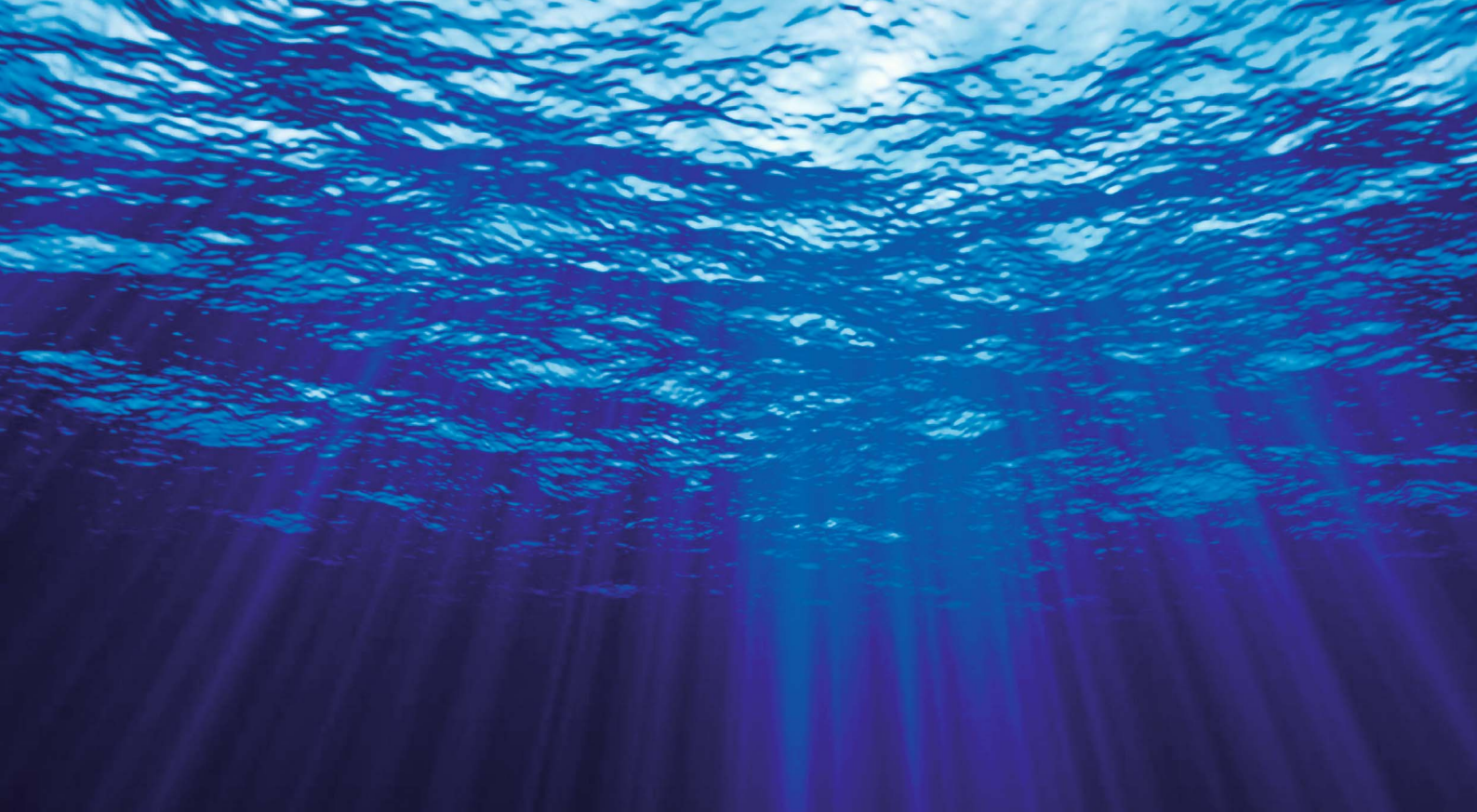


Drug related cybercrime and associated use of the Internet

Overview, analysis and possible actions by the Pompidou Group

P-PG / (2013)4

Pompidou Group
Groupe Pompidou

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Co-operation Group to Combat Drug Abuse and Illicit trafficking in Drugs

Pompidou Group
Groupe Pompidou

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Co-operation Group to Combat Drug Abuse and illicit trafficking in Drugs

P-PG (2013) 4

Drug related cybercrime and associated use of the Internet

Overview, analysis and possible actions by the Pompidou Group

1 Executive summary

According to various sources, the online trade of drugs is growing fast. Recent developments in web technologies have enabled the emergence of a new global online black market for illegal substances. New anonymous marketplaces such as Silk Road and Black Market Reloaded mark a paradigm shift in how drug crimes are committed today: Illegal substances are offered openly but there is no way to stopping it or to identifying the ones involved in the criminal activity. Law enforcement authorities are aware of the phenomenon but are struggling to find the effective means to tackle it.

There is a clear and outspoken need for sharing best practice and for the coordination of interventions against the drug trade in anonymous networks. The Pompidou Group – through its wide geographical and target group outreach, multidisciplinary approach as well as established networks and the capability of creating new ones – is in a good position to act as as a facilitator for a network of experts and professionals working to tackle the growing new trend.

Chapter two looks at different ways drugs are sold over the Internet today, having a specific focus on anonymous networks. Chapter three presents a review of existing activities related to online drug trade in selected international and national organisations. Chapter four analyses points of intervention. Finally, chapter five summarises the findings and gives recommendations for future activities.

Contents

Glossary of terms

Anonymous networks: Different sub-networks of the Internet, such as Tor, Freenet and I2P, inside of which the users' identities and locations are masked and all the communication is encrypted. Also referred to as the **Darknet** or the Dark Web. See p. 8 for more information.

Anonymous networks consist of **nodes**, which are typically pieces of software (e.g. "Tor Browser Bundle") running on volunteering individuals' computers. Information in the anonymous networks is transmitted through **circuits**, which are a series of interconnected nodes. See p. 8 for more information.

Payments for illegal purchases are increasingly done by using **virtual currencies** such as **Bitcoin**. Bitcoins allow for anonymous peer-to-peer money transfers, making it virtually impossible to follow the transactions or identify the holders of the electronic money. See p. 12 for more information.

2 Introduction

Cybercrime is one of the fastest growing forms of criminality today. Globally, its profits have surpassed those of the international illegal drug business, and its estimated costs for individuals, corporates and societies range from billions up to one trillion USD. Organised criminal groups are increasingly utilising the Internet in their activities.

The total size of the new online market for psychoactive substances is unknown, but several indicators point out that it is expanding fast. For example, EMCDDA reports that the number of websites selling new psychoactive substances has doubled every year since 2010, reaching 693 in January 2012. Also, the number of new sellers in Silk Road, the presumably biggest anonymous online marketplace for illegal drugs, grows by 50 every month. Customs report on increased number of drug seizures, delivered by mail and presumably originating from online marketplaces.

Another feature of the new online market is its increased capability to evade law enforcement interventions through an enhanced level of anonymity and encryption. The clandestine sub-networks of the Internet, originally developed for military purposes and generally known as the Darknet, form the technological platform for new online marketplaces for drugs.

On the marketplaces located in the Darknet, drugs are sold openly, but the identities and locations of the actors, as well as the marketplace itself are masked. The most sophisticated ones integrate different anonymising technologies and services, offering a convenient and relatively secure way to sell and buy illegal substances online. The technologies on which the marketplaces operate are constantly developed.

Even though the online market of illegal substances is still a fraction of the total drugs market, its rapid growth and increasing capability to conceal itself call for specific attention. In an interview for this study, Mr. John Carr, a Senior Expert Adviser to the United Nations (ITU) and an Expert Adviser to the European Union (European Network and Information Security Agency), described the anonymous networks as “hugely significant” for today’s crime prevention:

> *Criminals, in effect, have the capability of putting a great deal of the evidence of their crimes beyond the effective reach of law enforcement. Strong encryption is as yet unbreakable for all practical purposes, and it is certainly unbreakable in the context of routine police operations.*

The online market is extremely global by nature, facilitating the spread of new drugs and drug cultures. Mr. Carr concludes that the Darknet represents nothing less than a paradigm shift in the world of crime.

This document provides an overview of and analysis the current developments in the supply of illegal substances in the Internet and responses to counteract these that are under way. Specific attention is paid to online marketplaces in the Darknet. The primary angle of this analysis is supply reduction, but perspectives of demand and harm reduction are given where appropriate.

2.1 Cybercrime on the rise

Interpol introduces cybercrime as one of the fastest growing areas of crime. FBI’s Internet Crime Complaint Centre’s (IC3) complaint statistics show a steady growing trend, and Symantec reports a 93 % increase in web attacks from 2010 to 2011.

The estimates of the financial impact of cybercrime vary a lot, ranging from billions up to one trillion US dollars. The numbers are uncertain and probably exaggerated to some extent. Whatever the real figure, cybercrime is perceived as one of the most prominent threats to societies today. For example, the start of Europol’s European Cybercrime Centre (EC3) in January 2013 is a clear signal of the growing importance of cyber-security to the very competitiveness of the EU.

The online market of illegal goods, including narcotics, is typically not mentioned in the definitions of cybercrime. The Cyber-security Strategy of the European Union, for instance, refers to cybercrime as

> *a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g.*

fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).

INTERPOL's and Europol's definitions of cybercrime are very similar in content, and do not refer to the online drug market. The importance of drugs in the political agenda, both in Europe and beyond, has decreased in importance over the past decades, a phenomenon which is clearly reflected in the current strategy of the European Union. One of the Union's seven flagship initiatives is the Digital Agenda for Europe. None of its seven Pillars or 100 Actions relates to drugs, including the Pillar "Trust and Security".

Even though the importance of drugs in the sphere of cybercrime is currently low, the relevance of cybercrime in the drug market is growing and deserves special attention.

2.2 What has the Internet done to drug supply?

Cybercrime is extremely innovative by nature, posing a serious challenge to the existing law enforcement methods. The Internet provides several advantages to the supply of controlled substances:

1. It is a cost-effective way to promote any idea or product on a global scale. Unlimited by time and space, the Internet reaches and connects people and cultures, facilitating the fast spread of new products and trends everywhere on the planet. New drugs and ways of using and producing them are no exception.
2. The new information and communication technologies (ICT) offer powerful tools for operating anonymously and for preventing third parties from intercepting confidential communication. This includes not only communication between individuals and groups, but also the operating of marketplaces and selling of drugs anonymously.
3. The Internet is a constantly evolving ecosystem of ideas, technologies and businesses. The very nature of the wired world ensures that new, innovative ways of supplying illicit drugs - and evading the law enforcement authorities - will continue to develop.

As a result, a virtual but real, anonymous and globally operating black market of illicit goods and services has emerged. The most advanced versions are combining many of the existing technologies and online services in order to provide their customers a smooth and secure platform for shopping not only drugs, but arms, stolen goods, illicit services etc.

Anonymity to decrease risk

The technical building blocks for a completely untraceable process of doing business on illegal substances have been in place for a several years but have been put together and utilised in a full scale only quite recently. The new developments put law enforcement authorities in a situation, where they can see the criminal activity to take place, but have very few means - and often limited resources - to intercept it.

For example, the location, physical and virtual, of an online drug marketplace is typically hidden, which makes it virtually impossible to close it down. At the same time, all locations and identities of buyers and sellers have been masked, and all the direct communication between them is encrypted. This means that getting any information about who or where the suspects are or what they are buying, is practically impossible. What's more, the Internet provides anonymous ways to paying for the illicit purchases (see 3.4 for more).

This reduces the risk of the agents on the markets to get caught, and subsequently increases the attractiveness of engaging in the illicit activity.

New channels for trafficking

The virtual and global distribution of demand and supply has led to a partial rearrangement of drug trafficking. The orders from online marketplaces are typically small in size and delivered through postal or courier services. The sender may pack the drugs in vacuum-sealed bags to distract sniffer dogs, and use envelopes with company labels to make the shipment look less suspicious.

The buyer may be the end user of the product or a dealer who is purchasing narcotics to be delivered to the local market. The dealer may distribute the risk by ordering the substances in smaller shipments and to multiple locations.

A need for innovative approaches

The new avenues for drug supply through online marketplaces and to-door delivery call for new and innovative approaches of both supply and demand reduction. On the online marketplace, tactics of public presence, intelligence and infiltration have to be redesigned.

In customs and delivery services, improving the monitoring of mail deliveries, all the way from receiving the shipment to delivering it to letter box, may be a viable tactics. In addition, the discussion areas of the marketplaces are a way to meet the buyers and to make sure they know the risks involved and where to get treatment.

Just as the drug business is global, the prevention also needs a global approach. Cooperation, mutual support and sharing of information and best practice will be needed between different actors.

Possible interventions will be more discussed in-depth in 5.2.

2.3 Overlapping themes

Several other issues coincide with online drug markets.

1. Many of the Darknet websites selling drugs also offer other illegal goods like arms and stolen goods.
2. The Darknet also provides a forum for planning crimes and a channel for distributing materials related to child abuse and terrorism.
3. The more advanced marketplaces offer payment methods, the Bitcoin for instance (see 3.4), which are useful means for money laundering and avoiding taxes.

Any intervention targeted against online drug marketplaces is likely to come across with the abovementioned phenomena.

3 Description of the operational environment

3.1 How are psychoactive substances sold in the Internet

There are basically three ways of selling psychoactive substances in the Internet.

1. Individuals selling on discussion forums.
2. Online storefronts, operated by one individual or group of individual.
3. Online marketplaces, connecting buyers and sellers but not (necessarily) selling anything themselves.

The first type is more likely to be found in the Darknet or other restricted sites, whereas storefronts and marketplaces offering psychoactive substances can be found in both open and anonymous networks.

Public internet

Drugs

Illegal drugs can be found on sale on certain online marketplaces, often operating from China or India. For example, Tradett.com sells basically anything, including drugs, drug precursors and uncontrolled new psychoactive substances.

The sellers often promise "discreet delivery" but only disclose payment and shipping terms when contacted through an email address or contact form.

Drug precursors

Drug precursors are chemicals used in the manufacturing of controlled or illegal drugs. The chemicals, however, are widely used in the chemical industry to produce a wide variety of different legitimate products, ranging from plastics to cosmetics. Most drug precursors are controlled by authorities.

Drug precursor chemicals can be found on same marketplaces as illegal drugs. Selling anonymously online is also a way to work around the pre-export notification system.

In addition, the Internet hosts a range of storefronts offering cannabis seeds and production equipment.

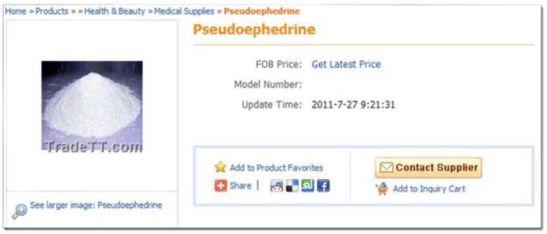
New psychoactive substances

Sellers of new psychoactive substances exploit loopholes in current legislations as well as differing classifications in different countries. Recently, about 50 new, uncontrolled psychoactive substances have entered the market every year, with legislation falling behind. Most of the new psychoactive substances are sold online.

EMCDDA has reported a dramatic increase in the number of websites selling new psychoactive substances. In January 2012, 693 online shops were identified, having more than doubled since January 2011 (314 shops) and quadrupled since January 2010 (170 shops).

Heroin – www.tradett.com

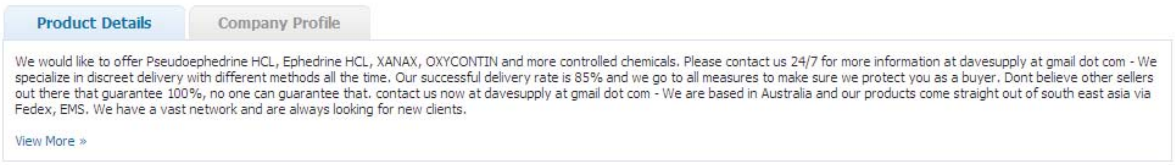
Cannabis seeds – www.amsterdammarijuanaseeds.com



Pseudoephedrine – www.tradett.com

MDAI – www.legaliiis.com

"Legal Highs, Herbal Highs, Stimulants, Aphrodisiacs and loads more" – www.herbalhighs.com



"We specialize in discreet delivery with different methods all the time. Our successful delivery rate is 85% and we go to all measures to make sure we protect you as a buyer". A service promise by a pseudoephedrine seller in www.tradett.com

Purchases in the online stores can be done by bank transfers and worldwide money transfer services such as Western Union or MoneyGram. The shipments are done through globally operating courier services.

Prescription-only medicines

The amount of medicines sold over the Internet has been on increase. In the United States, for example, the non-medical use of prescription drugs exceeds the use of most controlled substances.

Many of the pharmacies operating online sell unauthorised controlled substances, both prescription-only medicines and products that are illegal in many countries. The World Health Organization estimates that 50 % of medicines available from such websites are counterfeit, causing serious health risks to ones using them. In 2011, the Council of Europe drafted a convention, which constitutes, for the first time, a binding international instrument in the criminal law field on counterfeiting of medical products and similar crimes involving threats to public health.

Since 2008, INTERPOL has launched a multi-phase *Operation Pangea* to tackle the problem of unauthorised online pharmacies. Its latest phase, Pangea V, was operated between 25 September 25 and 2 October, 2012, and resulted in the shutdown of more than 18 000 illegal online pharmacies. In addition, pharmaceuticals worth USD 10.5 million were seized in the operation, which involved law enforcement, customs and regulatory authorities from 100 countries.

"Happy gardening" - mephedrone on sale at www.slyplants.com

Anonymous networks

In the Internet, there are several subnets, consisting of nodes run by volunteers. This study focuses on Tor (The Onion Router), which is the most popular of them. Other well-known anonymous networks are I2P and Freenet.

Tor allows for masking the identities and locations of users, administrators and servers, making all communication and transactions inside the network virtually anonymous and untraceable. While Tor is used for a number of valuable and legitimate purposes, it also serves as a platform for a virtual black market for drugs, arms and child pornography. It also offers various forums for planning of crimes and terrorist acts.

The development of Tor network technologies started in 1995 as a U.S. Navy project, which aimed at creating more secure communication networks. From 2004 onwards, it has been developed as an open source project funded by Electronic Frontier Foundation (EFF).

The purpose of the Tor project (www.torproject.org) is to

> *defend [Internet users] against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis.*

Tor network can be accessed with specific software called *Tor Browser Bundle*, or the *Tor client*. It is freely available at various sites, including the Tor Project website. Anyone running Tor client on his or her computer can also configure the software to function as a Tor network node. Tor clients form virtual circuits consisting of two or more Tor nodes, which relay client traffic to the destination server. The data is encrypted multiple times before being transmitted over the Tor network, so that the original data are available only at the exit node, the last node in the circuit. The slow speed of the connection and the need to install the Tor client are factors that currently curb the adoption of Tor network in larger scale.

Darknet marketplaces

All three ways to sell drugs – individuals, storefronts and marketplaces – are prevalent in the Darknet. This section focuses on marketplaces, as they comprise certain features, which make them worth closer inspection:

- they are truly global in terms of both supply and demand;
- their sales volumes are presumably bigger than of the other types;
- they rely on more sophisticated business models and technologies;
- means to intervene on marketplaces are at least partly transferable to the other types of selling.

Darknet hosts several online marketplaces for drugs and other illegal goods. The best known of them is Silk Road, which will be described in more detail in the following case study. Other known marketplaces are Black Market Reloaded and the General Store.

Typical features of the Darknet marketplaces are

- focus on illegal substances;
- masked identities and locations of buyers, sellers and the operators of the marketplace as well as of the marketplace itself;
- combination of different web technologies and services (Tor anonymity network, marketplace interface, virtual currency, strong encryption of private messaging etc.) into one operational unit;
- Bitcoins as method of payment;
- global delivery through postal and courier services;
- public rating of sellers.

Darknet marketplaces generally sell all kinds of drugs but also other kinds of products such as weapons, counterfeit products and literature as well as services such as hacking.

National Darknet sites

In addition to global marketplaces, there are also national Darknet sites, serving the public in their own language. Examples of such websites are the Russian websites RAMP: Russian Anonymous MarketPlace (http://ramp2bombkadwvgz.onion, Tor browser bundle required) and Shop of Magic Products (http://ovamadkumardi66b.onion), as well as the Finnish imageboard Thorlauta (http://zqiirytam276uogb.onion). In addition, the discussion board of Black Market Reloaded has subsections for several nationalities.

Case study: Silk Road

"Here's my point: Silk Road is about something much bigger than thumbing your nose at the man and getting your drugs anyway. It's about taking back our liberty and our dignity and demanding justice."

Dread Pirate Roberts, Founder of Silk Road

Silk Road
anonymous marketplace

Silk Road is the biggest, most technologically advanced and best-known marketplace for drugs in the Darknet, providing many lessons to be learned about the online drug market and its development.

Introduction

Silk Road is often referred to as the e-Bay or Amazon of drugs. Its Tor network address is http://silkroadvb5piz3r.onion. Going to the website requires the Tor client to be installed. The site has operated since February 2011 and has received a lot of attention especially in the U.S. and Australia.

Silk Road was brought to public awareness by an article in Gawker (a New York based blog) in June 2011. Having read the story, senators Charles Schumer and Joe Manchin urged U.S. Attorney General Eric Holder *"to take immediate action and shut down the Silk Road network".* The website is still in operation and growing in volume. Recently it was has been targeted by cyber attacks and has raised its capacity to resist attacks accordingly.

The operator of Silk Road is known as Dread Pirate Roberts (DPR). His true identity remains unknown. He is actively engaged in maintaining the website and communicating with the customers. DPR is a fierce proponent of liberal anarchism and abolition of state control.

Operation

Purchases at Silk Road are paid for in Bitcoins, an untraceable peer-to-peer "crypto-currency", a form of digital economy outside law. Bitcoins are exchangeable to national currencies and vice versa in dedicated web services such as Mt. Gox (mtgox.com). At Silk Road, payment takes place through system's built-in escrow account, where it is kept until the delivery of the products has been confirmed.

The products are shipped by regular mail or courier service to an address given by the buyer. Products are typically shipped in vacuum-sealed bags, making them difficult to detect by smelling. The delivery is often disguised in real or makeshift company envelopes.

The marketplace features an advanced feedback system, the purpose of which is to build trust between buyers and sellers. Feedback is always given upon finishing the purchase. The ratings of the sellers are public to the users.

Silk Road has user guides for buyers and sellers, promoting anonymity and security. The rules of the service strictly prohibit the marketing of weapons, child pornography, stolen goods, assassinations and stolen personal information. The product listing on the site is regularly moderated.

Market analysis

According to a measurement analysis done by a Dr. Nicholas Christin from Carnegie University in 2012, Silk Road brings together some 560 sellers and thousands (estimated up to between 30 000 and 150 000) of customers from around the world. About 50 new sellers register on the marketplace each month.

The annual transaction is estimated to reach USD 15 million, excluding deals closed through private listings called ”stealth listings”. The operator(s) of the website collects about USD 1.1 million as commission fees annually. In an interview for this study, Dr. Christin said the website has grown “quite a bit” since the end of data collection in July 2012.

Security issues

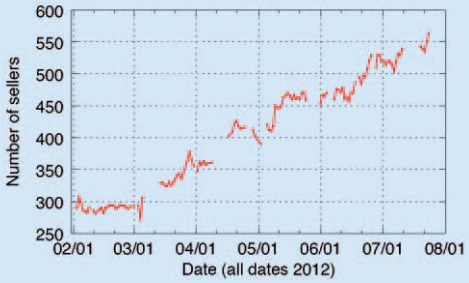
The IP addresses and consequently the physical locations of sellers, buyers and the web server as well as all transactions are protected by Tor anonymity and encryption. Login with username and password is requested upon entering the site.

The site features “stealth listings” of products, which are not shown in the normal Silk Road listings or linked to the site, and are only accessible through direct URL addresses. Stealth listings are used by buyers and sellers with established business relationships. The content of the stealth listings or the volume of sales through them is not known.

Country	Pct.
U.S.A.	43.83%
Undeclared	16.29%
U.K.	10.15%
Netherlands	6.52%
Canada	5.89%
Germany	4.51%
Australia	3.19%
India	1.23%
Italy	1.03%
China	0.98%
Spain	0.94%
France	0.82%

Country/Region	Pct.
Worldwide	49.67%
U.S.A.	35.15%
European Union	6.19%
Canada	6.05%
U.K.	3.66%
Australia	2.87%
World. excpt. U.S.A.	1.39%
Germany	1.03%
Norway	0.70%
Switzerland	0.62%
New Zealand	0.56%
Undeclared	0.26%

Above: Top 12 most frequent shipping origins (left), and acceptable shipping destinations (right).Below: Evolution of the number of sellers. Source: Christin, N. (Nov 2012)



A Delivery address is given to the seller in PGP-encrypted messages, and subsequently deleted from the Silk Road’s database.

Incoming Bitcoin payments are taken through a chain of dummy intermediaries (”tumbler”) to enhance anonymity. The site uses a mandatory escrow system to prevent swindling and a hedge against short-term fluctuations of Bitcoin.

The technical platform is constantly improving and increasing its security and Dread Pirate Roberts has stated in public that he is confident about Silk Road’s security measures against law enforcement tracking attempts.

3.2 New payment methods

The Internet has allowed for the development of new kinds of payment methods, which are also used to pay for drugs bought online.

Some of them function within existing economic systems (PayPal) but some are independent from national currencies and central banks, being virtual currencies (also known as electronic money) of their own right. Virtual currencies can be based on national currencies or gold (Webmoney, eGolder, Pecunix), but some of them are free-floating (Bitcoin).

Some of the new payment methods are administered by private companies, some are peer-to-peer currencies, the transactions of which are done directly between two individuals, without any intermediary. The licit uses for virtual currencies are still quite limited. They are often used because of their capability to retain their value (gold-based) or anonymity (peer-to-peer).

“Traditional”, non-virtual money transfer methods such as Western Union or MoneyGram have also been used to paying for drugs purchases.

Case study: Bitcoin

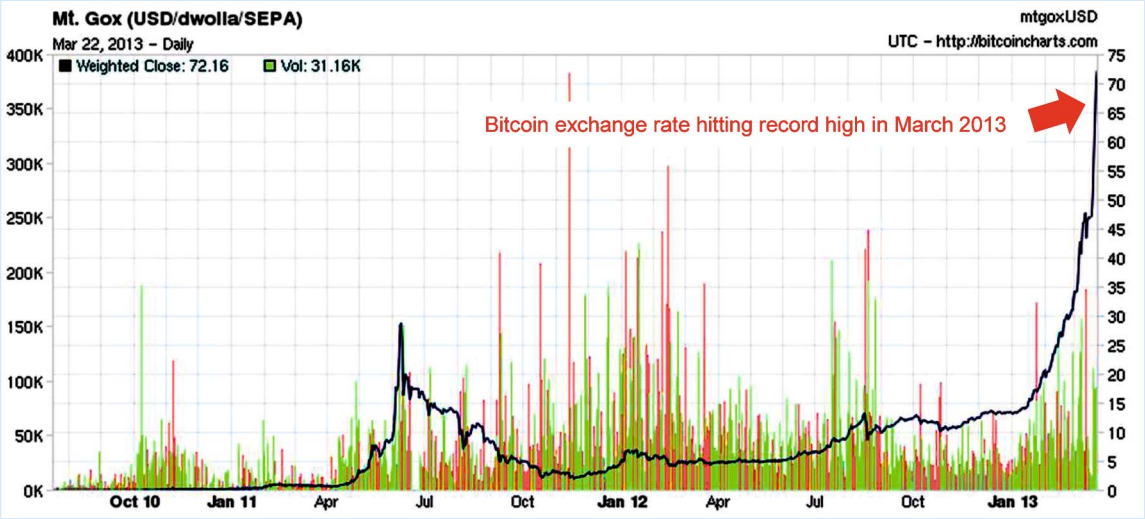
Of the new payment methods, Bitcoin (BTC) is especially interesting for several reasons. Firstly, it was the last missing link in securing full anonymity in the process of buying in the Darknet. Secondly, it has been widely adopted on the online drug markets. Thirdly, it is an ideological project, aiming at creating a currency – and a virtual economy – which are liberated from any control by government or other institutions. According to www.bitcoin.org,

> *Bitcoin is an experimental new digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: managing transactions and issuing money are carried out collectively by the network. Bitcoin is also the name of the open source software which enables the use of this currency.*

Bitcoin was started in 2009 by a pseudonymous founder known as Satoshi Nakamoto. It is an online-only currency, providing untraceable transactions as far as the holder of the Bitcoin "wallet" (a random series of numbers and characters) takes due care of security. Bitcoins can be exchanged for major real-world currencies in specialised services such as MtGox (www.mtgox.com).

Bitcoin's value is not fixed and is therefore floating. Bitcoin's exchange rate has fluctuated wildly during its existence, hitting record high during the writing of this study. The amount Bitcoins increases at a decreasing rate over time through a complex mathematical process called "mining", until it reaches 21 million, which is the maximum possible number of Bitcoins. The amount Bitcoins at the time of writing this report was 10 914 000, the total volume of the Bitcoin economy thus being about 400 million euros (about 37.7 €/BTC, after a steep rise over the past 6 months). The volume of Silk Road sales corresponds to about 4.5 % of the total BTCs exchanged through different services.

Attacking the Bitcoin economy has been introduced as one measure against the trade of illegal goods in the Darknet.



The development of Bitcoin's exchange rate against USD between July 2010 and March 2013. Source: bitcoincharts.com/charts/ (CC BY-SA 3.0)

3.3 Overview of existing activities

As a part of the study, a review of existing activities related to Darknet drug markets was done. The review covered a number of international organisations as well as national law enforcement authorities in Australia, Austria, Finland, the Netherlands, United Kingdom and the United States. The information was collected from the organisations' web pages, publications as well as press releases

and articles published in the media. In addition, several experts, both academics and practitioners, were interviewed for the review.

According to the review, national law enforcement authorities are aware of the phenomenon and some of them are already investigating cases dealing with trade originating from the anonymous marketplaces. In the Netherlands, the police are preparing an administrative advice for the Ministry of Justice. The phenomenon has also been identified by some of the international organisations but it has not become a priority. EMCDDA are considering exploring the issue in more depth.

The police authorities interviewed for the study reported several challenges in regards to investigations related to online drug trade:

- There is little information of and experience with the subject.
- There is no training related to the subject. Ability to investigate Darknet-related crimes depends on individual investigators' personal interests in and dedication to the subject.
- In some cases, the expertise related to cybercrime is located in specialised units but the investigation of drug cases is done on the municipal level, without enough exchange of information between the two levels.
- The resources for combatting cybercrime are scarce and often allocated to cases with a higher political priority, such as child pornography and terrorism.
- It seems that for the time being, there is no way to work around the anonymising and encrypting technologies applied in the Darknet.

Due to the new mode of operation brought about by the anonymous marketplaces, the customs increasingly encounter deliveries containing illegal substances, often packed in vacuum-sealed bags. Criminals prefer regular post, as their contents do not need to be reported to the customs in advance. In Europe, the Netherlands has been identified as a hub for illicit shipments. As a response, the customs in the New Zealand have scanned all postal deliveries from the Netherlands, and the Australian customs have tightened the monitoring of the deliveries from the country.

4 Analysis of possible points of interventions

The following interventions follow the business logic of Silk Road. See the process analysis on page 15 for an illustrated description.

Intervention point 1: Preventing the mainstreaming of online buying of drugs

Action 1: Keeping low profile
Silk Road has got a lot of public attention in the United States and in Australia, which have caused its user rates to skyrocket. As a communications strategy, being reactive rather than proactive is recommended. For possible media contacts, a fact sheet with key messages should be prepared.

Action 2: Describing it in the public as criminal and marginal activity, emphasising risks
Online market increases the availability of drugs by bringing the market home – or any other place where the access to anonymous networks is available. Drug users will get their substances anyway, online sales is just a way to make it easier, safer and in a more convenient fashion. For people who are not yet using drugs, online markets may lower the threshold to try and start using drugs.

Any communication to the public about buying and selling drugs online should emphasise that it

- is marginal and illegal activity
- is organised by and benefits criminal groups (and often harms many others),
- poses a threat to one's health (you never know what you get) and
- even though the marketplace itself is anonymous, shipping is monitored by the law enforcement authorities.

Action 3: Explaining the risks to those who have logged in to Silk Road
Silk Road has a lively community forum. Many of those who have logged in in order to buy drugs are likely to have a look there. An independent actor with professional credibility and a sincere harm reduction mission (possibly an NGO) could take an active role in providing reliable information on the forum about the risks and harms as well as preventing them. Getting the acceptance of the administrators of the site as well as the community itself is of key importance. Information about the real risks may put off some potential buyers. Drug users are often very knowledgeable about different substances and their uses, which calls for a high level of professionalism of any organisation carrying out the intervention.

Intervention point 2: Preventing the use of anonymising technologies

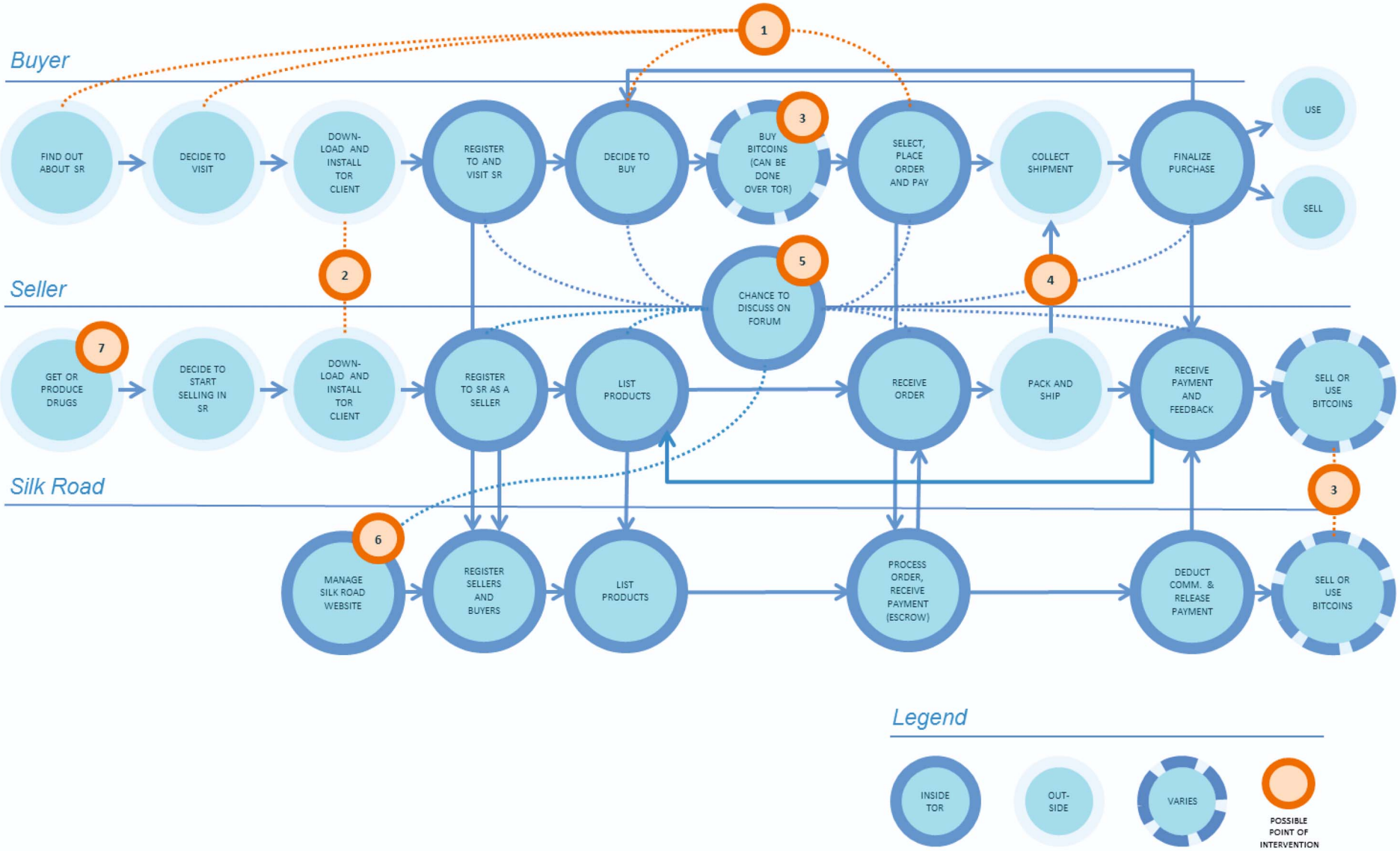
Technically this intervention is hardly possible because the Tor technology is developed and distributed as free open source software. The Chinese firewall can limit the communication of Tor nodes to a certain extent, but the developers of Tor are finding new ways to prevent the firewall from detecting Tor data transfers from other data streams.

Another possible approach is to criminalise the use of anonymising technologies. It would be a strong statement against freedom of speech and privacy, and politically difficult in many countries. Even considering it should be a matter of high-level political debate where the harms posed by anonymous networks (related not only to drugs) should be weighed against their benefits. Also, any government enacting such a law ought to have the resources to enforce it. Moreover, such a policy may have unexpected counter-effects and repercussions. Regardless of such considerations, these issues are of a more general nature that would fall into the remit of the Council of Europe's Cybercrime Convention and also the CoE Policy on Internet Governance.

Intervention point 3: Intervening the Bitcoin economy
Bitcoins are increasingly used on the online marketplaces to pay for drugs. The Bitcoin economy is highly volatile, with a history of strong value fluctuations. Silk Road uses hedging against fluctuations, which makes any attacks against the currency not only expensive but rather irrelevant, too.

What might, however be worth exploring is to try to identify the individuals doing the biggest Bitcoin exchanges in the dedicated services such as MtGox. This can probably not be done without a request

Buying drugs at Silk Road – process analysis



by courts in the countries where the Bitcoin exchanges operate, and may prove difficult to carry out in practice. There has been an attempt by the Bitcoin community to track down a wallet containing more than 500.000 Bitcoins, allegedly belonging to someone involved in Silk Road. The attempt ended up without success: The Bitcoins disappeared without a trace and the holder of the wallet was never revealed.

Intervention point 4: Improving the monitoring of mail and courier deliveries
Drugs acquired from online marketplaces are typically delivered to the customer by mail or courier. Improving the monitoring of the deliveries may be an effective way to both intercept illicit deliveries as well as to reduce the attractiveness of the delivery method among customers. Moreover, this is a strategy which has led to seizures and arrests in several countries. A more coherent way to operate, better resources and sharing of information and best practice between customs and delivery services might prove to have some impact.

Intervention point 5: Presence and information collection
Having a presence in Silk Road may have several different goals and modes of operation:

Action 1: Gathering information and building knowledge
Online drug markets are still a relatively new phenomenon, at least in the current magnitude. Learning about the modes of operation and structure of the existing online drug market, as well as following new trends and the prevalence of new psychoactive substances will be helpful for any future interventions against online drug markets.

Action 2: Police presence
The Silk Road community is quite paranoid. Visible presence of law enforcement might keep the community on their toes and newcomers from buying the drugs. The Drug Enforcement Agency of the United States has admitted their presence in Silk Road but has not disclosed any details of their activities. Whether clandestine action is better that public presence remains to be decided.

Action 3: Harm reduction intervention
Silk Road users discuss the risk and harm reduction possibilities on the community forum. A professional presence, in the way described in Action 3 of Intervention point 1, might be meaningful way to prevent harm and to make a contact to the online community.

Intervention point 6: Attacking Silk Road infrastructure
The Tor network is rather resistant against different forms of attacks, and is constantly developed to be able to better deal with different threats. Also, the defences of Silk Road are continuously improved, especially after two identified attacks against the site in late 2012. So far, the service has allegedly not been compromised, even though many have aspirations to bring it down. Considering the way the whole system has been built to resist attacks, taking this approach may not viable to agents without remarkable technological resources.

Intervention point 7: Detecting online suppliers through real-world investigations
Even though online suppliers are able to retain their anonymity while selling drugs in the Darknet, the procurement or production of the drugs has to be done in the same way as in the regular drug business. Combining information from regular drug investigations with information received from online marketplaces (country of origin and other clues) and possible test purchases (postmark, package, fingerprints) may help in tracking down online suppliers. Awareness-rising as well identification and dissemination of best practice may provide police officers with tools for cracking down on online suppliers.

Intervention point 8: Building expertise on the phenomenon (not in the process chart)
The knowledge of the new online drug market model is still quite scarce and scattered among different professionals and academics. There is a need to identify, collect, structure and disseminate the existing knowledge and best practice, related to supply (customs and police), demand and harm reduction.

Intervention point 9: Advocacy and raising awareness (not in the process chart)
European professionals and decision makers are still largely unaware about the emergence of the new anonymous black market in the Darknet. Yet still small in size, it is a growing trend, which is transforming the way drugs are bought. What's more, the Darknet offers channels not only for drugs but for other illegal and harmful products, services and information. Incorporating online drug sales into the cybercrime agenda and raising professionals' awareness should be considered as priorities of the intervention.

5 Conclusions and recommendations

Cybercrime and the online trade of drugs are a growing trend. The recent developments in web technologies have enabled the foundation of new, totally anonymous marketplaces for drugs. The trade on those marketplaces, despite being open and public within the Darknet, is beyond the reach of law enforcement authorities, and have caused confusion and frustration among them. Authorities in several countries are aware of the new phenomenon and are looking for ways to intervene it. There is a need for joint activity to build up professional readiness to fight the drug trade in the Darknet.

Recommendation 1: Building international networks to share knowledge and building expertise

The online drug trade is a global phenomenon, which calls for coordinated international action. As the current level of knowledge about anonymous drug markets is fairly limited and scattered, a recommended starting point is to collect the internationally existing knowledge and good practice, and to establish ways to provide it to professionals working with the subject. International professional networks are useful for both collecting and disseminating knowledge. On the national level, relevant and practical information has to be available to the professionals on all levels of the command chain.

Several investigations against suppliers operating in the Darknet marketplaces are underway, producing valuable information about how the drug business in the Darknet is done. Some police organisations are even documenting their findings for a wider use. There is a growing body of new research related to the technological, economic and social aspects of the Darknet marketplaces. Also, some prevention organisations working in the Darknet can provide useful information about the marketplace communities.

Recommendation 2: Deploying different strategies

Supply and harm reduction strategies are recommended in the Darknet. Tackling the supply of drugs directly is difficult because of the anonymity provided by the Darknet, but improving the monitoring of mail deliveries and understanding better how the Darknet functions as a parallel supply channel may help law enforcement authorities to curb the supply originating from the anonymous marketplaces.

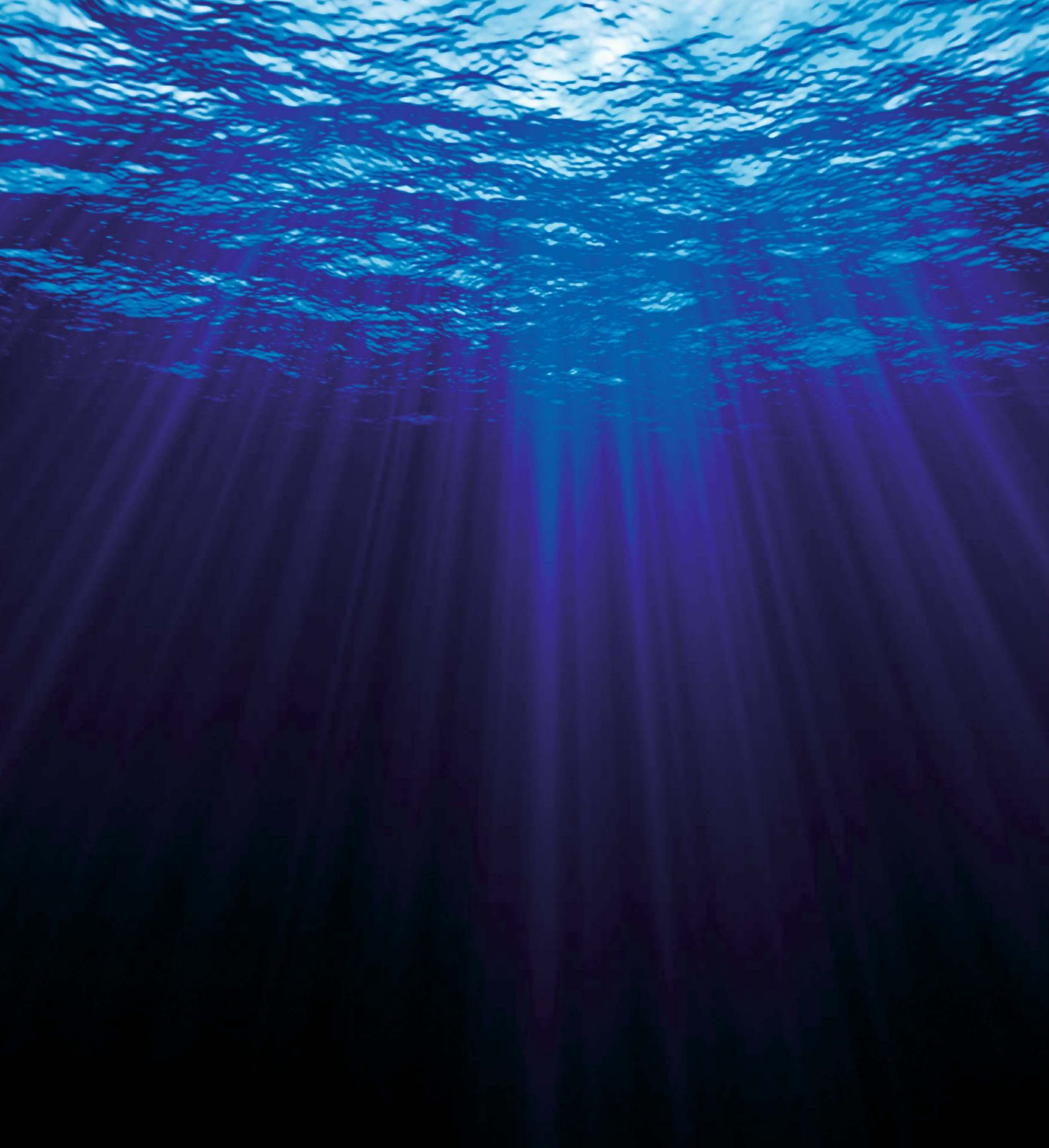
From harm reduction's point of view, the Darknet is an interesting opportunity to interact with the people who use and test on different kinds of psychoactive substances. It is both a channel to do harm reduction and way to learn about it. The study did not identify any treatment services provided in the Darknet, even though it would be a natural place to provide or market such services.

If a demand reduction strategy is to be implemented, secondary and tertiary reduction levels are possible, as the people in the marketplace are already using or considering using drugs. The Darknet is a very challenging environment for demand reduction as the people reached there are likely to have a very positive attitude towards drugs.

Recommendation 3: Forming operative partnerships with service providers

Drug trade in the Internet depends on a number of legal services, both public and private, which have the common interest with law enforcement authorities and drug prevention professionals to stop the trafficking in the illegal substances. Such services include Internet service providers, mail and courier services as well as the online currency exchange agencies providing Bitcoins. Forming partnerships with such organisation is recommended to secure the impact and sustainability of any intervention.

On the international level, organisations such as the Universal Postal Union, International Telecommunication Union, The European Telecommunications Network Operators' Association etc. are examples of potential partners.



Pompidou Group
Groupe Pompidou

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE