey.

The questions below consider **local (national) darknet websites** selling **drugs over Tor (The Onion Router), I2P (the Invisible Internet Project), OpenBazaar** or a similar hidden service network, using **cryptocurrencies** such as bitcoin, litecoin or dogecoin, hosting **multiple sellers** other than the site operators, and operating in **national/local languages** and within a fixed **national (or smaller) geographical scope**. For instance, the Tor-based Valhalla was founded in October 2013 as a Finnish-only marketplace for drugs and other illicit products. While global darknet markets that tend to operate in the English language are increasingly targeted by research, monitoring and international law enforcement activities, non-English-language markets, such as Valhalla, tend to be excluded from these activities and subsequent analyses, as they are more difficult to navigate. Data and information on these marketplaces are nevertheless important and need to be reflected in any up-to-date analyses of the online drug trade.

In collaboration with a relevant national partner involved in online investigations in relation to illicit drugs, please read carefully each question and provide your answers. Questions 1-3 relate to the numbers and key features of national/local darknet marketplaces. Questions 4-6 aim to elicit information about law enforcement strategies and data and information on recently completed or ongoing operations, and will be suitably anonymised.

Data protection note: As a matter of routine practice, the EMCDDA does not collect datasets that contain personal information, i.e. data that directly identify individuals or organisations or that can be used in combination to identify individuals or organisations. Such information is securely kept and not shared in public print or electronic publications.

Thank you for taking the time to answer these questions. If possible, please answer all questions.

Country . . . . . .

If not a member of the EMCDDA Reference Group on Drug Supply Issues, please indicate:

Name of organisation . . . . . .

Contact details, including name and email address/telephone number (optional) . . . . . .

1. To your best knowledge, are there any national and/or local darknet marketplaces according to the above definition?

   Yes |__| No |__|

2. If yes, how many unique national/local darknet marketplaces have come to the attention of law enforcement or monitoring/research agencies over the past year?

   |__|__|__|

3. Please name up to 10 significant darknet marketplaces, along with some key features (please insert additional lines as needed):

Name and URL	Geographical scope and language of operation	Type of software used (e.g. Tor, I2P)	Type of registration (e.g. open, invitation only)	Offers multisig ([1]) (yes/no)	Created (date)	Currently active (yes/no)	If not, reason for closure (e.g. law enforcement takedown, exit scam)	Estimated proportion of drug-related activity	Main drug types offered	Typical single-transaction volumes (in terms of money and quantities) for the top five drugs	Large transactions (> 1 000 g/ tablets/units) encountered (no/yes/ yes but very infrequently)	Turnover (annual or on a typical day, please specify)

4. Please briefly describe the law enforcement strategies applied in your country to tackle the trade of drugs on darknet markets.

   . . . . . .

   . . . . . .

5. Provide an example of recently completed or ongoing operations, including the process (e.g. investigation initiation, evidence gathering), the outcome (e.g. darknet market shutdown, arrest(s)), the key challenges and the lessons learnt (e.g. law enforcement skills required, key differences from real-world investigations).

   . . . . . .

   . . . . . .

6. Do you agree for (parts of) your case example (no5) to be used in the upcoming EMCDDA–Europol report? You will be consulted on the final draft.

   Yes |__| No |__|

([1]) Multisignature (often called **multisig**) is a form of technology used to add additional security and for cryptocurrency transactions. Multisignature addresses require another user or users to sign a transaction before it can be broadcast on the blockchain.

Annex 2

Acknowledgments and contributions

The EMCDDA and Europol are grateful to the following individuals for reviewing parts of this report: Nicolas Christin, Carnegie Mellon University; Anne Line Breteville-Jensen, Norwegian Institute of Public Health; Amanda Roxburgh, University of New South Wales; Brice De Ruyver, University of Ghent; and Lodewijk van Zwieten, Eurojust.

Country-specific contributions

Pascal Dierens and Emmanuel Smet, Federal Police, Belgium

Nelly Madjova, Ministry of the Interior, Directorate Analysis and Policies, Bulgaria

Adam Omasta, National Drug Headquarters, Criminal Investigation Services, Czech Republic

Jesper Boye, National Police, National Centre of Investigation, Denmark

Wolfgang Seiler, Bundeskriminalamt, Germany

Konstantina Stergiatou, Hellenic Police, Greece

Marc Geny, Office Central pour la répression du trafic illicite des stupéfiants (OCTRIS), France

Lidija Vugrinec, Office for Combating Drug Abuse (Reitox national focal point), Croatia

Angelo Longo, Central Directorate for Antidrug Services, Italy

Elena Demosthenous, Cyprus Antidrugs Council, Cyprus

Agnese Zile-Veisberga, Ministry of the Interior; State Police, Latvia

Renatas Vitkauskas, Criminal Police Bureau, Lithuania

Lina Jurgelaitienė, Drug, Tobacco and Alcohol Control Department, Lithuania

Sophie Hoffmann, Police Grand-Ducale, Service de Police Judiciaire, Luxembourg

Community and Media Relations Unit (CMRU), Malta Police Force, Malta

Ronald Meijer, Ministry of Security and Justice, Netherlands

Christian Mader, Federal Ministry of the Interior, Criminal Intelligence Service, Austria

Artur Malczewski, National Bureau for Drug Prevention, Ministry of Health (Reitox national focal point), Poland

Susana Silva, Unidade Nacional de Combate ao Tráfico de Estupefacientes, Seção Central de Informação Criminal (SCIC), Edifício Nova Sede da Polícia Judiciária, Portugal

Sergiu Popescu, Cocaine and Synthetic Drugs Trafficking Bureau, Romania

Stasa Savelj, National Police, Slovenia

Jari Yli-Pelkonen, National Bureau of Investigation, Finland

Stefan Kálmán, Swedish Police Authority, Department of National Operations, Sweden

Kai Arild Holm, National Criminal Investigation Service (Kripos), Norwegian Police Service, Norway

Eivind Tellefsen, National Criminal Investigation Service (Kripos), Norwegian Police Service, Norway

Nika Kobakhidze, Central Criminal Police Department, Ministry of Internal Affairs, Georgia

Artur Sivirean and Igor Stratulat, Ministry of Internal Affairs, National Investigation Inspectorate, Moldova

Professor Dr Jallal Toufiq, National Observatory on Drugs and Addictions, Morocco

Merita Vidishiqi, Ministry of Internal Affairs, Kosovo

Ana Nedic, Criminal Police Directorate, Ministry of Interior, Serbia

Sandra Sicovic, Intelligence Department, Customs Administration, Serbia

Yaron Stern, Cyber Unit, Investigation Branch, National Police, Israel

Abbreviations

alpha-PVP	alpha-pyrrolidinovalerophenone
CGN	carrier-grade NAT
DEA	Drug Enforcement Administration
DMT	N,N-dimethyltryptamine
DXM	dextromethorphan
EC3	European Cybercrime Centre
ECJ	European Court of Justice
EIO	European Investigation Order
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EU	European Union
ENP	European Neighbourhood Policy
Europol	European Union Agency for Law Enforcement Cooperation
FBI	Federal Bureau of Investigation
GBL	gamma-butyrolactone
GDS	Global Drug Survey
GHB	gamma-hydroxybutyric acid
GPS	global positioning system
HSI	Homeland Security Investigations
I2P	Invisible Internet Project
ICE	Immigration and Customs Enforcement
ICJ	International Court of Justice
IP	internet protocol
IPA	Instrument for Pre-Accession Assistance
ISP	internet service provider
LSD	lysergic acid diethylamide
MDA	3,4-methylenedioxyamphetamine
MDMA	3,4-methylenedioxy-N-methylamphetamine
MDPV	methylenedioxypyrovalerone
MLA	mutual legal assistance
MT-45	1-cyclohexyl-4-(1,2-diphenylethyl)piperazine
MXE	methoxetamine
NAT	network address translation
NPS	new psychoactive substances
OCG	organised crime group
PCP	phencyclidine
PGP	Pretty Good Privacy
Tor	The Onion Router
UNSCR	United Nations Security Council Resolution
2C-B	2,5-dimethoxy-4-bromophenethylamine
25I-NBOMe	4-iodo-2,5-dimethoxy-N-(2-methoxybenzyl)phenethylamine
4-AcO-DMT	4-acetoxy-dimethyltryptamine

HOW TO OBTAIN EU PUBLICATIONS

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct Information Centres. You can find the address of the centre nearest you at: http://europa.eu/contact

On the phone or by e-mail

Europe Direct is a service that answers your questions about the European Union. You can contact this service

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696 or
– by electronic mail via: http://europa.eu/contact

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU Publications

You can download or order free and priced EU publications from EU Bookshop at: http://publications.europa.eu/eubookshop. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact)

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

About this report

This joint EMCDDA–Europol publication on drugs and the darknet is based on a synthesis of information from a range of sources. The analysis takes a multidisciplinary approach to illuminate how darknet markets function and how they relate to criminal behaviour. The report brings together the latest findings from international research, fresh empirical data, and operational information and intelligence. The review is comprehensive but accessible and policy-oriented, intended to facilitate discussions at EU level on how to respond to the growth of darknet drug markets. This is accompanied by the identification of key priority areas that require attention and where activities are likely to have most impact.

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.

www.emcdda.europa.eu

About Europol

Europol is the European Union Agency for Law Enforcement Cooperation, whose mission is to support its Member States in preventing and combating all forms of serious international and organised crime and terrorism. Europol employs almost 1 000 staff at its headquarters in The Hague. They provide a unique and evolving set of operational products and services to EU law enforcemeant authorities for their everyday work, including efforts to tackle illicit drug trafficking, money laundering, cybercrime and terrorism. Europol's focus is to look further ahead for more opportunities to streamline cooperation and the fight against organised crime and terrorism, with the ultimate goal of achieving a safer Europe for the benefit of all EU citizens.

www.europol.europa.eu

Publications Office