Part of the Toolbox on

PARTY DRUGS AND CRIME

Darknet drug markets

Recommendations drawn from a barrier model

EUCPN
EUROPEAN CRIME PREVENTION NETWORK

EU 2020 HR

“

This paper formulates concrete recommendations for action by means of a barrier model that can be applied to the trade of party drugs through darknet drug markets.

”

ACKNOWLEDGEMENTS

The EUCPN Toolbox on Party Drugs and Crime has been developed by the EUCPN Secretariat in collaboration with the Croatian Presidency. We would like to thank the Croatian Presidency, in particular Mr Ivan Pakšić.

We are grateful to the experts who were willing to share their views and serve as a sounding board for the author:

- Annemie De Boye, ARIEC
- Dirk Minten, Belgian Federal Police

Citation
EUCPN (2021). Darknet drug markets: recommendations from the barrier model. Part of the EUCPN Toolbox on Party Drugs and Crime. Brussels: EUCPN

Author
Chadia Dehbi, Research officer, EUCPN Secretariat

Part of the project 'EUCPN Secretariat', March 2021, Brussels

With the financial support of the European Union's Internal Security Fund - Police

All the papers which make up the EUCPN toolbox on party drugs and crime are available for download at

https://eucpn.org/toolbox-partydrugsandcrime.

CONTENTS

PREFACE

This paper forms part of the EUCPN Toolbox published on the occasion of the Croatian Presidency of the EUCPN, which has opted to zoom in on the prevention of party drugs.

The main goal of this paper is to formulate concrete recommendations for action by means of a barrier model that can be applied to the trade of party drugs through darknet drug markets. Additionally, we want to place the spotlight on the administrative approach and more specifically on the method of creating a barrier model.

The introductory chapter reiterates the main insights from a separately published background paper *'Darknet drug markets: the criminal business process explained.'*, which aims to clarify the topic of (online) drug markets and party drugs by revisiting drug market stereotypes, by viewing illegal drug markets from an economic perspective and by zooming in on darknet drug markets. Furthermore, the administrative approach is explained and linked to the creation of a barrier model for the trade in party drugs by means of darknet drug markets. In the next chapter, we simultaneously explain what a barrier model is and create one for the trade in party drugs by means of darknet drug markets. The final chapter formulates concrete recommendations for action so that national and local governments and police organisations can develop their full potential in the prevention of and fight against the trade in party drugs by means of darknet drug markets.

This paper is one of four parts of the toolbox in the topic of party drugs and crime.

- Party drugs and crime: understanding the phenomenon
- Party drugs and crime: effective approaches
- Darknet drug markets: the criminal business process explained
- Darknet drug markets: recommendations drawn from a barrier model

DARKNET DRUG MARKETS

AN EXECUTIVE SUMMARY

The reality of drug markets can be viewed as a continuum that is more varied than commonly assumed. It is therefore fruitful to revisit some drug market stereotypes. Strongly hierarchical drug markets are rather atypical for drug markets. Drug markets more often take the form of horizontal structures that consist of a wide range of individuals who move freely across the supply chain. Additionally, with regard to the persons involved, it is important to remember that offenders are not outsiders. They are part of society and transcend all demographics and their role in the drug trade is often easily fitted in their everyday (conventional) lives.

The criminal business process behind darknet drug markets roughly consists of the four consecutive steps of (1) setting up a marketplace, (2) running a marketplace, (3) selling drugs and (4) shipping drugs. Several players, from a developer and a managing administrator to a moderator who helps with maintenance and supporting customers, are involved in setting up and running a marketplace.

In so far as the actual selling of drugs is concerned, the main motives of vendors to sell drugs on darknet markets are the stability of the business channel and the lack of physical contact. The online vendor is less dependent on social network connections than an offline trader, however a good reputation remains important, because the buyer not only functions as a customer, but also provides feedback on the purchases made. This feedback, which often forms part of discussions on forums, is one of the elements that influence the purchase decision of a buyer. Additionally, research stresses the importance of trust between vendors and buyers on darknet drug markets.

In a final step, the drugs need to be shipped. This involves a transition from online to offline activities, as the actual purchased goods need to change hands from vendor to buyer. Before transportation, the suspicious physical appearance of drugs needs to be concealed. To do this, drug traders can rely on several suppliers of legal goods and services, such as a company that supplies envelopes for stealth packaging. Online sales and transportation via postal and parcel services are inseparably linked. Facilitating the illegal trade, public or private postal and parcel services and legal and illegal courier services carry out the actual delivery.

After having described the overall picture and criminal business process of darknet drug markets, the next step is to identify promising possibilities for preventative actions. A barrier model is a method of mapping a complex form of crime in a transparent manner. It identifies the steps criminals have to take to be able to commit a crime, as well as which parties and opportunities are involved. By creating a barrier model, it is possible to determine what barriers can be set up by public and private partners to effectively disrupt the work of the criminals.

1. SETTING UP MARKETPLACE	2. RUNNING MARKETPLACE	
Facilitators		
Developers Administrator Internet Service Providers	Administrators Moderator Web designer	
Opportunities		
TOR encryption software Decentralised markets	TOR encryption software Virtual offender convergence setting	
Signals		
Lifestyle mismatching income	Lifestyle mismatching income	
Partners		
Internet Service Providers	Internet Service Providers White hats	
Barriers		
Scientific research		

	3. SELLING DRUGS	4. SHIPPING DRUGS
	Moderator Vendors Buyers Cryptocurrency exchangers	Supplier of stealth packaging (Il)legal courier services Public postal services Private parcel delivery services Food delivery services Encrypted communication services
	TOR encryption software Freely accessible Culture of trust Community Prohibition of drugs	Sophisticated concealment Increase of parcel shipment
	Lifestyle mismatching income	Frequent ordering of consignments Modified delivery vans Increased use of bitcoin ATMs
	(Cryptocurrency exchangers)	Supplier of stealth packaging Legal courier services Public postal services Private parcel delivery services Food delivery services Customs
	Proactive online investigations Continuous observations	Educate law enforcement, customs and postal services Extend competences of postal services Inform and call-to-action of - courier and food delivery companies - social media and encrypted communication companies - stealth packaging companies - internet service providers Implement licensing regulations

After applying this method to darknet drug markets, there are two domains of action and two target groups that appear to be promising in the prevention of and fight against the illegal trade in synthetic drugs through darknet drug markets.

1. To enhance the capacities of government authorities in order to increase chances of detection

- Create a legal framework that allows law enforcement to proactively investigate online
- Build an up-to-date body of knowledge based on continuous observations on darknet drug markets
- Educate law enforcement, customs and postal services about the latest developments
- Extend the competences of postal services to intercept and inspect suspicious items
- Encourage further scientific research into drug sources, links to offline markets, illicit money flows and the roles of organised crime in relation to darknet drug markets

2. To engage suppliers of legal goods and services in setting up barriers that impede the criminal business process

- Inform and call courier and food delivery companies to action concerning their role in delivering drug packages to their final destination
- Inform and call social media and encrypted communication companies to action concerning their role in facilitating communication and the coordination of the shipment of drug packages to their final destination
- Inform and call stealth packaging companies to action concerning their role in concealing drug packages so they can pass through customs and other checkpoints
- Inform and call internet service providers to action concerning their role in hosting darknet drug markets
- Implement licensing regulations applicable to suppliers of legal goods and services who consciously contribute to the criminal process

01 INTRODUCTION

Drug markets are increasingly becoming digitally enabled. While the proportion remains relatively modest, it is the fast pace at which this is increasing that is worrying. An overall challenge in understanding and tackling cybercrime is that it is often described as a single activity, while in reality it is a series of crimes aimed at a certain goal. Especially in the context of darknet drug markets, where crimes are committed both online and offline, the challenge is even greater.

The reality of drug markets can be viewed as a continuum that is more varied than commonly assumed. Some drug market stereotypes need to be revisited. A strongly hierarchical drug market is rather atypical for drug markets. They are rather horizontal structures consisting of a wide range of individuals who move freely across the supply chain. Furthermore, drug offenders and users are not outsiders, they are part of society and transcend all demographics. Additionally, the labour needed in the logistical process is easily incorporated within the daily (conventional) lives of drug offenders.

The criminal business process behind dark net drug markets roughly consists of the four consecutive steps of (1) setting up a marketplace, (2) running a marketplace, (3) selling drugs and (4) shipping drugs.

Setting up a marketplace requires a developer, who builds the website and an administrator, who functions as treasurer and manager. Also the internet service provider facilitates the setting up of a marketplace by offering internet access and hosting domain names. To run a marketplace, the administrator is assisted by a moderator, who maintains the website and supports customers.

The main motives for vendors to sell drugs on darknet markets include the stability of the business channel and the lack of physical contact. The online vendor is less dependent on social connections than an offline trader. However a good reputation remains equally important. As the buyer not only functions as a customer, but also provides feedback on purchases made. This feedback, which often forms part of discussions on forums, is one of the elements that influence the purchase decision of a buyer. Additionally, research has underlined the importance of trust between vendors and buyers on darknet drug markets.

Once they have come to an agreement and the payment is set up through one of the various online (crypto)currencies, the drugs need to be shipped. In this step, there is a transition from online to offline activities, as the actual purchased goods need to change hands from vendor to buyer. Before transportation, the suspicious physical appearance of drugs needs to be concealed. To do this, drug traders can rely on several suppliers of legal goods and services, such as a company that supplies envelopes for stealth packaging. Online sales and transportation via postal and parcel services are inseparably linked. Facilitating the illegal trade, public or private postal and parcel services and legal and illegal courier services carry out the actual delivery.[1]

Impact of COVID-19 on drug markets

Europol reports that darknet drug markets are gaining relevance as a retail sales channel due to COVID-19. It is deemed likely that newly adopted behaviour such as making use of home deliveries, which is increasing for individual transactions, will continue to take place in the longer term. Even though the way the trend is presenting itself varies from country to country, buying drugs is an activity increasingly being carried out with the support of internet services. This could take place either on the surface web, via mobile apps or web shops, or on the darknet market.[2]

02 BARRIER MODEL FOR DARKNET DRUG MARKETS

"An administrative approach to serious and organised crime is a complementary way to prevent and tackle the misuse of the legal infrastructure through multi-agency cooperation by sharing information and taking actions in order to set up barriers."[3]

The barrier model method fits within the larger framework of the administrative approach[4]. The European Network on the Administrative Approach tackling serious and organised crime (ENAA) describes five pillars for a successful implementation in its *EU Handbook on the Administrative Approach in the European Union.* The first pillar is the prevention and tackling of misuse of the legal infrastructure by serious and organised crime. The goal is to prevent criminals from acquiring a legal income or misusing businesses to facilitate crime and directing their criminal proceeds to this purpose.

Second, the administrative approach needs to be seen as complementary to the traditional criminal justice measures. The combination of both approaches is more powerful, moreover administrative measures on their own will not be sufficient to tackle organised crime groups (OCGs).

Consequently, the third pillar stresses the importance of multi-agency cooperation. The administrative approach is often referred to as 'working apart together'. Each government agency has its own field of responsibility and corresponding competences. Joining forces creates a synergy. A typical cooperation might be between the police, the public prosecutor's office and the tax authorities.

The fourth pillar promotes another form of cooperation between agencies, namely the sharing of information. Government agencies might need access to data that falls outside of their competences to confirm suspected links between OCGs.

Finally, the fifth pillar consists of taking actions to set up barriers. Although it might not be straight forward, public administrations, especially at the local level, have the power within their competences to take actions that will frustrate and hinder OCGs. The idea of the administrative approach is to equip local administrations with useful tools to do so.[5]

2.1. Building a barrier model

Joeri Vig and Lienke Hutten from the Dutch Centre for Crime Prevention and Safety (CCV) explain the barrier model in the EU Handbook on the Administrative Approach as follows:

> The barrier model is deployed to map a complex form of crime in a transparent manner. It identifies the steps criminals have to take to be able to commit a crime. The model also highlights which parties and opportunities make the crime possible. This makes it possible to determine what barriers can be set up by public and private partners to effectively disrupt the work of the criminals. The barrier model can also be applied when mapping out potential abuses in a business process.

> The barrier model is a method of determining which barriers the partner organisations can set up to combat criminal activities. For every component of production, transport, sales, etc., it is reviewed which partner is in the best position to prevent criminal organisations or individuals from abusing legal structures. The different barriers imply multiple signals that cause government agencies, companies, persons to come into contact with a certain crime phenomenon and notify the authorities.

> The barrier model provides focus in forming an impression of or preventing criminal activities, including within the investigation procedure and helps to look at criminal practices from an administrative and financial perspective. By applying the barrier model, many government departments have realised that they have a role to play in combating serious and organised crime.[6]

The building blocks of a barrier model are:

- a. Facilitators
- b. Opportunities
- c. Signals
- d. Partners
- e. Barriers

A. Facilitators

Facilitators are those persons or parties that support criminals in their efforts. Simply by offering their products and services, they are knowingly or unknowingly facilitating the crime process. Real estate, transport and logistics, financial services and ICT are, generally speaking, the main facilitating sectors.

Within the context of the trade in party drugs on darknet drug markets, the facilitators involved in setting up and running a marketplace and selling drugs are less tangible than those involved in shipping drugs. Although not unachievable, a profound knowledge of darknet cyberspace in all its aspects is needed to identify or at least hinder and frustrate these actors. The developer not only facilitates, but also creates a darknet drug market that serves as a platform for all other players. The administrator aids the online drug trade by managing the sales platform in all its aspects, ranging from deciding who is allowed to sell what to finalising the illegal transactions. The moderator smooths the operations by answering requests to enhance customers' convenience. The web designer creates a website for the vendor on which he can offer his illegal goods. The cryptocurrency exchangers exchange money for cryptocurrencies and play a crucial role in the transactions. All of these actors operate under the cloak of anonymity and never have to meet face-to-face or even share remotely the same location.

More tangible and more diverse are those who willingly or unwillingly facilitate the shipping of drugs. Generally speaking, these are suppliers of legal goods and services. The sole fact that they are essential levers in the shipping process of illegal drugs does not criminalise them, because their goods and services serve legitimate purposes. Companies that specialise in stealth packaging decrease the risk of detection when passing through customs or other check points. Public postal services, private parcel and food delivery services act as facilitators by physically transporting the package from vendor to buyer. Encrypted communication services facilitate the shipping of drugs by providing shielded communication between vendor and buyer, which makes it possible to reach detailed agreements with regard to the final destination of the package.[7]

In sum, all of the above mentioned actors are key players in the criminal business process. Without these facilitators, the online trade would not be possible. Consequently, these are interesting focus points for actions.

B. Opportunities

Crime does not happen in a vacuum. The circumstances or opportunities need to be right. Overall, opportunities for committing crime can be divided up into five categories: infrastructure (a catering business to meet each other); machines and raw materials (computer); financial, legal and administrative services (money exchange); shielding, security and promotion (CCTV) and opportunities unwillingly created by the government (by prohibiting something that is great demand). Additionally, opportunities can exist in the form of resources such as money or weapons.

When applying the concept of opportunities to darknet drug markets, it becomes clear that the existence of the TOR anonymisation software is undeniably the most important opportunity for darknet drug markets. First, as a shield, it allows for one of the greatest strengths of darknet drug markets: anonymity. Second, as an infrastructure, it provides a virtual convergence setting for offenders, where offenders can meet new potential partners or discuss ongoing business. Furthermore, the TOR anonymisation software allows non-traceable communication between vendor and buyers and buyers among themselves. Additionally, feedback and discussion forums are very well-developed and form a continuous growing body of knowledge about how to avoid detection. It provides almost instant responses to developments in law enforcement.[8] In this

online community, users have a high degree of trust towards each other, which further enhances good interactions. An additional opportunity is that the darknet drug market is freely accessible by everyone with a computer and an internet connection, which therefore has a positive effect on the potential client base. A financial opportunity can be found in the cryptocurrency exchangers that provide safe transactions and a conversion of the profits achieved.

Also other developments have the effect of providing this criminal business process with several opportunities. The increase in global trade, of which legitimate online purchases form a major part, has led to a dramatic increase of the volume of packages that pass through postal services. As a consequence, services in charge of carrying out checks are forced to narrow their focus on areas that engender a high degree of suspicion.[9] On top of this, concealment methods are becoming increasingly sophisticated.[10] Finally, the prohibition of drugs also forms a crucial opportunity for illegal drug trade and related crime.

Opportunities for the criminal business process can also be interpreted as elements that are needed as part of the operation. In other words, from a prevention or law enforcement perspective, some of the aforementioned opportunities are promising focal points for actions. If criminals lose their easy access to certain suppliers of legal goods and services, the online drug trade operations will be hindered.

C. Signals

Even though crime often takes invisible forms, at every stage in the criminal business process there may be indicators or signals that activities are taking place. These signals can be financial (e.g. large cash payments), social (e.g. a lifestyle that does not match the person's income), logistical (e.g. 'track and trace' turned off during transport), physical (e.g. catering business without customers) or administrative (e.g. ownership of several businesses without employees).

When it comes to darknet drugs markets, a major part of activities takes place behind closed doors on the internet. Consequently, signals are less likely to be picked up than in case of other drug crimes. Nevertheless, administrators, moderators and especially vendors obtain profits which cannot be explained by legal activities. This might result in a lifestyle that does not match their income. Another money-related signal might be an increased use of bitcoin-ATMs in public

spaces. Other signals might be picked up at parcel delivery services in the form of frequent ordering of consignments or hiding places in modified delivery vans.[11]

D. Partners

There are several sorts of partners that can add to a joint approach to organised crime. These partners may originate from the public or private sector, or from within society. Each sector has its own merits. It is important to take into account from which sector the partners originate, because this may have a significant impact on the extent to which information can be exchanged, which is crucial within the administrative approach.

Additionally, depending on the extent to which certain actors are unknowingly facilitating the drug trade, facilitators have the potential of being useful partners. Evidently, those who are running, selling and buying on darknet drug markets will not cooperate in their own demise. Suppliers of stealth packaging are important facilitators and potential partners. However, it seems unlikely that the sector is unaware of the illicit use of their legal goods and would consequently be willing to contribute to a joint approach against illegal trade.

Nevertheless, a collaboration between public and private parties is an added value.[12] Evidently, internet service providers and encrypted communication services are important facilitators of darknet drug markets, which makes them potentially promising partners for the purpose of unravelling location, identity or communication. A second group of promising partners consists of customs, postal and courier services. These sectors are on the frontline of overseeing and executing the shipping of (illegal) packages.

Partners can be identified on a country level. Major EU based suppliers such as Germany, the Netherlands and the UK are important players in online drug markets. Overall, 24 EU countries account for approximately 46% of the global drug revenues.[13]

E. Barriers

Last but not least, a barrier model sets out to create obstacles or barriers for criminals. The barrier model is a collection of instruments that the crime fighting partners share. We can distinguish between several kinds of barrier: economic, legal, information and criminal law barriers. Likewise, one can distinguish between repressive barriers and preventive barriers.

Types of barriers			
Economic barriers	**Legal barriers**	**Information barriers**	**Criminal law barriers**
- Fines - Tax measures - Confiscation - Blocking bank accounts	- Administrative enforcement - Supervision - Licensing system - Prohibition of production	- Awareness raising campaigns - Enhancing information exchange - (Negative) image creation	- Confiscation of illegally obtained assets - Confiscation of property - Ban on practising a profession

The types of barriers can be set up within the context of darknet drug markets will be discussed in the next and final chapter of this paper.

Further reading on the administrative approach and the barrier model:
Spapens, et al., 2015
Centre for Crime Prevention and Safety (CCV), 2011

1. SETTING UP MARKETPLACE	2. RUNNING MARKETPLACE	
Facilitators		
Developers Administrator Internet Service Providers	Administrators Moderator Web designer	
Opportunities		
TOR encryption software Decentralised markets	TOR encryption software Virtual offender convergence setting	
Signals		
Lifestyle mismatching income	Lifestyle mismatching income	
Partners		
Internet Service Providers	Internet Service Providers White hats	
Barriers		
Scientific research		

	3. SELLING DRUGS	4. SHIPPING DRUGS
	Moderator Vendors Buyers Cryptocurrency exchangers	Supplier of stealth packaging (Il)legal courier services Public postal services Private parcel delivery services Food delivery services Encrypted communication services
	TOR encryption software Freely accessible Culture of trust Community Prohibition of drugs	Sophisticated concealment Increase of parcel shipment
	Lifestyle mismatching income	Frequent ordering of consignments Modified delivery vans Increased use of bitcoin ATMs
	(Cryptocurrency exchangers)	Supplier of stealth packaging Legal courier services Public postal services Private parcel delivery services Food delivery services Customs
	Proactive online investigations Continuous observations	Educate law enforcement, customs and postal services Extend competences of postal services Inform and call-to-action of - courier and food delivery companies - social media and encrypted communication companies - stealth packaging companies - internet service providers Implement licensing regulations

2.2. Using a barrier model

A barrier model should be perceived as a first step, as a means to an end. The creation of a barrier model in itself will not aid the prevention of or fight against (organised) crime. Once created, the barrier model can serve as the foundation for drawing up a larger plan of action.

It is crucial to set concrete objectives, with corresponding measures and activities, so that they are measurable for evaluation purposes. Once the objectives are defined, it is up to the group of partners to list measures. Evidently, proposed measures should take into account the commitment and competences of the partners involved. In most cases, strategic choices will have to be made, as not all measures can be executed simultaneously. These decisions should be made in close dialogue with all partners, as it is preferable for everyone to be on the same page.[14] One partner should function as the coordinator who oversees the plan and reminds the other partners of their commitment. Last, but not least, the plan of action should leave scope, in terms of time and money, for evaluation. Without a proper process and outcome evaluation, there is no way of knowing whether the plan was executed as intended or whether it has yielded the expected results.[15]

The criminal business process of party drugs, or synthetic drugs in general, is not chronologically structured. The acquisition of material, production, distribution and sales do not happen sequentially. Patterns are erratic. Due to the fact that these criminals think on their feet and adapt their way of working, law enforcement might struggle to get a grip. In the same way that law enforcement, as a well organised and structured organisation, might have trouble getting a grip on this in some cases, a barrier model might suffer the same problem. It approaches criminal operations as if they were rational well-structured business processes, while it appears that the synthetic drug world can be very unpredictable and is largely based on improvisation.[16] Consequently, barrier models, just as other instruments used to fight crime, need to be updated regularly in order to stay useful.[17] Especially within the context of synthetic drugs; a world that is notorious for its innovation and for the speed with which it adapts to obstacles that are erected.

03 RECOMMENDATIONS

As explained before, the barrier model is a method of mapping a complex form of crime in a transparent manner. Where the paper *'Darknet drug markets: the criminal business process explained.'* describes in detail how darknet drug markets operate, this paper focussed on how this translates in the form of barrier model specific terminology: facilitators, opportunities, signals and partners. In this last chapter, recommendations will be made with regard to barriers that may prevent and hinder the trade in synthetic drugs carried out by means of darknet drug markets.

The criminal business process of darknet drug markets can be divided into four stages. The setting up and running of a darknet drug market, together with the selling of the drugs themselves are online components that are mainly situated within the sphere of cybercrime. The final stage, which involves shipping the drugs, moves the criminal business process offline.

3.1. Increase chance of detection in cyberspace

Taking down the TOR network itself is not only nigh on impossible[18], and is not desirable. Because although it forms the core of darknet (drug) markets, it simultaneously provides a safe channel for the oppressed to communicate and has many other legitimate purposes. The same argument goes for the cryptocurrency system.[19] What is more, a shutdown of a darknet drug market is inconvenient for most involved, however it appears to have little effect in the medium term.[20] Trust in darknet drug markets does take a hit after a shutdown by law enforcement and

as we know that trust is an important factor in the operations, this is not entirely negligible. Nevertheless, administrators learn from law enforcement interventions. Consequently, new vendors, in order to be allowed access to the more recent established darknet drug markets, need to be introduced by an already known individual.[21]

Deterrence is the most important preventive function of the criminal justice system, of which law enforcement forms part. However, in order for deterrence to work, it needs to meet three conditions related to punishment: severe enough, immediate and certain. Research shows that the latter condition is the most promising for crime prevention. Furthermore, to be sure of being punished, one must be sure of being apprehended.[22] Consequently, it is important to improve the chance of detection in cyberspace. However, the major benefit of darknet drug markets is the anonymity provided by encryption technology.[23] In order to increase the chance of detection, additional capacity should be built in two domains.

First, in terms of creating a legal framework that allows to match law enforcement competences to the needs that are typical for darknet (drug) market investigations. Currently, online investigations are underemployed. Law enforcement is hindered from doing so as a result of legal challenges. For example, in many countries, officers, do not have the legal means to operate as online undercover officers, which limits their operative capacities. Proactive online investigations should form part of routine practices.[24]

Second, it is recommended to keep a finger on the pulse in order to obtain a continuously up-to-date body of knowledge about how darknet drug markets operate. Once collected, this information should then also be disseminated promptly, not only to law enforcement, but also to other partners that could benefit from it and could contribute to the prevention and hindering of darknet drug markets.

Overall, darknet drug markets are extremely agile in adapting their modus operandi and law enforcement and other partners need to shift at the same speed it they want to keep up with the arms race.

3.2. Potential for action in shipping

The digitalisation of drug markets is a challenge for players that are active in the prevention and law enforcement sectors. It will also lead to a remapping of the drug landscape and will result in changes to or a decrease in the roles of some facilitators such as drug traffickers, street dealers and other intermediaries. This is because in a model such as darknet drug markets, the producer more often deals directly with the consumer. Nevertheless, in this changing landscape, the suppliers of legal goods and services will play an increasingly important role.[25]

Even though tackling the shipping of drugs involves some challenges, such as increased global trade and sophisticated concealment methods, intervening in the delivery model is recommended. Where the online actions and communication are strongly encrypted, the physical delivery of the package has been identified as the key vulnerability of darknet drug markets.[26] And even though postal systems are seen as the major bottlenecks of the online drug trade system, it appears that vendors are not worried about packages being seized. The chance of being caught is low. And when a package is intercepted, the package is, in most cases, destroyed or returned to the sender.[27] The strategy up until now has involved dismantling websites and apprehending buyers, however prosecutions of vendors have been very limited in Europe.[28]

While there is little discussion on the need to apprehend the producers, major dealers, middle-men and vendors, a debate is under way as to how drug users should be approached: as criminals or rather from a health perspective.[29] The EU Agenda and Action Plan on Drugs 2021-2025 clearly favours the health perspective in this regard.[30]

As mentioned before, a high enough (perceived) risk of apprehension has a deterrent and preventive effect.[31] One of the objectives should therefore be to increase the chances of detection and interception. Only then can certain competences, such as existing forensic techniques, be fully exploited. Police, customs and postal services each have their own competences of which they should make maximum use, and they should also exchange information and set up a common plan of actions.[32]

It is recommended to involve postal services alongside customs. Rather counterintuitively, research shows that although the internet provides the opportunity to trade globally, international transactions are not the norm. The fewer borders to cross, the lower the perceived risk for both vendors and buyers. For example, after the closure of the Silk Road, a Finnish marketplace arose that only caters for national buyers.[33] Under the terms of international drug treaties, customs services have more extensive powers to check cross-border items, while domestic correspondence is in general better protected under privacy regulations.[34] This discrepancy between the high volume of drug packages passing through the postal services and the limited competences of the postal services, should be addressed.

Europol has darknet investigation teams that, amongst other tasks, focus on centralising expertise, carrying out training and building capacities.[35] It is however recommended not only to train law enforcement, but also other partners such as postal services and courier companies.

Even though the packaging and transporting of drugs through postal services have greater similarities with the more conventional forms of smuggling than with cybercrime, information technology still provides several opportunities to facilitate the smuggling activities.[36] As described earlier, encrypted communication channels such as Telegram, Wickr or Signal facilitate the drop-off. Even more, there are legitimate companies that offer ICT that specifically shield communication from authorities. Such a company is trusted and well-known amongst criminals.[37] Consequently, it might prove advantageous to inform the management and leadership of communication companies of their role in the criminal business process within illegal drug trade and to incite them to take action.

Overall, because of the increasing importance of suppliers of legal goods and services, there is a need for open-mindedness and a willingness to involve and cooperate with (private) partners. On the one hand there are government partners such as the police, customs and postal services, and on the other hand there are partners from key industries such as information technology, social media, payment services, courier services, stealth packaging…[38] When collaboration is not possible, in some cases it might be necessary to use licensing regulations or prosecution of suppliers of legal goods and services who consciously contribute to the criminal business process of the illegal drug trade.

3.3. Needs for future action

Research is needed in order to close knowledge gaps concerning the online trade of drugs. Darknet drug markets are expanding and are challenging traditional drug markets and are likely to make parts of it obsolete. However, the interaction between online and offline is currently still poorly understood.[39] For instance, even though wholesale via darknet drug markets is limited, the large volume of small quantity sales suggests that vendors possess large stocks. How do they obtain their supply? How does a traditional established wholesaler come into play?[40] Furthermore, it remains unclear to what extent the players in the online drug trade can be considered as 'organised'. It appears that many vendors on darknet drug markets do not fit the profile of OCGs and rather fit the profile of lone wolfs.[41] Concluding, important knowledge gaps concerning darknet drug markets relate to

- drug sources
- links to offline markets
- illicit money flows
- role of organised crime[42]

Alongside filling in the gaps of poorly understood parts of the criminal business process, research needs to be encouraged because darknet drug markets are extremely agile in adapting their modus operandi.

3.4. Conclusion

In conclusion, there are two promising areas of action and two target groups in the prevention of and fight against the illegal trade of synthetic drugs through darknet drug markets.

1. To enhance the capacities of government authorities in order to increase chance of detection

- Create a legal framework that allows law enforcement to proactively investigate online.
- Build an up-to-date body of knowledge based on continuous observations on darknet drug markets
- Educate law enforcement, customs and postal services with regard to the latest developments
- Extend the competences of postal services to intercept and inspect suspicious items
- Encourage further scientific research into the sources of drugs, links to offline markets, illicit money flows and roles of organised crime in relation to darknet drug markets

2. To engage suppliers of legal goods and services in setting up barriers the criminal business process

- Inform and call courier and food delivery companies to action concerning their role in delivering drug packages to their final destination
- Inform and call social media and encrypted communication companies to action concerning their role in facilitating the communication and coordination of the shipment of drug packages to their final destination
- Inform and call stealth packaging companies to action concerning their role in concealing drug packages so they can pass through customs and other checkpoints
- Inform and call internet service providers to action concerning their role in hosting darknet drug markets
- Implement licensing regulations applicable to suppliers of legal goods and services who consciously contribute to the criminal process

ENDNOTES

1 EUCPN (2021), Darknet drug markets: the criminal business process explained. Part of the EUCPN Toolbox on Party Drugs. Brussels: EUCPN.

2 EMCDDA and Europol, EU Drug Markets: Impact of COVID-19, Luxembourg: Publications Office of the European Union, 2020, 12.

3 European Network on the Administrative Approach, Third EU Handbook on the Administrative Approach in the European Union, Brussels: ENAA, 2020, 20.

4 A more in-depth explanation of the administrative approach can be found in ibid.

5 Ibid., 27.

6 Ibid., 34.

7 EUCPN (2021), Darknet drug markets: the criminal business process explained. Part of the EUCPN Toolbox on Party Drugs. Brussels: EUCPN.

8 James Martin, Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket', *Criminology & Criminal Justice* 14:3 (2014), 358.

9 Ibid.

10 Ibid.

11 These signals were pointed out by expert Dirk Minten in a personal communication.

12 European Network on the Administrative Approach, Third EU Handbook on the Administrative Approach in the European Union.

13 EMCDDA and Europol, Drugs and the Darknet: Perspectives for Enforcement, Research and Policy, Luxembourg: Publications Office of the European Union, 2017, 35.

14 Centre for Crime Prevention and Safety (CCV), Manual for the Administrative Approach to Organised Crime, Utrecht: CCV, 2011, 34.

15 Ibid., 36.

16 Pieters Tops et al., *The Netherlands and Synthetic Drugs: An Inconvenient Truth,* The Hague: Eleven International Publishing, 2018, 25.

17 Gisela Bichler, Aili Malm, and Tristen Cooper, Drug Supply Networks: A Systematic Review of the Organizational Structure of Illicit Drug Trade, *Crime Science* 6:1 (2017), 15.

18 Martin, Lost on the Silk Road, 357.

19 Nicolas Christen, Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace: Carnegie Mellon University, 2012, 10.

20 Eileen Ormsby, Silk Road: Insights from Interviews with Users and Vendors, in: J. Mounteney, A. Oteo, and P. Griffiths (Eds.), *The Internet and Drug Markets*, Luxembourg: EMCDDA, 2016, 67.

21 Joost van Slobbe, The Drug Trade on the Deep Web: A Law Enforcement Perspectiv, in: J. Mounteney, A. Oteo, and P. Griffiths (Eds.), *The Internet and Drug Markets*, Luxembourg: EMCDDA, 2016, 81.

22 Daniel S. Nagin, Deterrence in the Twenty-First Century, *Crime and Justice* 42:1 (2013), 53.

23 Anita Lavorgna, How the Use of the Internet Is Affecting Drug Trafficking Practices, in: J. Mounteney, A. Oteo, and P. Griffiths (Eds.), *The Internet and Drug Markets*, Luxembourg: EMCDDA,, 2016, 89.

24 Ibid.

25 Martin, Lost on the Silk Road, 365.

26 EMCDDA and Europol, Drugs and the Darknet, 60.

27 Christen, Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace, 11.

28 van Slobbe, The Drug Trade on the Deep Web: A Law Enforcement Perspectiv, 80.

29 EMCDDA (Ed.), *The Internet and Drug Markets*, Lisbon: EMCDDA, 2016, 81.

30 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-606-commission-communication_en.pdf

31 Nagin, Deterrence in the Twenty-First Century, 53.

32 EMCDDA and Europol, Drugs and the Darknet, 60.

33 J. Mounteney, A. Oteo, and P. Griffiths, What Is the Future for Internet Drug Markets?, in: J. Mounteney, A. Oteo, and P. Griffiths (Eds.), *The Internet and Drug Markets.*, Luxembourg: EMCDDA,, 2016, 129.

34 Kristy Kruithof et al., Internet-Facilitated Drugs Trade: An Analysis of the Size, Scope and the Role of the Netherlands, Santa Monica: RAND Corporation, 2016, 26.

35 EMCDDA and Europol, Drugs and the Darknet, 62.

36 Martin, Lost on the Silk Road, 354.

37 Nadine Bijlenga and Edward Kleemans, Criminals Seeking ICT-Expertise: An *Exploratory Study of Dutch Cases, European Journal on Criminal Policy and Research* 24 (2018), 260.

38 EMCDDA and Europol, Drugs and the Darknet, 69.

39 Ibid., 51.

40 Ibid., 53.

41 Ibid.

42 Ibid., 56.

BIBLIOGRAPHY

Bichler, Gisela, Aili Malm & Tristen Cooper. Drug Supply Networks: A Systematic Review of the Organizational Structure of Illicit Drug Trade. *Crime Science* 6:1 (2017), 2. https://dx.doi.org/10.1186/s40163-017-0063-3.

Bijlenga, Nadine & Edward Kleemans. Criminals Seeking ICT-Expertise: An Exploratory Study of Dutch Cases. *European Journal on Criminal Policy and Research* 24 (2018), 253-65. https://dx.doi.org/10.1007/s10610-017-9356-z.

Centre for Crime Prevention and Safety (CCV). Manual for the Administrative Approach to Organised Crime. Utrecht: CCV, 2011.

Christen, Nicolas. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. Carnegie Mellon University, 2012.

EMCDDA (Ed.). *The Internet and Drug Markets*. Lisbon: EMCDDA, 2016.

EMCDDA & Europol. Drugs and the Darknet: Perspectives for Enforcement, Research and Policy. Luxembourg: Publications Office of the European Union, 2017. https://dx.doi.org/10.2810/834620.

EMCDDA & Europol. EU Drug Markets: Impact of COVID-19. Luxembourg: Publications Office of the European Union, 2020. https://dx.doi.org/10.2810/19284.

European Network on the Administrative Approach. Third EU Handbook on the Administrative Approach in the European Union. Brussels: ENAA, 2020. https://administrativeapproach.eu/publications/third-eu-handbook.

Kruithof, Kristy, Judith Aldridge, David Décary-Hétu, Megan Sim, Elma Dujso & Stijn Hoorens. Internet-Facilitated Drugs Trade: An Analysis of the Size, Scope and the Role of the Netherlands. Santa Monica: RAND Corporation, 2016.

Lavorgna, Anita. How the Use of the Internet Is Affecting Drug Trafficking Practices. In: J. Mounteney, A. Oteo, and P. Griffiths (Eds.). *The Internet and Drug Markets*. Luxembourg: EMCDDA, 2016, 85-90.

Martin, James. Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket'. *Criminology & Criminal Justice* 14:3 (2014), 351-67. https://dx.doi.org/DOI: 10.1177/1748895813505234.

Mounteney, J., A. Oteo & P. Griffiths. What Is the Future for Internet Drug Markets? In: J. Mounteney, A. Oteo, and P. Griffiths (Eds.). *The Internet and Drug Markets*. Luxembourg: EMCDDA, 2016, 127-33.

Nagin, Daniel S. Deterrence in the Twenty-First Century. *Crime and Justice* 42:1 (2013), 199-263. https://dx.doi.org/10.1086/670398.

Ormsby, Eileen. Silk Road: Insights from Interviews with Users and Vendors. In: J. Mounteney, A. Oteo, and P. Griffiths (Eds.). *The Internet and Drug Markets*. Luxembourg: EMCDDA, 2016, 61-7.

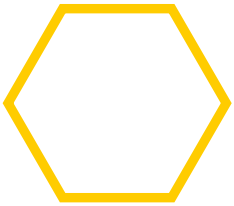
Spapens, Antonius, Maaike Peters & Dirk Van Daele. *Administrative Measures to Prevent and Tackle Crime*. The Hague: Eleven International Publishing, 2015.

Tops, Pieters, Judith van Valkenhoef, Edward van der Torre & Luuk van Spijk. *The Netherlands and Synthetic Drugs: An Inconvenient Truth*. The Hague: Eleven International Publishing, 2018.

van Slobbe, Joost. The Drug Trade on the Deep Web: A Law Enforcement Perspectiv. In: J. Mounteney, A. Oteo, and P. Griffiths (Eds.). *The Internet and Drug Markets*. Luxembourg: EMCDDA, 2016, 77-83.

CONTACT DETAILS

EUCPN Secretariat
Email: eucpn@ibz.eu
Website: www.eucpn.org



TWITTER.COM/EUCPN
FACEBOOK.COM/EUCPN
LINKEDIN.COM/COMPANY/EUCPN