The illicit drug trade on the dark net: Analysing the need for a new EU Framework

Master Thesis

Name: Yasmine Hassan

Student number: s1750283

Program: International Relations – European Union Studies

Supervisor: Dr. J.S. Oster

2nd Reader: Dr. E. Cusumano

Abstract

The tools and means of the illicit drug trade change over time due to technological innovation. Consequently, the trade in illicit drugs nowadays also occurs on the dark net – that part of the internet that is intentionally hidden and requires specific privacy enhancing software to gain access. As a result, governments and law enforcement agencies are faced with a new phenomenon. Several scholars and EU reports have called for a new approach. With this thesis, the application of the current European Framework on illicit drugs is applied to three characteristics of the illicit drug trade on the dark net: the lack of borders, its dependency on conventional postal services and the level of anonymity.

This study found that the consequences of these characteristics in the field of jurisdiction, controlled deliveries and privacy do not necessarily constitute problems for the application of the current EU Framework on the illicit drug trade on the dark net.

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION

Throughout human history, people have used drugs or other forms of psychoactive substances; it is estimated that people in South America have been chewing coca leafs from approximately 1000 BC onwards (Boekhout van Solinge, 2004, p 9). The cultivation of the opium poppy for its psychoactive effect (used for heroin and other opiates), has existed for over 8000 years (Boekhout van Solinge, 2004, p 8). The prohibition on drugs however, is a relative recent issue and has evolved in a worldwide 'war on drugs' which aims for a world without illicit drugs use (HRW, 2017). The European Union has developed an EU Drugs Strategy (2013-20) and an EU Action Plan on Drugs 2013-2016 (together referred to as 'EU Framework') which aims to reduce the drug supply, drug demand and drug-associated risks and harms.

However, as technological innovation emerged, new methods and means became available for the trade in illicit drugs, such as the internet. The internet has rapidly evolved from 1962 onwards and has impacted almost every aspect of everyday live[1] (Leiner et al., 1997). The internet can be divided in multiple areas. That part of the internet that can be approached by search engines such as Google is known as 'the surface web'. A large part of the internet is hidden from search engines and includes specific governmental websites or password encrypted sites such as webmail. This is referred to as the 'deep web'. A portion of this 'deep web' is predominantly used for illegal activities and is referred to as the 'darkweb' or the 'dark net'[2]. This part of the internet can only be accessed with special software, such as The Onion Router, otherwise known as Tor (Barratt & Aldridge, 2016, p 2; Huang et. al., 2016, p 1).

The concept of online marketplaces such as eBay or Amazon can also be applied to the dark net, though in this capacity these marketplaces are known as cryptomarkets. Where marketplaces such as eBay allow for several payment methods (e.g. Mastercard or iDeal), cryptomarkets depend on cryptocurrencies, mainly the bitcoin, which are generally perceived as anonymous. And rather than the legal goods that are offered on eBay, the listings on cryptomarkets mainly concern the trade in illicit goods, including illicit drugs.
In this thesis, the applicability of the current EU Framework on this form of illicit drug trade will be analysed.

[1] As been elaborated on in for example Giddens, A. (2013). *The consequences of modernity*. John Wiley & Sons; or Castells, M. (2011). *The rise of the network society: The information age: Economy, society, and culture* (Vol. 1). John Wiley & Sons; or McLuhan, M., & Powers, B. R. (1989). *The global village: Transformations in world life and media in the 21st century*. Oxford University Press, USA.
[2] From this point onwards, the term dark net will be used as it corresponds with the terminology of the European union and its agencies.

CHAPTER 2. STUDY CHARACTERISTICS

2.1. EXISTING LITERATURE

Several studies have been conducted on the illicit drug trade on the dark net, which are mainly descriptive. For example, studies as conducted by for example Mounteney et al. (2016b) or Aldridge & Décary-Hétu (2016a) provide a general overview of the illicit drug trade on the dark net and its characteristics. In addition, some studies have a country-specific focus with the aim of mapping the situation for that country (e.g. Broséus et. al., 2016; Phelps & Watt, 2014; Kruithof et al., 2016a). Other studies perform behavioural analyses on the users of these cryptomarkets (e.g. Aldridge & Askew, 2017; Décary-Hétu et. al., 2016; Cox, 2016a; Tzanetakis et al., 2016) or have an ethnographic approach to understand the underlying notions, such as activism (e.g. Maddox et. al., 2016; Gehl, 2016). Few studies focus on the reaction of law-enforcement agencies in general (e.g. Van Slobbe, 2016) or on specific operations conducted by law-enforcement agencies (e.g. Décary-Hétu & Giommoni, 2017).

In addition to studies on the illicit trade in specific, many studies concern cryptomarkets in general and lack a specific focus on the illicit drug trade. These studies often focus on the required technologies and their characteristics. For example, Cox (2016b) provided a general overview of the application of the bitcoin and encryption on these cryptomarkets, while some studies focus on the role and technological implications of the Tor browser (e.g. Chaabane et al., 2010; Huang & Bashir, 2016; He et al., 2007; Moore & Rid, 2016; Bancroft & Reid, 2017) or the bitcoin (e.g. Juhász et al., 2016; Grinberg, 2011; Böhme et al., 2015) in specific.

Few studies analyse the illicit drug trade on the dark net in the realm of cybercrime. Martin however does and argues that a new category of cybercrime should be established for this form of illicit drug trade (Martin, 2014).

This touches upon the topic of internet governance. An extensive amount of studies has been conducted in this field, which can roughly be divided in two strands; those with a technological focus and those with a theoretical or political focus. Studies such as conducted by Lessig (1998), Lessig (2009), Berman (2002) or Goldsmith & Wu (2006) focus on the technical regulation which include the regulation of code and protocols. Code and protocols constitute the building blocks of cyberspace and are therefore valuable as these have the ability to shape

it. As Mueller (2002) stated about the *'domain name issue'*[3] on the intersection of technical management and regulatory control:*"Where does one end and the other begin?"* (Mueller, 2002, p 8). Studies as for example those of Netanel (2000), Goldsmith (1998) or Sassen (2000) on the other hand, approach internet governance from a more theoretical or political point of view. This often concerns the notion of self-governance and these studies often conclude that there is a lack of self-governance of the internet and a form of regulation is in fact required.

Overall, the societal relevance of understanding the illicit drug trade on the dark net and its effect on policy implementation becomes clear in policy documents, meeting reports and threat assessments performed by the European Union. For example, the dark net was characterized as the *"[..] key facilitator for various criminal activities, including the trade in illicit drugs[..]*" in the 'Serious and Organised Crime Threat Assessment' by EUROPOL (Europol, 2017, p 22). Other documents that address the significance of cryptomarkets in the field of the illicit drug trade or organised crime in general include the annual 'European Drug Report', the annual 'World Drug Report', the 'Meeting Report from the Internet and Drugs expert meeting of 7 & 8 June 2015' and publications of the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) such as the 'EU Drug Markets Report'. These reports however, are rather descriptive and merely provide a broad overview of the problem without precisely identifying the bottlenecks for policy implementation or governance. Generally, these documents highlight the need for additional research or a more effective approach.

Overall, the above-mentioned studies generally lack a specific focus on the consequences for governance or policy implementation that originate from the characteristics of the illicit drug trade on the dark net. Most of the literature merely describes this phenomenon, despite the societal relevance that is indicated by EU agencies.

[3] Every internet site has been assigned a specific set of numbers which makes the internet site visible online ('IP address'). Though, for people to easily access that internet site, this set of numbers is then linked to a set of letters ('domain name system/DNS'). In practise this would mean that the website of Leiden University can be accesses through https://www.universiteitleiden.nl in addition to its IP address 132.229.13.193. A logical assumption then is that webpages should not have identical IP addresses nor identical domain names. The Internet Corporation for Assigned Names and Numbers (ICANN) is involved in this process: it coordinates the "*Internet's naming system*" (ICANN, n.d.). Even though ICANN prefers to say that this coordination falls under "*[..]technical management[..]",* it is perceived as, in fact, a form of power (Mueller, 2002, p 7; Sassen, 2000, p 22). Moreover, ICANN states on its website: "*ICANN coordinates these unique identifiers across the world. Without that coordination we wouldn't have one global Internet"* (ICANN, n.d.).

2.2. RESEARCH QUESTION

To address the above-mentioned research gap, this thesis aims to answer the research question:

To what extent can the current European framework against traditional illicit drugs be applied on the illicit drug trade on the dark net?

This research question consists out of two components. First, it entails an analysis of the current European Framework which consists out of the EU Drugs Strategy 2013-2020 and the EU Action Plan on Drugs 2013-2016. The EU Drugs Action Plan for the period 2017-2020 is expected mid-2017 and therefore not included in this thesis. This analysis serves to identify the characteristics of this EU Framework in addition to its objectives and actors.
Secondly, this research question involves the application of the EU Framework on the illicit drug trade on the dark net. This requires an understanding of the dark net, the applied technology and its overall characteristics prior to the analysis of the applicability of this EU Framework.

Most of the previously mentioned research conclude that the characteristics of the illicit drug trade require a new approach. The two forms of illicit drug trade are indeed different from each other, however, do the characteristics of the illicit drug trade on the dark net indeed affect the applicability of the EU Framework? An understanding of the consequences of these characteristics is necessary to determine whether a new or adjusted EU Framework is required. This thesis aims to contribute to this understanding by analysing the consequences that follow the characteristics of the illicit drug trade on the dark net.

2.3. METHODOLOGY

Primary and secondary sources will be primarily analysed to provide an answer to the research question.

The primary sources will include legal documents of the European Union and the United Nations. Although the focus will be on European sources, it is important to conceptualize the trade in illicit drugs, hence the (minor) use of UN documents. Moreover, a few legal documents of the Court Case against Ross Ulbricht, the administrator of the most well-known cryptomarket, Silk Road, will be used to exemplify the concept of cryptomarkets.

Information about the required technologies and their principles are mainly stored online, for example in FAQs sections or developers guides on the websites of Tor and bitcoin. These sources will also be included in this thesis.
In addition, policy papers and reports from relevant European institutions will be analysed. Examples include the annual report of Europol and the background paper for the Directorate General Migration and Home Affairs. These documents provide me the discourse that exists in the European Union, both on traditional and online illicit drug trade.

The secondary literature used for this thesis will consist out of academic articles. These articles are especially valuable to the extent that they help me identify the most important characteristics of the illicit drug trade on the dark net that should be considered in this thesis.

The analysis will consist out of a combination of legal research and a form of content analysis. As a result, this thesis has characteristics of a policy paper to the extent that it pinpoints the issues related to this field that might need a different approach. The legal research in combination with a 'light' form of content analysis serves to allow both a theoretical as a practical approach to the analysis.

As the illicit drug trade on the dark net encompasses multiple distinct characteristics that could potentially affect the applicability of the EU Framework, it won't be feasible to include all these characteristics in the analysis. Therefore, only three characteristics will be included in the analysis, namely the lack of borders, its dependency on conventional postal services and the level of anonymity. These characteristics are identified by previous studies. It will be determined whether these thee characteristics constitute problems for the application of the EU Framework. It does so by first describing which legal domain is particularly related to that characteristic before the objective(s) of the EU Framework which could be consequently affected, are identified.

Regarding the EU Framework, many actors are involved, including the Member States, EU bodies (e.g. the European Commission) and EU specialized agencies (e.g. Europol). This thesis mainly addresses the specialized EU agencies as these are, arguably, most experienced in this field and their reports can offer essential information on this topic (level of transparency).

2.4. THEORETICAL FRAMEWORK

The notion that illicit drug trade on the dark net can be countered is part of the general notion of internet governance. There are two distinct theories that are especially relevant in this regard, cyberidealism and cyberrealism. These two theories have a fundamentally different approach to the governance of the cyberspace, which will be presented in this chapter. Their differences will be demonstrated with their perception on three issues, identified by Goldsmith, concerning the internet: the classification of cyberspace, the borderless nature of cyberspace and the notion of optimism (Goldsmith, 1998, p 1119 & 1112 & 1127).

The internet can be considered or classified as either a separate 'place' ('cyberspace') or as a tool for communication (a 'means' or 'tool'). A cyberidealist approach corresponds to the former perception, where the cyberrealism school of thought corresponds to the latter (Oster, 2017, p 208). Those who hold a cyberidealist point of view would regard cyberspace as a world on its own, separated from the offline world. The 'Declaration of the Independence of Cyberspace by John Perry Barlow in 1996 is in line with the cyberidealist notion of cyberspace. This Declaration was addressed to governments, which he refers to as "*governments of the Industrial World*". With statements such as "*we are creating a world [..]"* or *"[..] the global social space we are building[..]"*, the dissociation (though one-sided) from the 'normal' or offline world becomes clear (Barlow, 1996). Cyberrealists on the other hand, would disagree. According to this school of thought, cyberspace is not separated from the offline world and it merely considers it as a communication tool. Moreover, those who use the internet are in fact physically present in the offline world and consequentially, their actions, though executed on the internet, have the potential to create 'real-world effects' (Oster, 2017, p 208). As a result, the users of the internet are *"[..] no more removed than telephone users, postal users or carrier-pigeon users*" (Goldsmith, 1998, p 1121).

Another important aspect of the internet or cyberspace is that it is transnational - it is not confined to the legal sovereign territories that currently exist. Consequentially, cyberidealists would argue that the internet may not be governed by any existing governments, nor would cyberspace fall within their jurisdiction. It therefore considers any governmental attempt to regulate the internet illegitimate and secondly, it considers it unfeasible (Oster, 2017, p 207). In contrast, someone with a cyberrealist point of view would argue otherwise and argue that governments could regulate the internet as their laws apply to the users of the internet that are

physically located in the offline world (Oster, 2017, p 208). In other words, governments could still apply their laws and rules on the citizens located in their territory, regardless of whether the content or goods are *"[..]beyond the state's physical control"* (Goldsmith, 1998, p 1123).

Finally, a third issue with regards to the internet concerns the notion of optimism. Barlow has stated in his 'Declaration' that "*where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract*" (Barlow, 1996). This translates to an assumption of self-organisation of cyberspace. Though, a cyberrealist approach would consider this as a rather optimistic point of view. According to them, self-organization on the internet would not occur (Radin & Wagner, 1998, p 1296-1297).

In short, there is a clear distinction between the two schools of thoughts. A Cyberidealist perspective on the one hand, would consider cyberspace (or wish to see cyberspace) as a separate place, without legitimate rules imposed by governments and where instead community will decide what is good or bad. Cyberrealists on the other hand, would argue that cyberspace is not a location, but rather a means of communication. They would consequentially argue that the existing rules and jurisdictions would apply and that this generates order and justice.

This thesis applies the theory of cyberrealism and considers the internet as a means of communication. Consequently, this thesis considers the dark net as a new tool for the trade in illicit drug rather than a new field of crime. More importantly, the existing International and European legislation will be applied on the illicit drug trade on the dark net.

2.5. OUTLINE THESIS

Chapter 3 will address the traditional (or offline) illicit drug trade. In this chapter, both the International Legal Framework and the European Legal Framework on illicit drug trade will be provided before an overview of the current situation of illicit drug use in the European Union is provided. Moreover, chapter 3 addresses the reasoning behind the European Framework and presents an overview of its objectives and its actors.

Chapter 4 will focus on the illicit drug trade on the dark net. It first provides information about the dark net in general such as its characteristics and the technology that is required in order access and utilize it: privacy enhancing technology and cryptocurrency. Two examples will be discussed in detail (Tor software and bitcoin) as these serve as the most famous and most-used examples of these required technologies. Chapter 4 then continues with providing information

about cryptomarkets before addressing the most well-known example of Silk Road and its aftermath.

The application of the EU Framework will then be analysed in chapter 5. For each of the three characteristics, the main legal domain will be discussed prior to the consequences this would have for the implementation of the EU Framework.

Based on these findings, chapter 6 will answer the research question.

CHAPTER 3 TRADITIONAL ILLICIT DRUG TRADE

3.1 LEGAL FRAMEWORK

3.1.1. INTERNATIONAL LEGAL FRAMEWORK

The International Legal Framework merely consists out of three complementary and mutually supportive United Nations Treaties: The 1961 Single Convention on Narcotic Drugs, as amended by the 1972 Protocol, the 1971 Convention on Psychotropic Substances and the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (UNODC, 2017).

There is, however, an interesting difference between the three Conventions. The first two Conventions mainly deal with control measures that should be in place to ensure that narcotic drugs and psychotropic substances are limited to the use for medical and scientific purposes (UNODC, 2017; 1961 Convention, paragraph 9 preamble). It can be stated that the 1961 Convention applies a health-focussed approach, where *"[..]adequate provisions must be made to ensure the availability of narcotic drugs for [..]"* medical and scientific purposes and that "*[..]addiction to narcotic drugs constitutes a serious evil for the individual [..]"(*1961 Convention, paragraph 3-4, preamble).

In contrast, the 1988 Convention focusses predominantly on the illicit drug trade and the related criminal activities (UNODC, 2017; 1988 Convention, article 2). For example, the preamble of the 1988 Convention states that Parties are "*aware that illicit traffic generates large financial profits and wealth enabling transnational criminal organizations to penetrate, contaminate and corrupt the structures of government, legitimate commercial and financial business, and society at all its levels"* (1988 Convention, paragraph 6 preamble). In other words, the focus has shifted from a health perspective to an organized crime perspective.

Regarding the regulations, the 1961 Convention categorizes drugs in four groups (called schedules), each with a different level of control (1961 Convention, article 2). Additional provisions are laid down on limiting the cultivation, manufacture and trade of these substances conducted by States (1961 Convention, articles 21-32). In addition, article 12 of the 1988 Convention also includes measures to prevent diversion of the substances that are used in the manufacturing of narcotic drugs (so-called precursors). In addition, article 3 (1) (i) of the 1988 Convention lays down the criminal offences, which include, but are not limited to "*The production, manufacture, extraction; preparation, offering, offering for sale, distribution, sale,*

delivery on any terms whatsoever, brokerage, dispatch, dispatch in transit, transport, importation or exportation of any narcotic drug or any psychotropic substance contrary to the provisions of the 1961 Convention, the 1961 Convention as amended or the 1971 Convention". Moreover, article 3 (1) (v) of the 1988 Convention clarifies that the "*organization, management or financing of any of the offences* (..) is deemed as an offence.

3.1.2. European Legal Framework

Even though the three Conventions of the United Nations serve as the basis for EU Law on illicit drug trafficking, additional European Law exist. The Treaty on the Functioning of the European Union (hereinafter TFEU) sets out two classes of crimes on which harmonization measures may occur and these are listed in article 83 TFEU (Chalmers et al., 2014, p 655). The first class concerns serious offenses with a transnational dimension and includes illicit drug trafficking (TFEU, Article 83 (1)). In addition to this primary Law, secondary legislation exists for so-called Euro-crimes: "*Fraud and counterfeiting, money laundering, human trafficking, terrorism, corruption in the private sector, drug trafficking, sexual exploitation of children, cybercrime, organized crime and racism and xenophobia*" (Chalmers et al., 2014; p 657).

The same classification scheme as in the UN Conventions apply and Framework Decision 2004/757/JHA lays down the minimum provisions on the criminal acts and penalties of illicit drug trafficking. The same actions as mentioned in article 3 (1) (i) of the 1988 Convention are punishable (2004/757/JHA, article 2 (1) (a)).

The rules regarding precursors as laid down in the 1988 Convention are implemented by the EU. Regulations 273/2004/EC (amended by 1258/2013/EC) and 111/2005/EC (amended by 1259/2013/EC), accompanied with Implementing Regulation 2015/1011/EU (which deals with the rules for implementation) respectively deal with the intra-EU trade and trade with third countries in precursors. These Regulations focus on the required documentation that is needed to trade in these precursors, whether intra-EU or with third countries. This way, *"[..] diversion of such substances [..]"* is prevented (111/2005/EC, article 1).

It is worth addressing the gravity that is being given in cases concerning drug related crimes or drug trafficking by the Court of Justice of the European Union (CJEU). In, for example, Land *Baden-Württemberg v Panagiotis Tsakouridis (Case 149/09)* the Grand Chamber of the European Court of Justice ruled that *"[..] trafficking in narcotics as part of an organised group*

could reach a level of intensity that might directly threaten the calm and physical security of the population as a whole or a large part of it" (C-145/09, para 47). Moreover, it can even justify expulsion of a Union citizen under directive 2004/38 due to *"[..] the concept of 'imperative grounds of public security'"(*C-145/09, para 56). This clearly shows the seriousness of illicit drug trade and the gravity it has been given by the ECJ.

3.2. SHORT OVERVIEW OF THE SITUATION

Worldwide, there are 250 million people, between the age 15 and 64 years, who have used illicit drugs in 2014 according to the United Nations Office on Drugs and Crime (UNODC). This is equal to 1 in 20 adults, a prevalence that has remained rather stable in the past four years (UNODC, 2016, p 1). The three most widely used drugs are cannabis with an estimated 182,5 million users in 2014; opiates and opioids with around 33 million users in 2014; and amphetamines with approximately 19,4 million users in 2014 (UNODC, 2016, p 43 & 36 &52), The use of cocaine has increased over the years and it is estimated that there were around 18,3 million users in 2014 (UNODC, 2016, p 1 & 35).

In the European Union alone, approximately 88 million people between the age 15 and 64 years have used illicit drugs in the past (EMCDDA 2016, p 37). The top three of most widely used drugs in the EU are cannabis, cocaine and MDMA (which falls under the category amphetamines) with respectively 22,1 million users, 3.6 million users and 2,5 million users in 2015 (EMCDDA, 2016, p 13).
Interestingly, the market shares are slightly different. The three drugs with the highest market shares are cannabis (38%), heroin (28%) and cocaine (24%), of which heroin is responsible for a large, significant proportion of the health and social costs that are related to its use (EMCDDA & Europol, 2016, p 22 & 73).

Due to efforts of law enforcement, there have been 78 000 cocaine seizures in Europe in 2014 with a total of 61.6 tonnes and 32 000 heroin seizures which corresponds with a total of 8.9 tonnes (EMCDDA & Europol, 2016, p 98 & 76). Despite the high numbers, the tonnes seized corresponds to a very small amount of the estimated, worldwide, production. For example, in 2015 a total of 327 tonnes of heroin was produced and in 2014, approximately 746-943 tonnes of cocaine was produced (UNODC, 2016, p 26 &35)[4].

[4] Data on the world-wide production of cannabis and MDMA are currently unknown.

3.3. Objectives of the European Framework and its actors

As has become clear with the UN Treaties, there are two main issues related to the illicit drug trade.
First, there are significant health concerns which *"[..] generate costs for public health (on drug prevention and treatment, healthcare and hospital treatment)[..]"* (DG HOME, 2017).

Secondly, the trade in illicit drugs is associated with criminal activity in general. Out of all the criminal markets in the European Union, the illicit drug market is the largest market among them. It is estimated that the illicit drug market generates EUR 24 billion in profits a year. Moreover, approximately 35 % of the criminal groups in the European Union are active in the illicit drug market (Europol, 2017, p 34).
The illicit drug trade has "*[..]connections and impacts throughout the criminal sphere, the licit economy, government institutions and society more generally*" and can therefore not be treated in isolation (EMCDDA & Europol, 2016, p 27). Figure 1 shows the ramifications of the illicit drug trade. First, the illicit drug trade is associated with wider criminal activity, such as human trafficking and terrorism. Once engaged in criminal activities, criminals may be attracted to other forms of criminal behaviour as well, for example to increase their profits. Moreover, criminal networks and 'logistical infrastructure' may easily be utilised for other illicit activities or illicit traffic (EMCDDA & Europol, 2016, p 33).
Secondly, the illicit drug trade affects society as a whole due to for example environmental degradation and drug related violence. Neighbourhoods that are associated with the illicit drug trade might become no-go areas resulting in the degradation of that neighbourhood. As a result, non-users are also affected by the harms of the illicit drug trade (EMCDDA & Europol, 2016, p 39).

Thirdly, it affects the legal economy due to e.g. the related money laundering practices and the infiltration of financial flows originating from illicit practices. The illicit drug trade generates large amounts of money which result in direct and indirect consequences for the economy due to efforts to legitimize the large amounts of money and the impact of the losses of business (e.g. those in no-go areas) (EMCDD&Europol, 2016, p 28 & 32).
Fourth and finally, the illicit drug trade puts strains on governmental organizations, as the illicit drug trade is associated with an increase in governmental expenditure. (EMCDD&Europol, 2016, p 37).

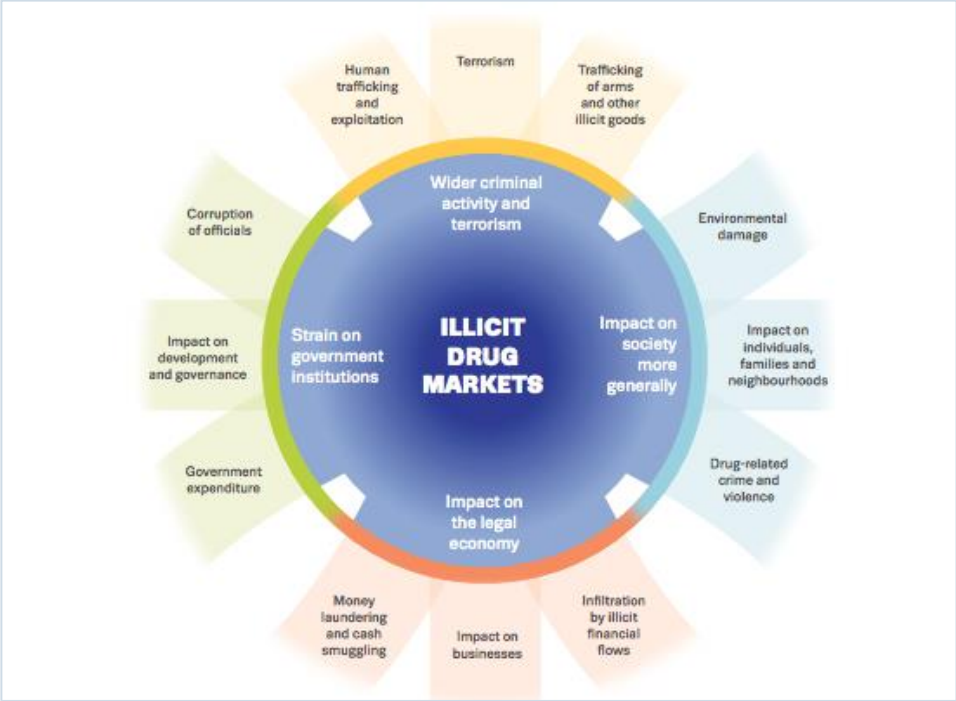

FIGURE 1 THE RAMIFICATIONS OF ILLICIT DRUG MARKETS. SOURCE: EMCDD & EUROPOL (2016)

To counter the above issues, the Council of the European Union (hereinafter the Council) adopted the EU Drugs Strategy for 2013-2020 in December 2012. This document states the priorities in this field and is accompanied by 4-year EU Drugs Action Plans (EU Drug Strategy, 2012, para 1).

The aim of this EU Drug Policy is to "*[..]contribute to a reduction in drug demand and drug supply within the EU, as well as a reduction as regards the health and social risks and harms caused by drugs [..]*" (EU Drug Strategy, 2012, para 6). To accomplish this, an "*[..]integrated, balanced and evidence-based approach*" is applied where national policies are being complemented and supported and a framework for "*[..]coordinated and join actions [..]*" is provided that also serves to guide "*[..]EU external cooperation in this field*" (EU Drug Strategy, 2012, para 6). The Strategy consists out of five objectives which include two policy fields (1) drug demand reduction and (2) drug supply reduction and three themes: (1) coordination (2) international cooperation and (3) research, information, monitoring and evaluation (EU Drug Strategy, 2012, para 11).

The Action Plans provide an overview of the specific actions together with its responsible bodies, assessment tools and a timetable (EU Drugs Strategy, 2012, para 11). Currently, the Action Plan for the period 2017-2020 is being prepared and will include the results of public

consultation (EC MHA, 2017). The Action Plan 2013-2016 lists 15 objectives (equally divided among the EU Strategy objectives) alongside 54 actions with their timetable, responsible parties and indicators (Action Plan, 2013).
The implementation of this Strategy is allocated to the Member States, existing EU bodies (e.g. the Council), EU agencies (e.g. Europol and EMCDDA) and bodies outside of the EU (e.g. UN and WHO) who are ought to use existing instruments within their mandate to ensure that the approach is complementary (EU Drug Strategy, 2012, para 15).

In December 2016, a mid-term assessment of the EU Drugs Strategy and Action Plan 2013-2016 was published which stated that eight of the 15 objectives of the Action Plan were either on target or completed, mostly in the regarding the objectives coordination and research, information, monitoring and evaluation. However, least progress has been made under the objectives drug demand reduction and international cooperation (EC, 2016, p 10). There are several EU bodies that are involved in the policymaking processes (e.g. European Council), legislative processes (e.g. European Commission) and policy implementation (e.g. Europol) (EMCDDA & Europol, 2016, p 157). Especially the latter includes specialised EU agencies that can be divided among three pillars: police cooperation, judicial cooperation and research. Each of them plays a significant role in the EU Drug Strategy and its Action Plan.

The most important agency within the field of police cooperation is Europol. As law-enforcement agency, Europol was formally established as an entity of the European Union in 2009 by Council Decision 2009/371/JHA (hereinafter ECD)[5]. Its (general) objective is *"[..]to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States*" by exchanging and analysing criminal intelligence (ECD, 2009, article 3; EMCDDA & Europol, 2016, p 158).
With regards to the illicit drug trade, Europol is frequently mentioned in the objective of drug supply reduction and international cooperation (Action Plan, 2013; p 6-10 & 18-19). To meet its objective, Europol provides "*[..]customised products and support services[..]*" which include expertise in the field of forensics, the dismantling of cultivation sites or synthetic drugs laboratories and participation in so-called Joint Investigation Teams (JITs) (EMCDDA & Europol, 2016, p 158).

[5] Prior to the ECD, it was established with the Treaty of the European Union in 1992

Europol works closely together with two other agencies within the field of police cooperation, CEPOL and FRONTEX. The former, the European Police College or CEPOL, provides training courses for national law enforcement officers. The latter, the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex) participates in joint operations to counteract cross-border crime such as illicit drug trafficking (EMCDDA & Europol, 2016, p 159).

Besides police cooperation, judicial cooperation plays a significant role in the European Strategy (EMCDDA & Europol, 2016, p 158). Eurojust was formally established in 2002 with Council Decision 2002/187/JHA (hereinafter CD). This Council Decision has been amended in 2003 (Council Decision 2003/659/JHA; predominantly focused on its budget) and 2008 (2009/426/JHA; predominantly focus on enhancing its capabilities and cooperation with third parties). Eurojust has competence over the same crimes for which Europol has competence over and its (general) objectives are to offer legal assistance and to improve and stimulate coordination and cooperation between the competent authorities of the Member States (CD, 2002, article 2).
With regards to the illicit drug trade, Eurojust is mainly involved in the objective of reducing the drug supply and in the field of international cooperation (Action Plan, 2012, pp 8). Eurojust aims to overcome possible conflicts of jurisdiction and aims for the most efficiently prosecution of the drug traffickers and their networks (Eurojust, 2016, p 1). In 2016 alone, Eurojust handled 253 drug trafficking cases (Eurojust, 2017, p 35). In addition, Eurojust is involved in Joint Investigation Teams (JITs) and is involved in the coordination of controlled deliveries (EMCDDA & Europol, 2016, p 158).

Finally, as the EU Strategy aims for an evidence-based approach, the pillar of research is crucial. The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) was formally established in 1993 by Council Decision 302/93 which was recast in 2006 (Regulation 1920/2006) after being amended several times.
EMCDDA predominantly focusses on research in the field of illicit drugs and its consequences. By collecting and analysing existing data, improving data-comparison methods and the dissemination of data, its objective is to provide *"[..] factual, objective, reliable and comparable information at European level concerning drugs and drug addiction and their consequences*" (EC 2006, 2006, article 1 & 2). In the Action Plan 2013-2016, EMCDDA is mainly involved in the objective of research and drug demand reduction. Predominantly it is

involved in monitoring the European situation and its related policy considerations (Action Plan, 2012, p 17-20).

CHAPTER 4 ILLICIT DRUG TRADE ON THE DARK NET

4.1. CHARACTERIZATION OF THE DARK NET

As has been stated in the introduction, the illicit drug trade on the dark net is rapidly evolving.

The Oxford Dictionary defines (under 'dark web') this part of the internet as follows: "*The part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable."* This definition successfully describes three characteristics of the dark net.

First, it acknowledges that the dark net is part of the world wide web and not a new or separate medium. Secondly, it stresses the importance of the special software that is required. Finally, it mentions the aim of its users, which is to be anonymous and untraceable.
As been stated in the introduction, the world wide web ('the internet') can be divided into the so-called 'surface web' and the 'deep web' (Barratt & Aldridge, 2016, p 2). The difference between these sections lies in how search engines, such as Google and Yahoo, can access their content with so-called crawlers (Bergman, 2001, p 1; Madhavan et al., 2008, p 1241). A crawler is a term for a program that automatically scans websites and follows the available links on those website to other websites (Google, 2017). This requires a website to be linked to other websites and secondly, that the content on these websites follows a fixed path. In other words, it should be a static website and not depending on the user, and the website should be part of the HTTP protocol (Bergman, 2001, p 1; Madhavan et al., 2008, p 1241). Content on the 'deep web' is not static; its content depends on user input by form submissions (Madhavan et al., 2008, p 1241). Examples include password secured governmental, medical or educational sites where the content depends on the user. With their study, Bin He et al., suggested that the 'deep web' is 500 times larger than the surface web (He et al., 2007, p 95). However, some content on the 'deep web' is intentionally hidden and is only accessible when special 'anonymizing software' is used (Barratt & Aldridge, 2016, p 2). This part of the 'deep web' is called the dark net.

This relates to the second characteristic the definition by the Oxford Dictionary provides: the need to use special software to access the dark net. The term that is used to describe this software is 'privacy enhancing technology' or PET (Huang & Bashir 2016, p 1 & Wang &

Kobsa 2008, p 2). In chapter 4.2. I will elaborate on the characteristics of this kind of technology together with an example.
Because of the special technology that is used, information send through the internet is anonymized.

This relates to the third characteristic that was presented by the definition in the Oxford Dictionary: the aim or intention of its users. As Wang and Kobsa define it, "*anonymity of a user means that she cannot be identified nor tracked online"* (Wang et. al., 2008, p 15).

In addition to the three characteristics mentioned above, there is another crucial characteristic of the dark net: it won't exist without the commitment of its users. As Moore and Rid state, it is "*[..]a distinct network supporting cryptographically hidden sites"* (Moore & Rid 2016, p 15). This definition successfully underlines the fact that the dark net is in fact a network. In a normal situation, information that is sent over the internet goes from the sender to receiver. However, when using PET, information from the sender is redirected trough different points ('middle points') before it reaches the receiver. This way, the sender and receiver are never directly connected which makes it possible to browse unanimously (Huang & Bashir, 2016, p 1; The Tor Project Inc., 2017a). This is only possible when users are willing to serve as middle points. In other words, without the contribution of the individual users, anonymous browsing in the form that currently exist is not possible (The Tor Project Inc., 2017a; Huang et. al., 2016, p 2).
In short, the dark net exists within the current structures of the world wide web which can only be accessed with PET. It aims to offer anonymity and is made possible by the commitment of users.

4.2. Required software

4.2.1. Privacy Enhancing Technology

There are several PETs such as Freenet, Ip2 and WASTE but the most famous example is 'The Onion Router' or Tor (hereinafter Tor). Tor is the most widely used PET, both in popularity and scope (Moore & Rid, 2016, p 15; Huang & Bashir, 2016, p 1; Barrratt & Aldridge, 2016, p 2).
Initially, the concept of onion routing was invented by the United States' Naval Research Laboratory. It was described as "*[..] an infrastructure for private communication over a public network"* which would provide "*[..] anonymous connections that are strongly resistant to both*

eavesdropping and traffic analysis" (Reed et. al.,1998, p 482). The main goal of this technology was to prevent traffic analysis, the ability to obtain identifying information from a certain connection, and as a side-effect, eavesdropping could be prevented (Reed et. al., 1997, p 1).

These anonymous connections were used to provide online freedom of speech and more importantly, to obtain access to the internet in counties where (political) censorship was enforced (Moore & Rid, 2016, p 16; Chaabane et. al., 2010, p 167). By sending information through connected machines ('onion routers'), the sender and receiver are never directly connected. Moreover, the information itself is disarranged ('encrypted') as well, making interpretation of the information by outsiders strenuous (Reed et. al., 1997, p 483).

In 2004, the '*second generation onion router*', called Tor, was presented by a collaboration between the Naval Research Laboratory and the Free Haven Project (Dingledine et. al., 2004, p 1). Additional features were presented to improve the anonymity. Tor is currently an open source project and the software can be easily downloaded from the internet. It is currently under supervision of 'The Tor Project Inc.' though there is no "*[..] authority in control of the network*" (Abbott, 2010, p 1).

Principles

Once the software from the Tor Project Inc. ('the Tor browser) is downloaded, there are two services offered. First, it allows anonymous browsing (Abbott, 2010, p 1; Moore et. al., 2016, p 15-16). It is based on the principle of onion routing; information that is sent over the internet ('traffic') is wrapped in cells with a fixed size, making the information encrypted. The cells are sent through a network of 'onion routers' which are individually referred to as nodes or relays. Each relay can unwrap a part of the fixed-size cell ('decrypt') hence the analogy with an onion; it peels off a layer each time (Dingledine et. al., 2004, p 1; Abbott, 2010, p 3).

Traffic flows through a minimum of three relays (at least a guard, middle and exit relay) and the actual path is referred to as a circuit. Each relay only 'knows' from which relay the information came from (its predecessor) and to which relay it gives its information to (its successor). The circuit itself remains unknown for each relay (Huang & Bashir, 2016, p 1-2; Dingledine et. al., 2004, p 1). The relays are publically listed in the Tor directory, though there is one type of relay that is not, these are so-called bridge relays (Chaabane et. al., 2010, p 168). Bridge relays provide access to the circuit in situations where the relays that are listed in the Tor directory are blocked by internet providers or governments. Once set up, these bridge

relays function as a guard relay and they keep the access to the Tor circuit hidden (The Tor Project Inc., 2017b; Abbott, 2010, p 7; Chaabane et. al., 2010, p 168).

Secondly, the Tor browser allows hosting, meaning that it allows its users to host exchanges or in other words, "*[..] create and administer proxy servers[..]*" (Abbott, 2010, pp 1; Moore & Rid, 2016, p 15-16). These proxy servers are in fact the Tor relays or nodes. In other words, it gives its users the opportunity to function a relay. This refers to the notion of community. Without users functioning as relays, onion routing is impossible.

In addition to the two services, the Tor network enables hidden services ('rendezvous points'). The so-called 'rendezvous-points' serve as a *"[..] building block for location-hidden services [..]"* that makes it possible to build an untraceable server within the Tor network as it does not reveal its IP-address (Dingledine et. al., 2004, p 8; Moore & Rid, 2016, p 17-18). Other users can connect to this hidden server (after they are informed about its existence) with the use of a random relay which then serves as a 'rendezvous point'. At this 'rendezvous point', communication will take place where both the anonymity and privacy of its users is ensured as well of that of its server provider (Dingledine et. al., 2004, p 8-9; Moore & Rid, 2016, p 18; The Tor Project Inc., 2017c).

4.2.2. CRYPTOCURRENCY

To make anonymous transactions on these cryptomarkets, cryptocurrencies are used. The best-known cryptocurrency is the bitcoin (EMCDDA & Europol, 2016, p 48; Cox, 2016b, p 41).

In 2008, a person or group of persons presented under the pseudonym Satoshi Nakamoto the bitcoin," *[..]a peer-to-peer electronic currency system[..]*" wich is *"[..] partially anonymous[..]"* (Nakamoto, 2008; Grinberg, 2011, p 160; Reid & Harrigan, 2013, p 1; Böhme et al., 2015, p 213).

Electronic currency was not new at that time however, there was one problem, the issue of double-spending (Swan, 2015, p 2). The system was based on trust; both parties would have to trust that the other party had transferred the money and that that money was not already spent elsewhere. Bitcoin offered a solution for this. Instead of transactions based on trust, these transactions instead carried cryptographic proof in the form of digital signatures and a

publically available transaction history (Nakamoto, 2008, p 1; Reid & Harrigan, 2013, p 1-2; Böhme et al., 2015, p 219; Vigna & Casey, 2015, p 15).

Principles

The technology behind bitcoin is referred to as the Blockchain technology or the 'Distributed Ledger Technology' (ENISA, 2016, p 5). The principle of this technology is that all the information is stored in blocks which will form a string ('ledger') as the succeeding blocks are 'build' upon its predecessor (Vigna & Casey, 2015, p 129- 133; Swan, 2015, p 2). The Blockchain itself can be described as "*[..] a giant spreadsheet for registering all assets, and an accounting system for transacting them on a global scale that can include all forms of assets held by all parties worldwide*" (Swan, 2015, p xi). As a result, the Blockchain technology can be used for various occasions, from financial transactions to even sealing a marriage (Swan, 2015, p 10).

A bitcoin transaction can be described as an electronic coin transfer request from one address to another. A bitcoin address is a sequence of 26-35 alphanumeric characters, which can only be used once. That is the reason users hold several (automatically generated) bitcoin addresses. These addresses are known as the 'public key' (Vigna & Casey, 2015, p 125; Bitcoin Wiki, 2016a).

The sender 'signs' the request with his private key. This is referred to as the public-key encryption system and results in a pending transaction with information which consist out of the two public keys, the amount requested and the 'timestamp' (Nakamoto, 2008, p 2; Vigna & Casey, 2015, p 126). This information will be reduced to an alphanumeric (where the only letters that are being used are a-f) string of 64 characters, known as a 'hash'. All transactions that will supersede the transaction within a 10 minutes' timeframe will be combined with that 'hash' to generate a 'hash' for the block known as a 'block hash'. In other words, this is a 'hash' that captures/stores all the transactions within the 10 minutes' timeframe of that block (Bitcoin, 2017; Vigna & Casey, 2015, p 129; Böhme, 2015 p 217)

Multiple 'miners' are trying (often in groups, in so-called 'mining pools') to find this 'block hash' the fastest. Mining is described as "*[..]the process of making computer hardware do mathematical calculations for the Bitcoin network to confirm transactions[..]"* (Bitcoin, 2017b). In practise, Bitcoin mining has similarities with solving a puzzle or with bookkeeping (Vigna & Casey, 2015, p 128; Doguet, 2012, p 1127). Nakamoto was the first miner: he solved a mathematical calculation that 'released' 50 bitcoins as a reward. This 'block' that he created

is referred to as "*node number one*" or the "*Genesis Block*" (Vigna & Casey, 2015, p 44). Without 'miners', this system won't exist; in other words, the notion of community plays a very important role.

When consensus is reached (by the miners) on the correct 'block hash', a sequential 'block number' is assigned to that block. Then, other miners will perform a 'proof-of-work', meaning that they will test the legality of the proposed transaction of a specific block, preventing the occurrence of double-spending. Verification will be based on the history that is stored in the Blockchain. Once the legality is confirmed, the transactions will take place and the process will start again from the beginning (Nakamoto, 2008, p 2-3; Vigna et. al., 2015, p 131-132; Böhme, 2015, p 217; Bitcoin, 2017a).

The ledger, or the Blockchain, is publically available. All the transactions (including public keys and the amount of bitcoins involved) are publically listed (Nakamoto, 2008, p 2; Reid et.al., 2013, p 7). Even though this information is publically available, the bitcoin is perceived as relatively anonymous. The addresses (public keys) don't show personal information (unless the user publicize that the address is theirs) and information about the transaction itself (what is bought with it) is not attached to the information that is being 'hashed', hence not publically listed (Nakamoto, 2008, p 5; Vigna & Casey, 2015, p 126; Reid & Harrigan, 2013, p 15). However, as will be discussed later in this thesis, the traceability of the transaction-flow can potentially be used by law-enforcement agencies.

4.3 CRYPTOMARKETS

Approximately 3-5% of Tor traffic consists out of the use of hidden services and even though this service is 'neutral', the anonymity these hidden services provide make this technology alluring for criminals (Moore & Rid, 2016, p 16; Abbott, 2010, p 4; Everett, 2009; p 12). For example, a hidden server can host an online marketplace for the trade in illicit goods, such as drugs. These marketplaces are known as cryptomarkets (Zajácz, 2017, p 29; Phelps & Watt., 2014, pp 262; Aldridge & Décary-Hétu, 2016b, p 7-8). These markets make use of several strategies to enhance their users' anonymity. It combines PET (mainly Tor) to hide the IP addresses and to enable encrypted communication, with anonymous and decentralized cryptocurrencies, such as Bitcoin (EMCDDA, 2016, p 18; Broséus et al., 2016, p 7). Examples of such cryptomarkets that deal (or have dealt) with illicit drug trade include Agora and Evolution but the most famous is Silk Road (Broséus et. al., 2016, p 9; Aldridge & Décary-Hétu, 2016a, p 24-25).

In recent years, the illicit drug trade via cryptomarkets has increased, despite law enforcement efforts (Global Drug Survey, 2017; UNODC, 2016, p 24). Moreover, research found that between 2013 and 2016, the revenues doubled and the number of transactions have even tripled (Kruithof et al., 2016a, p 61). In January 2016, it was estimated that the total revenues of the illicit drug trade on cryptomarkets were between EUR 10.5 million and EUR 18.5 million (Kruithof et al., 2016a, p 61). The revenue per capita is the highest in the Netherlands namely EUR 1 million in January 2016 (Kruithof et al., 2016a, p 41 &74). Figure 2 shows the estimated monthly revenue by drug type.

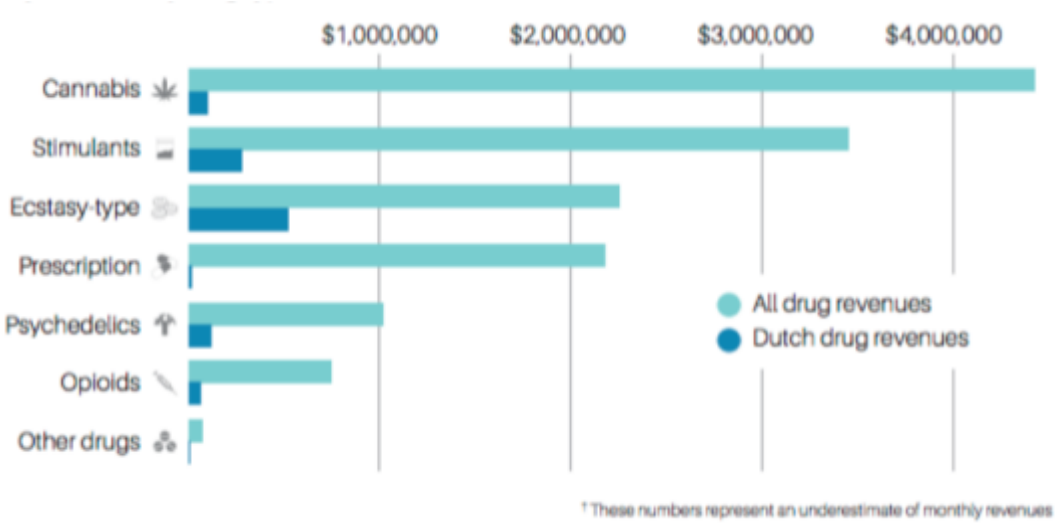

FIGURE 2 MONTHLY REVENUES BY DRUG TYPE. SOURCE: KRUITHOF ET AL. (2016B)

This figure also shows the range of drugs that is available on cryptomarkets which is often perceived as a wider range than would be available offline (Barratt et al., 2014, p 778; Aldridge & Décary-Hétu, 2016, p 26). Studies showed that, as a result, 30% of those who purchased drugs on cryptomarkets, also used a wider array of drugs compared to when they bought the illicit drugs offline (UNODC, 2016, p 25). In addition, research found that the drugs purchased on the dark net are generally considered to be of better quality (Barratt et. al., 2014, p 778; Aldridge & Décary-Hétu, 2016, p 27; UNOCD, 2016, p 25).

Cryptomarkets are often referred to as an *"eBay for drugs"*, partly because the ease of purchasing (Zajacz, 2017, p 23; Phelps et. al., 2015, p 263). However, in addition to the consumer-to-consumer and the business-to-consumer transactions (like eBay), research suggested that wholesale, meaning business-to-business, accounts for a significant share in

revenue terms for cryptomarkets (Kruithof et al., 2016, p 45; Aldridge & Décary-Hétu, 2016a, p 27).
The reasons for its popularity include the above mentioned perceived quality of the drugs and and wide range of drugs that is available. However, there are more characteristics at hand and this thesis will focus on three in particular.

First, the illicit drug trade on the dark net is not limited by borders. As a result, these drug markets become 'open' markets rather than 'closed' as more people, even those without any connection to the vendor can obtain access (Aldridge & Décary-Hétu, 2016a, p 23). Moreover, rather than being restricted to the local market, vendors on these cryptomarkets are given the opportunity to reach customers globally (Kruithof et al., 2016, p 25; Mounteney et al., 2016b; p 13).

Secondly, and some might label this characteristic as an enabler of the former, the illicit drug market possesses a significant offline characteristic as the illicit drugs is shipped via conventional postal/parcel services (Kruithof et al., 2016, p 25; Aldridge & Askew, 2017, p 102). Vendors use several methods to limit the changes of being caught; examples include vacuum packaging and sending multiple smaller packages. Buyers on the other hand try to limit suspicion by frequently ordering online (also on regular online marketplaces) and bonding with the mailman (Tzanetakis et al., 2016, p 66-67; Aldridge & Askew, 2017, p 104-105). However, some vendors try to avoid custom searches and therefore limit cross-border shipping (Tzanetakis et al., 2016, p 66-67; Martin, 2014, p 359; Décary-Hétu et al., 2016, p 71). Nonetheless, postal deliveries are generally considered to be the bottleneck, both by EMCDDA and vendors (Mounteney et al., 2016a, p 130; Kruithof et al., 2016, p 26; Aldridge & Askew, 2017, p 104; Trautman, 2016, p 5).

Thirdly, and maybe the most important characteristic concerns the high level of anonymity these cryptomarkets offer to their vendors and customers. As a result, the perceived risk of being caught by law enforcement agencies is small. In addition, buyers identify the decreased risk of drug-related violence as a benefit what contributes to their motive to use this medium (UNODC, 2016, p 25; Mounteney et al., 2016b, p 13; Kruithof et al., 2016a, p 84). The notion of trustworthiness is key in these cases and this is embodied in the significant role feedback systems play on cryptomarkets. These feedback systems function as 'quality control' and

increases trust as a result (Décary-Hétu et al., 2016, p 71; Phelps & Watt, 2014, p 267; Cox, 2016a, p 53).

4.4. EXAMPLE: SILK ROAD AND ITS AFTERMATH

As stated before, the most famous cryptomarket is Silk Road. Silk Road functioned from January 2011 to October 2013 and was created by 'Dread Pirate Roberts' - a pseudonym that represents a person (or group of people) (Phelps & Watt, 2014, p 262).

65% of the listings on Silk Road were related to the illicit drug trade which corresponds with around 13 000 listings for controlled substances, including opioids, precursors and stimulants (Phelps & Watt, 2014, p 265; Complaint, 2013, para 19a). Other listings included 'services' mostly concerning computer-hacking; 'digital goods' such as pirated media content; and 'forgeries', predominantly fake identity documents (Complaint, 2013, para 19).

Once a Silk Road account was set up, users could place items in their 'shopping card' and purchase the goods. The amount of bitcoins required for the purchase were transferred to a so called 'escrow system', where the administrators of Silk Road functioned as a middle-man. The escrow system was aimed to offer its users a form of trust; only when the order was delivered, the amount of bitcoins placed in the escrow system was transferred to the vendor. A commission was held back by the Silk Road administrators, usually between 8-15% (Phelps & Watt, 2014, p 263 & 266; Aldridge & Askew, 2017, p 106; Complaint, 2013, para 22; Kruithof et al., 2016a, p 23; Mounteny et al., 2016b, p 15).

During the FBI investigation on Silk Road from November 2011 onwards, over 100 undercover purchases were made (Complaint, 2013, para 20). The person behind DPR and believed founder of Silk Road, Ross William Ulbricht, was eventually arrested and Silk Road was taken offline by the FBI. Soon after, other cryptomarkets emerged, including Silk Road 2.0 (Décary-Hétu & Giommoni, 2016, p 58; Aldridge & Décary-Hétu, 2016a, p 24). Ross Ulbricht was found guilty on all charges including 'distribution/aiding and abetting the distribution of narcotics'; 'distribution/aiding and abetting the distribution of narcotics by means of the internet';'conspiracy to distribute narcotics; and 'continuing criminal enterprise' and will serve the rest of his life in prison (Judgement, 2015,p 94, para 16-24).

On 5 November 2014, 'Operation Onymous' was launched, which led to the seizure of several cryptomarkets (including Silk Road 2), a confiscation of USD 1.3 million worth in bitcoins and the arrest of 17 people, including 'B.B/ Defcon' who was the operator of Silk Road 2.0 (UNODC, n.d.; Décary-Hétu & Giommoni, 2016, p 58-59).
Operation Onymous was an international law-enforcement cooperation consisting out of law-enforcement agencies from 17 countries (mostly EU) and "[..] *coordinated by Europol's European Cybercrime Centre (EC3), Eurojust, the FBI, and the U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI)."* (UNODC, n.d.; Décary-Hétu & Giommoni, 2016, p 58; Europol, 2014).

In addition to the actors within in the 'traditional' European Framework, the European Cybercrime Centre (EC3) plays a significant role in tackling the illicit drug trade on the dark net. The goal to establish the EC3 was included in 'the EU Internal Security Strategy in Action: Five steps towards a more secure Europe' (referred to as ISSA) from the European Commission. It was stated that *"[..]the cybercrime centre should become the focal point in Europe's fight against cybercrime*" (ISSA, 2010, p 9).

After the establishment was announced, the EC3 was eventually opened on 11 January 2013 at Europol in The Hague (EC, 2012, p 4; Europol, 2013). It exists "*[..] within existing structures [..]"* and therefore the legal basis is formed by the existing Europol framework (EC, 2012, p 6; EC3, 2014, p 6). In addition, EC3 focusses mainly on three domains: 'cybercrimes committed by organised crime groups'; 'cybercrimes which cause serious harm to their victims'; and 'cybercrimes affecting critical infrastructure and information systems in the Union'(EC, 2012, p 4; EC3, 2014, p 4).

CHAPTER 5: ANALYSIS

5.1. CLASSIFICATION & SCOPE

During the trial of Ross Ulbricht, the judge stated that "*there must be no doubt that you cannot run a massive criminal enterprise and, because it occurred over the internet, minimize the crime committed on that basis*" (Judgement, 2015, p 95, line 7-9). This statement underlines the important concept of the scope of law.

The current existing legal framework on the trade in illicit drugs (see chapter 3.1.) does not codify the drug trade on the dark net in specific nor the drug trade on the internet in general. The punishable actions that are associated with illicit drug trafficking, such as offering for sale and manufacturing are codified in both the Treaties of the UN and EU and the EU Regulation. However, the punishable actions are not limited by the means that are used to perform these actions. In other words, these actions, such as offering for sale, are not restricted to offline practises. Therefore, it remains under the scope of International and European Law.

A second statement made by the judge draws attention to another important point, namely the classification of this form of illicit drug trade: "*Count One charges narcotics trafficking. Count two charges narcotics trafficking over the internet. It is clear Count One is a lesser included offense of Count two and that's why it is vacated*" (Judgement, 2015, p 14, line 6-9). Based on this statement, the determination of the punishable act in the realm of Cybercrime is interesting.

According to the European Union, criminal acts *"[..]that are committed online by using electronic communications networks and information systems*" would constitute a cybercrime (MHA, 2017). However, illicit drug trade on cryptomarkets are not specifically codified in the European Convention on Cybercrime, adopted by the Council of Europe in 2001, nor in any of the additional protocols. The Convention on Cybercrime, also known as the Budapest Convention, pursues a shared criminal policy which can protect the community against cybercrime (ETS185, 2001, p 2).

Nonetheless, there are several typologies to conceptualize cybercrime. One example includes the dichotomy between 'computer-focussed' and 'computer-assisted' cybercrime (van Slobbe, 2016, p 77; Martin, 2014, p 353). This dichotomy is based on the capability of a crime to exist

without the internet. ‘Computer-focussed’ cybercrimes are completely dependent on the internet and would not exist without it, nor would these crimes be known without the internet. Examples of this include hacking or infecting computers with malware. On the other hand, there are ‘computer-assisted’ cybercrimes. These crimes exist without the internet though the means to commit these crimes are facilitated by new technologies, such as the internet. Crimes such as online fraud or theft would fall under this category. (Martin, 2014, p 353-354; Papakonstantinou, 2010, p 456-457; van Slobbe, 2016, p 77).

Applied to the illicit drug trade on the dark net, this dichotomy does not provide a univocal categorization. Some would argue that illicit drug trade on the dark net would fall under the broad sense of cybercrime, ‘computer-assisted’, as the illicit drug trade would also exist without the internet (e.g. van Slobbe, 2016, p 77). However, others would argue that the uniqueness of this form of illicit drug trade makes classification based on this dichotomy impossible. They would argue that a new concept would be appropriate as its dependency on technology/computers comes in different degrees; it is highly dependent on computer technology as it relies on privacy enhancing technology and cryptocurrency while it is also dependent on conventional postal services, a feature that does not necessarily depends on computer technology (Martin, 2014, p 353-356).

For this thesis, the broad sense of cybercrime is applied as it is believed that the internet functions as a means that facilitates the offline illicit drug trade. Without the internet, the illicit drug trade would still exist, though in the ‘traditional’ form. This fits the conceptualization of a ‘computer-assisted’ cybercrime.

In short, this form of illicit drug trade still falls under the scope of UN and EU legislation on illicit drug trade. Moreover, the Convention on Cybercrime applies as this thesis conceptualized the illicit drug trade on the dark net as a ‘computer-assisted’ cybercrime.

5.2. Characteristic 1: Lack of borders

5.2.1. Main legal domain: Jurisdiction

The absence of borders with an open and global market as a result, highlights the importance of jurisdiction in relation to these cryptomarkets.

There are five concepts of jurisdiction. First of all, there is territorial jurisdiction where jurisdiction is either exercised over acts that originate from ('subjective territoriality') or those that are completed within ('objective territoriality') its territory. Secondly, there is nationality-based jurisdiction which describes the jurisdiction that States can exercise over their nationals (regardless of their psychical location). Thirdly, with passive personality jurisdiction, jurisdiction can be exercised based on the nationality of the victims. Fourthly, protective jurisdiction could enable States to exercise jurisdiction over acts that target their state interest. Finally, with universal jurisdiction every state has the potential to exercise jurisdiction for crimes that are *"[..] widely condemned by the international community"* (Scharf, 2007, p 276; Oster, 2017, p 115; Cottim, 2010, p 2-7). The latter is perceived as the most controversial concept of jurisdiction (Scharf, 2007, p 276).

Jurisdiction in the Convention on Cybercrime is addressed in article 22, paragraph 1, where it is stated that States should adopt legislation that makes it possible for a State to either exercise nationality-based jurisdiction or territorial jurisdiction (Cybercime Convention, 2001, article 22; Cottim, 2010, p 8). Applying these concepts of jurisdiction to the dark net provides challenges as there are often multiple territories and nationalities involved. The often varying locations and nationalities of e.g. the vendors and/or the buyers and, less prominent due to Tor software, the location of the server/ internet service provider) make it difficult to determine where a crime exactly took place (Cottim, 2010,p 12; van Slobbe, 2016, p 79; Brenner & Schwerha IV, 2007; Menthe, 1997, p 93-97). In addition, difficulties with obtaining evidence in other jurisdictions can occur (Brown, 2015, p 58). Moreover, challenges can occur when the acts are not (or to a lesser extend) codified in national law in either of these states (Cottim, 2010, p 12; Mounteney et al., 2016b, p 13).

As been discussed in chapter 3, Eurojust plays a significant role in situations where jurisdiction is unclear or debated on. In these cases, Eurojust assists in determining jurisdiction after taking issues such as 'availability and admissibility of evidence', 'sentencing powers' and 'costs and resources' into account (Eurojust 2016, p 3-4).
Moreover, in the Cybercrime Convention itself, it is stated in article 22, paragraph 5, that a consultation shall take place when multiple States claim jurisdiction. However, this is not obligatory as it reads "*[..] where appropriate [..]"* (Cybercrime Convention, 2001, article 22). As a result, some argue that the rules concerning jurisdiction should change; either a mandatory consultation (Cottim, 2010, p 18) or primarily jurisdiction based on nationality (Menthe, 1997,

p 102) or some would even suggest a new interpretation based on a "*substantial connection*" for a State (Swantesson, 2015, p 74).

5.2.2. Consequences for applicability EU Framework

Strengthening judicial cooperation in cross-border drug related crimes is mentioned as an objective in the EU Drug Strategy and its Action Plan, especially in the domain drug supply reduction (Action Plan, 2013, p 8). The discourse, as described above, shows that this objective would also apply to the illicit drug trade on the dark net and the related conflicts of jurisdiction that can occur. In that sense, the illicit drug trade on the dark net does not generate a new problem that should be addressed in a new EU strategy or framework.

Even though the lack of borders could indeed result difficulties in claiming jurisdiction, this is not a new phenomenon; it is even one of the reasons Eurojust came into existence. It is inherent to cross-border crime and would therefore also apply to e.g. traditional illicit drug trafficking.

Therefore, I argue that the lack of borders and the related potential jurisdiction problems does not constitute a reason for a new EU framework.

5.3. Characteristic 2: Dependency on conventional postal services

5.3.1. Main legal domain: Controlled delivery

The main offline characteristic of the illicit drug trade on the dark net concerns the drug delivery by conventional postal services. This has been identified as a bottleneck (see chapter 4.3) and could therefore generate possibilities for law-enforcement agencies to perform 'controlled deliveries'.

As codified in the 1988 Convention, a controlled delivery concerns *"[..]the technique of allowing illicit or suspect consignments of narcotic drugs, psychotropic substances, substances {..} to pass out of, through or into the territory of one or more countries, with the knowledge and under the supervision of their competent authorities, with a view to identifying persons involved in the commission of offences established in accordance with article 3, paragraph 1 of the Convention"* (1988 Convention, Article 1(g)).

This investigation technique is frequently used in cross-border crimes and drug cases in particular (Eurojust, 2015a, p 19; EMCDDA, n.d.). A controlled delivery can either be within

the borders of a State ('internal controlled delivery') which would occur when customs detect the consignment or it can involve multiple countries ('external controlled delivery') when a package is being traced from beginning to end (Cutting, 1983). Aim of a controlled delivery is to gather intelligence what can be used as evidence against the persons involved and their network, which could eventually lead to drug supply reduction (Cutting, 1983; Eurojust 2017, p 35-36).

Secondary legislation on European level exists; there are three Conventions that pursue States to implement legislation in this field[6]. Only one of these, the Schengen Convention, addresses controlled deliveries for illicit drug trafficking in specific as it reads that States *"[..]in accordance with their constitutions and their national legal systems, to adopt measures to allow controlled deliveries to be made in the context of the illicit trafficking in narcotic drugs and psychotropic substances."* (Schengen Convention, Article 73 (1)).

However, rules and guidelines often depend on the country involved and differences between EU member states exist (EMCDDA, n.d; Eurojust, 2015b, p 13-25). Studies have showed that differences between States exist in for example the set pre-conditions (such as the need for a Mutual Legal Assistance request (MLA) which would provide information sharing between States); the distinguished competent authorities that should be contacted for authorization; or the safety margins of the controlled delivery (EMCDDA, n.d; Eurojust, 2015b, p 13-25; Tak, 2000, p 352).

5.3.2. Consequences for applicability EU Framework

Partly because of the differences between States, several obstacles that Member States encounter have been identified by Eurojust (Eurojust, 2015b, p 8). These obstacles are listed in figure 3.

[6] Other secondary Law that deals with controlled deliveries: (1) Article 22 of the Convention on Mutual Assistance and Cooperation between Customs Administrations /CMACCA; (2) Article 12 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union/CMACMMSEU. These do not mention illicit drugs in specific but only 'extraditable offenses' which can include drug trafficking.

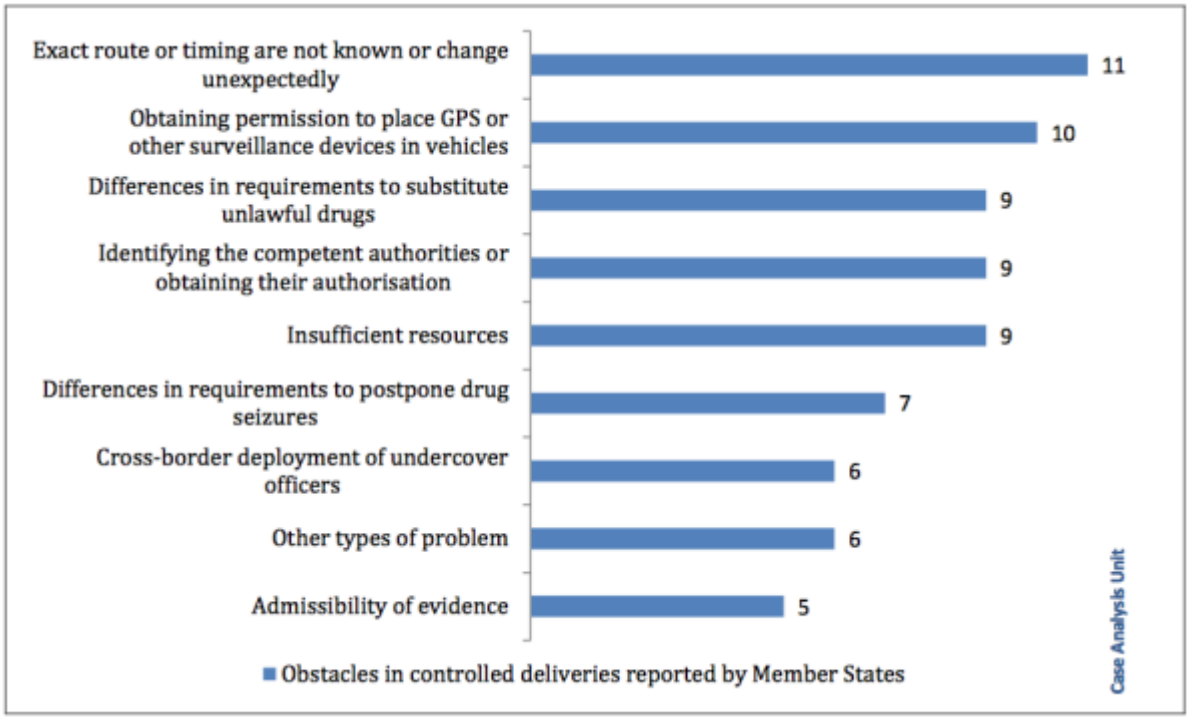

FIGURE 3 OBSTACLES IN CONTROLLED DELIVERIES. SOURCE: EUROJUST 2015B

The most reported obstacle concerned the difficulties in obtaining permission because the exact route, timing or drugs involved was unknown at the time of requesting a controlled delivery (Eurojust, 2015b, p 3). The admissibility of evidence was identified as a (small) obstacle as a result of adversarial legal systems (e.g. Ireland) (Eurojust, 2015b, p 7). Overall, the obstacles listed in figure 3 can be divided in legal and practical obstacles and show the need for cooperation and harmonization in this field.

However, these obstacles do not require a new framework as the EU strategy does not become unsuitable as a result. Enhancing cooperation and harmonizing efforts are included in the EU Drug Strategy and its Action Plan. For example, in the domain drug supply reduction, the improvement of cross border 'counter narcotic activities' and 'intelligence led' activities for law-enforcement agencies is included (Action Plan, 2013, p 6-7).

The same accounts for judicial harmonization (Action Plan, 2013, p 8). In this sense, the current European Framework already addresses the key-issues (cooperation & harmonization) related to this characteristic. Moreover, even though this is an important characteristic of the illicit drug trade on the dark net, the effects of this characteristic take place offline, what places this in the same line as any other cross-border crime. The fact that it started online does not generate new problems. As a conclusion, the effects of this characteristic do not urge for a new, specified, EU framework.

5.4. CHARACTERISTIC 3: LEVEL OF ANONYMITY

5.4.1. MAIN LEGAL DOMAIN: PRIVACY

The obtained anonymity through 'privacy enhancing software' and the use of cryptocurrencies is highly related to the field of privacy. Privacy is a highly-discussed topic, especially in relation to surveillance/security and often generates tension between citizens (privacy protection) and law-enforcement agencies (surveillance). Policy on e.g. encryption is therefore "*[..]becoming a crucial test of the values of liberal democracy in the twenty-first century"* (Moore & Rid, 2016, p 7).

The core document of the EU concerning privacy is the Data Protection Directive 95/46/EC (hereinafter DPD)[7] and aims to "*[..] protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.*" (DPD, 1995, article 1). Its legal basis is codified in both the TFEU (article 16) and the EU Charter of Fundamental Rights (Article 7 and 8).

The rules laid down in the DPD concerning the processing of personal data do not apply "*[..] in the course of an activity which falls outside the scope of Community law [..]"* or in cases that concern "*[..] public security, defence, State security {..} and the activities of the State in areas of criminal law [..]" (DPD, 1995, article 3.2).* In these situations, including illicit drug trafficking, Council Framework Decision 2008/977[8] (hereinafter CFD) applies which concerns the protection of personal data in police and judicial cooperation in criminal matters. This Directive strives to balance the "*[..] protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy [..]"* on one hand and *"[..]guaranteeing a high level of public safety [..]"* on the other hand (CFD, 2008, article 1). This Directive does not apply to Europol as Europol (among other agencies) is governed by acts which include data protection provision (CFD, 2008, recital, para 39).

[7] This Directive will be repealed on 28 May 2018 and replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the processing of Personal Data and on the Free Movement of such data which entered into force on 24 May 2016.

[8] This Council Framework Decision will be repealed on 6 May 2018 and replaced by Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data which entered into force on 5 May 2016.

Regarding Europol, the ECD included Europol-specific articles on data processing. Europol can "*[..] process information and intelligence, including personal data [..]"* when it is deemed *"[..]necessary for the achievement of its objectives[..]"* (ECD, 2009, article 10.1). As discussed in chapter 3.3., counter cross-border crime, such as illicit drug trafficking, is part of its objectives. In other words, to counter the illicit drug trade, Europol can process information including personal data.

One of the systems in place that are used to process such data are analysis work files (hereinafter AWF) which are used for criminal analysis (ECD, 2009, article 10.4 & 14; Europol, 2012, p 14-17). Additional rules for the processing of data for these AWFs are laid down in Council Decision 2009/936/JHA (hereinafter CDAWF).
Any information that relates to an 'identifiable natural person' should be considered as 'personal data' according to the CDAWF where an *'identifiable person'* refers to someone *"[..] who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (*CDAWF, 2009, article 1e). However, it is also stated that "*an individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time, cost and manpower"* (R(87), 1987, p2; Europol, 2012, p 13). This has been agreed upon by the Member States on the Council of Europe Convention 108 and only applies to personal data in the police sector.

Several categories of personal data may be processed in AWFs, where processing refers to *"[..] any operation or set of operations which is performed upon personal data[..]*" which include operations such as collecting, storing or adaptation (CDAWF, 2009, article 1e). A non-exhaustive list of categories is provided in the CDAWF which may be subject to processing and include 'personal details', 'economic and financial information', and 'behavioural information' (CDAWF, 2009, article 6). However, data that reveals someone's "*[..] racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and data concerning health or sex life [..]*" should be proven "*[..] strictly necessesary for the purposes of the analysis work file concerned*" (CDAWF, 2009, article 5.2).

Despite the rules that are laid down in the ECD and the CDAWF, ambiguity exist when applied to data related to the cryptomarkets. As discussed in chapter 4, both the IP addresses of the server and the users are hidden because of the Tor hidden service. Moreover, transactions are

performed with the partly-anonymous bitcoin. Whether these should be considered as personal data is ambiguous.

As been stated earlier, new legislation on Data Protection will apply from May 2018 which include provisions "*fit for the digital age*" (EC Justice, n.d.). Even though these do not concern the processing of personal data by EU bodies, such as Europol, it is worth to include their stance on this sort of data, especially since the existing provisions do not provide certainty.
According to recital 30 of Regulation 2016/679, it is stated that online identifiers, such as IP-addresses, "*[..] may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them".* In addition, article 3(1) of Directive 2016/680 includes online identifiers as 'personal data'.
This is in line with two judgements of the Court of Justice of the European Union (CJEU) [9] on, inter alia, the interpretation of 'personal data' under the Data Protection Directive. Nonetheless, these judgements show that regardless of the additional information that is necessary to identify someone by an IP-address, it is still required as personal data.
With the use of PETs, IP-addresses can, in principle, not be traced back to 'identifiable persons'. Nonetheless, it is not impossible, as the FBI proved with the seizure of Silk Road. As discussed in chapter 4, the Tor directory lists all the relays (except for bridge-relays). Due to this directory, the FBI could identify an IP-address that was not linked with any known relays (Tor directory) in the traffic data of Silk Road. This IP-address was assigned to an Icelandic server which appeared to host the Silk Road website and after identification led to the identification of several back-up servers (Tarbell Declaration, para 6-17; Zajácz, 2017, p 29). However, there are still doubts about the method that was being used by the FBI and some even claim that the FBI hacked the server (Arthur, 2013; Zajácz, 2017, p 29).
This shows that there are possibilities to obtain IP-addresses despite the use of Tor hidden services, which then could potentially be regarded as personal data. However, then the notion of "*[..]an unreasonable amount of time, cost and manpower[..]"* as described in

[9] In *Scarlet Extended SA v Société belge des auteurs, compositeurs et édieurs ECRL (SABAM), the CJEU ruled that* from the point of view of the ISP (Internet Service Providers), IP-addresses should be considered as personal data as *"[..] they allow those users to be precisely identified"* (C-70/10, para 51). In *Patrick Breyer v Bundesrepublic Deutschland, the CJEU ruled that a dynamic IP-address (one that is assigned with every new connection) should be considered as personal data as it has the potential to "[..]identify the data subject with additional data[..]" (C582/14, para 49).*

Recommendation (87) comes into play. Unfortunately, the determination of such is rather subjective. As a result, no incontestable determination can be made, based on the current legal sources.

Regarding the cryptocurrency, bitcoin, the same questions could potentially arise. As been stated above, bitcoins are regarded as a 'partly anonymous currency'. This anonymity is twofold: both the public keys (the addresses) and the transaction itself (what is bought with it) are considered anonymous. This corresponds with an 'address unlinkability' and 'transaction unlinkability' which respectively correlate to a 'user network' and a 'transaction network' (Androulaki et al., 2013, p 38; Reid & Harrigan, 2013, p 204).
Both the 'user network' and the 'transaction network' make it possible to identify its users especially since the Blockchain (and therefore all the transactions) are publically available.
There are various methods to recover identifiable information, especially concerning 'the user network' (Reid & Harrigan, 2013, p 212 – 222; Androulaki et al., 2013, p 40-43). Examples include the voluntary disclosure of one's public-key, which, if combined with other available information, could identify an individual or identification through the corresponding IP-addresses (Reid & Harrigan, 2013, p 213-214; Juhász et al., 2017, p 11).
In other words, bitcoin related data has the potential to identify individuals. Some therefore argue that it should fall under the scope of data protection (Fuster, 2016, p 198; Sorge, 2013, pp 8).
In addition, one could say that it should be included as 'economic and financial data'. Even though bitcoins are generally not perceived as a fiat currency since its value is not legally backed, a ruling from the CJEU indirectly confirmed that bitcoin is a currency within the EU, at least in the realm of value added tax (VAT) exemptions. In *Skatteverket v. David Hedqvist,* the CJEU exempted the exchange of bitcoins for 'traditional currencies' and vice versa from VAT as the bitcoin, according to the CJEU, "*[..] has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators"* (C-264/14, para 52) This placed the bitcoin in line with other VAT exemptions as mentioned in article 135 (1) (e) of the VAT Directive, which concerns *"[..] currency, bank notes and coins as legal tender[..]"* (C-264/14, para 52). As a result, data related to Bitcoins should arguably be considered as personal, financial, data.

Finally, as has become clear in previous chapters, international cooperation and intelligence (including personal data) exchange is crucial in the field of cross-border crimes, including illicit

drug trade. This is codified in the ECD. Within the EU, Europol may exchange data with several EU institutions/agencies, including Eurojust and EMCDDA when a working agreement is in effect or when the exchange is deemed *"[..] necessary for the legitimate performance [..]"* (ECD, 2009, article 22). Moreover, if the data was communicated to Europol by a Member State, Europol needs consent from the Member State involved prior to transmitting the data to a EU agency. If the data was obtained by Europol itself, transmission of that data should not be liable to obstruction or jeopardizing a Member State involved (ECD, 2009, article 24).
In addition to the transmission of data within the EU and its institutions, article 23 ECD provides for the necessities for the exchange of data with third parties. The exchange of personal data is only allowed where a so-called operational agreement between Europol and that party is in place (Europol, 2012, p 22; ECD, 2009, article 23). This operational agreement is based on the guarantee of an "*[..]adequate level of data protection ensured by that entity*" (ECD, 2009, article 23.6b).

5.4.2. Consequences for applicability EU Framework

The processing of data (not personal data alone) is included in the EU Strategy and its Action Plan, both in the field of drug supply reduction and in the field of information, research, monitoring and evaluation and involve both EU agencies and third countries (Action Plan, 2013, p 6 – 8 & 17-20).
The ambiguity of personal data in this field and therefore its processing by EU bodies such as Europol and Eurojust and the transmission to third parties could potentially result in problems.

The characteristic of encryption and the obtained level of anonymity with the illicit drug trade on the dark net could therefore constitute difficulties in the execution of the EU Strategy and its Action Plan. However, this does not necessarily ask for a different EU Strategy, but rather for a less ambiguous codification of 'personal data' under EU law in relation to the rules and standards for processing this data by EU agencies.
In other words, this characteristic affects the applicability of the EU Framework mainly because of another factor: the potential ambiguous codification of personal data in this field.

CHAPTER 6. CONCLUSION

Traditionally, the trade in illicit drugs took place offline. More recently, technological innovation that was intended to safeguard (online) anonymity in areas with governmental restrictions, was applied to the trade in illicit goods, including drugs. These so-called cryptomarkets exist on the dark net and depend on software such as 'privacy enhancing software' (e.g. Tor) and cryptocurrencies (bitcoin).
The most well-known example of a cryptomarket is Silk Road which was seized in 2013 by the FBI soon after which Operation Onymous took place which took down (among others) Silk Road 2. Regardless of these successes, policy documents by the European Union stress the need for action in this field. Therefore, this thesis aimed to answer the following research question:

To what extent can the current European framework against traditional illicit drugs be applied on the illicit drug trade on the dark net?

As the size of this thesis does not permit a full analysis of all the characteristics of the illicit drug trade on the dark net, this thesis focussed on three distinct characteristics of the illicit drug trade on the dark to answer this research question. For each of these characteristics, the main legal domain was identified before the objective(s) of the EU Framework that could consequently be affected by it were identified.

The first characteristic concerned the lack of borders which is highly related to the notion of jurisdiction. Even though this could result in difficulties in determining jurisdiction, this is not a new phenomenon, it is inherent to cross-border crime. In that sense, the illicit drug trade on the dark net does not generate a new problem for the execution of the current EU Framework.
The same conclusion can be drawn concerning the second characteristic, the dependency on conventional postal services. The same obstacles that are previously identified by Eurojust would apply and therefore this characteristic of the illicit drug trade on the dark net does not constitute a new problem concerning the EU Framework.
The level of anonymity could however negatively affect the application of the EU Framework. This characteristic is associated with the legal domain of privacy. Despite the use of privacy enhancing technology and the use of cryptocurrency, there is a possibility that IP-addresses or bitcoin transactions can be linked to an individual. This would then potentially be regarded as

‘personal data’. However, the ambiguity in this field could result in difficulties in the application of the EU Framework, most importantly in the field of intelligence sharing. However, this does not necessarily require a new EU Framework, as this could be solved by less ambiguous provisions on the processing of personal data by EU agencies such as Europol.

Overall, it can be concluded that the current European Framework could be applied to the illicit drug trade on the dark net, to the extent that it only applies this applicability is only analysed for three characteristics of the illicit trade on the dark net: its lack of border, its dependency on conventional postal services and the level of anonymity.

BIBLIOGRAPHY

(E-) Books

- Boekhout van Solinge, T. (2004). *Dealing with Drugs in Europe. An investigation of European Drug Control Experiences: France, the Netherlands and Sweden.* The Hague: BJU Legal Publishers.
- Chalmers, D., Davies G. & Monti, G. (2014). *Chapter 14: EU Criminal Law.* In: European Union Law. 3rd edition. Cambridge: United Kingdom.
- Fuster, G. G. (2016). *EU Data Protection and Future Payment Services.* In: Bitcoin and Mobile Payments. Palgrave Macmillan UK.
- Goldsmith, J., & Wu, T. (2006). *Who controls the Internet?: illusions of a borderless world*. Oxford University Press.
- Lessig, L. (2009). *Code: And other laws of cyberspace*. 2nd edition.
- Mueller, M. L. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. MIT press.
- Oster, J. (2017). *The Jurisdictional Question & Internet Governance and Regulation*. In: European and International Media Law. Cambridge: United Kingdom.
- Papakonstantinou, V. (2010). *Cyberspace And Cybercrime.* In: Handbook of Electronic Security and Digital Forensics. World Scientific Publishing Co. Pte. Ltd.
- Reid, F., & Harrigan, M. (2013). *An analysis of anonymity in the bitcoin system*. In: Security and privacy in social networks. Springer New York.
- Scharf, M. P. (2007). *Jurisdiction with Respect to Crime: Universal Jurisdiction and the Harvard Research.*
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.
- Vigna, P., & Casey, M. J. (2015). *The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order*. St. Martin's Press.
- Wang, Y. & Kobsa, A. (2009). Privacy-enhancing technologies. *Handbook of research on social and organizational liabilities in information security* (pp. 203-227). IGI Global.

Cases

- Case C-70/10. *Scarlet Extended SA v Société belge des auteurs, compositeurs et édieurs ECRL (SABAM).* Judgement of 24 November 2011.
- C-145/09. *Land Baden-Württemberg v Panagiotis Tsakouridis.* Judgement of 23 November 2009.

- C-264/14. *Skatteverket v. David Hedqvist.* Judgement of 22 October 2015.
- C-582/14. *Patrick Breyer v Bundesrepublic Deutschland.* Judgment of 9 October 2016.
- United States of America v. Ross William Ulbricht. Complaint of 27 September 2013. 13 Mag. 2328 (FM).
- United States of America v. Ross William Ulbricht. Declaration of Christopher Tarbell.
- United States of America v. Ross William Ulbricht. Judgement of 29 May 2015. S1 14 Cr. 68 (KBF) (S.D.N.Y., 2014).

Publications & articles

- Abbott, R. (2010). An onion a day keeps the NSA away. *J. Internet Law,* 13(11), 22-28.
- Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy, 41 (2017),* 101-109.
- Aldridge, J. & D. Décary-Hétu. (2016). Cryptomarkets and the future of illicit drug markets. *The Internet and drug markets, edited by EMCDDA*. Insights 21, pp 23-32. Publications of the European Union, Luxembourg. Referred to as Aldridge, J. & D. Décary-Hétu. (2016a)
- Aldridge, J. & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, 35 (2016), 7-15. Referred to as Aldridge, J. & D. Décary-Hétu. (2016b)
- Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in bitcoin. *International Conference on Financial Cryptography and Data Security* (pp. 34-51).
- Arthur, S. (2013). Silk Road: suspicions grow that server was hacked ahead of arrests. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2013/oct/08/silk-road-hack-suspicion-fbi-server on 26 March 2017.
- Bancroft, A., & Scott Reid, P. (2017). Challenging the techno-politics of anonymity: the case of cryptomarket users. *Information, Communication & Society, 20*(4), 497-512.

- Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets*(* but were afraid to ask). *International Journal of Drug Policy, 35*, 1-6.
- Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction*, 109 (5), 774-78.
- Bergman, M. K. (2001). White paper: the deep web: surfacing hidden value. *Journal of electronic publishing*, 7(1).
- Berman, P. S. (2000). Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to Private Regulation. *U. Colo. L. Rev.*, 71, 1263 – 1310.
- Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *The Journal of Economic Perspectives*, 29(2), 213-238.
- Brenner, S.W. & Schwerha IV, J.J. (2007). Cybercrime havens – Challenges and solutions. *Business Law Today* 17(2).
- Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., & Décary-Hétu, D. (2016). Studying illicit drug trafficking on Darknet markets: structure and organisation from a Canadian perspective. *Forensic science international*, 264, 7-14.
- Chaabane, A., Manils, P., & Kaafar, M. A. (2010). Digging into anonymous traffic: A deep analysis of the tor anonymizing network. *Network and System Security (NSS), 2010 4th International Conference on* (pp. 167-174).
- Cottim, A.A. (2010). Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article of the COE Convention on Cybercrime. *Law and Technology: Looking into the Future: Selected Essays*.
- Cox, J. (2016). Reputation is everything: the role of ratings, feedback and reviews in cryptomarkets. *The Internet and drug markets, edited by EMCDDA*. Insights 21, pp 49-54. Publications of the European Union, Luxembourg. Referred to as Cox (2016a).
- Cox, J. (2016). Staying in the shadows: the use of bitcoin and encryption in cryptomarkets. *The Internet and drug markets, edited by EMCDDA*. Insights 21,

pp 41-47. Publications of the European Union, Luxembourg. Referred to as Cox (2016b).

- Cutting, P.D. (1983). The technique of controlled delivery as a weapon in dealing with illicit traffic in narcotic drugs and psychotropic substances. *Bulletin on Narcotics* 35(4). Retrieved from: https://www.unodc.org/unodc/en/data-and-analysis/bulletin/bulletin_1983-01-01_4_page003.html on 20 April 2017.
- Décary-Hétu, D. & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitunal analysis of the effects of Operation Onymous. *Crime Law and Social Change* 67: 55-75.
- Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2016). Going international? Risk taking by cryptomarket drug vendors. *International Journal of Drug Policy*, *35*, 69-76.
- Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation onion router. *Naval Research Lab Washington DC.*
- Doguet, J. J. (2012). The Nature of the Form: Legal ad Regulatory Issues Surrounding the Bitcoin Digital Currency System. *La. L. Rev.*, *73*, 1119-1153.
- European Cybercrime Centre, EC3. (2014). First Year Report. *Europol.*
- Eurojust. (2017). Eurojust Annual Report 2016. The Hague.
- Eurojust. (2016). Guidelines for deciding 'which jurisdiction should prosecute'. Revised in 2016.
- Eurojust. (2015). Implementation Report of the Action Plan on Drug Trafficking. Strategic Project: Enhancing the work of EUROJUST in drug trafficking cases. The Hague. Referred to as Eurojust, 2015a.
- Eurojust. (2015). Issue in focus number 1 – First Addendum to the Implementation Report. The Hague. Referred to as Eurojust, 2015b.
- European Commision, prepared by EY and RAND Europe. (2016). Mid-Term Assessment of the EU Drugs Strategy 2013-2020 and Final Evaluation of the Action Plan on Drugs 2013-2015. *Publications of the European Union, Luxembourg.* Referred to as (EC, 2015).
- European Monitoring Centre for Drugs and Drug Addiction. (2016). European Drug Report 2016: Trends and Developments. *Publications of the European Union, Luxembourg.* Referred to as EMCDDA (2016)

- European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol. (2016). EU Drug Markets Report: In-Depth Analysis. *Publications of the European Union, Luxembourg.*
- European Union Agency for Network and Information Security (ENISA), 2016 "Distributed Ledger Technology & Cybersecurity.
- Europol. (2012). Data protection at Europol. *Publications of the European Union, Luxembourg.*
- Europol (2017). European Union Serious and Organised Crime Threat Assessment.
- Everett, C. (2009). Moving across to the dark side. *Network Security*, 2009(9), 10-12.
- Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New media & society*, 18(7), 1219-1235.
- Goldsmith, J. (1998). Regulation of the internet: Three persistent fallacies. *Chicago-Kent Law Review 73*, 1119.
- Grinberg, R. (2011). Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal.* 11/11/2011, p 159-208.
- He, B., Patel, M., Zhang, Z., & Chang, K. C. C. (2007). Accessing the deep web. *Communications of the ACM*, *50*(5), 94-101.
- Huang, H. Y., & Bashir, M. (2016). The onion router: Understanding a privacy enhancing technology community. *Proceedings of the Association for Information Science and Technology*, *53*(1), 1-10.
- Juhász, P. L., Stéger, J., Kondor, D., & Vattay, G. (2016). A Bayesian Approach to Identify Bitcoin Users. Retrieved from: https://arxiv.org/pdf/1612.06747.pdf 26 March 2017.
- Kruithof, K., Aldridge, J., Décary Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands. *Santa Monica, CA: RAND Corporation, 2016.* https://www.rand.org/pubs/research_reports/RR1607.html. Referred to as Kruithof et al. (2016a).
- Kruithof, K., Aldridge, J., Décary Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). The Role of the 'dark web' in the trade of illicit drugs. *Santa Monica, CA: RAND Corporation, 2016.*

https://www.rand.org/pubs/research_briefs/RB9925.html Referred to as Kruithof et al. (2016b).

- Lessig, L. (1998). Open code and open societies: values of internet governance. *Chi.-Kent L. Rev.*, 74, 1405 – 1420.
- Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication & Society*, 19(1), 111-126.
- Madhavan, J., Ko, D., Kot, Ł., Ganapathy, V., Rasmussen, A., & Halevy, A. (2008). Google's deep web crawl. *Proceedings of the VLDB Endowment*, 1(2), 1241-1252.
- Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice*, 14(3), 351-367.
- Menthe, D.C. (1998). Jurisdiction in Cyberspace: A theory of International Spaces. *Michigan Telecommunications and Technology Law Review.* 4(1) 69-103.
- Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, 58(1), 7-38.
- Mounteney, J., Griffiths, P. Vandam, L. (2016). What is the future for internet drug markets? In: *The Internet and drug markets, edited by EMCDDA*. Insights 21, pp 127-133. *Publications of the European Union, Luxembourg*. Referred to as Mounteney et al., 2016a.
- Mounteney, J., Oteo, A. & Griffiths, P. (2016). The internet and drug markets: shining a light on these complex and dynamic systems. In: *The Internet and drug markets, edited by EMCDDA*. Insights 21, pp 13-17. *Publications of the European Union, Luxembourg*. Referred to as Mounteney et al., 2016b.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
- Netanel, N. W. (2000). Cyberspace self-governance: A skeptical view from liberal democratic theory. *California Law Review*, 88(2), 395-498.
- Phelps, A., & Watt, A. (2014). I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation*, 11(4), 261-272.
- Radin, M. J., & Wagner, R. P. (1999). The myth of private ordering: rediscovering legal realism in cyberspace.

- Reed, M. G., Syverson, P. F. & Goldschlag, D. M., (1997). Anonymous connections and onion routing. *IEEE Journal on Selected areas in Communications*, 16(4), 482-494.
- Sassen, S. (2000). Digital Networks and the State Some Governance Questions. *Theory, Culture & Society*, 17(4), 19-33.
- Sorge, A. K. G. C. (2013). Practical Aspects of the Bitcoin System. Retrieved from: https://arxiv.org/pdf/1308.6760.pdf on 26 March 2017.
- Svantesson, D. J. B. (2015). A new jurisprudential framework for jurisdiction: Beyond the Harvard Draft. *American Journal of International Law*, 109, 69-74.
- Tak, P.J.P. (2000). Bottlenecks in International Police and Judicial Cooperations in the EU. *European Journal of Crime, Criminal Law and Criminal Justice* 8(4) 343-360.
- Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2016). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy*, 35, 58-68.
- United Nations Office on Drugs and Crime. (2016). World Drug Report 2016. United Nations, New York. E.16. XI.7.
- Van Slobbe, J. (2016). *The drug trade on the deep web: a law enforcement perspective.* In: *The Internet and drug markets,edited by EMCDDA*. Insights 21, pp 77-83. *Publications of the European Union, Luxembourg*.
- Zajácz, R. (2017). Silk Road: The market beyond the reach of the state. *The Information Society*, 33(1), 23-34.

Legislation, meeting reports & communications

- 2008/C OJ C115/47 Consolidated version of the Treaty on the Functioning of the European Union.
- Communication from the Commission to the Council and the European Parliament. COM(2012) 140 final. Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. Referred to as EC 2012.
- Communication from the Commission to the European Parliament and the Council. COM/2010/0673 final. The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Referred to as ISSA, 2010.

- Convention on Psychotropic Substances of 1971, United Nations, New York (Vol. 1019).
- ETS No.185 Convention on Cybercrime Budapest, 23.XI.2001.
- Meeting Report from the Internet and Drugs expert meeting of 7 & 8 June 2015
- OJ L 22/1. Council Regulation (EC) No 111/2005 of 22 December 2004 laying down rules for the monitoring of trade between the Community and third countries in drug precursors.
- OJ L 47/1. Regulation (EC) No 273/2004 of the European Parliament and of the Council of 11 February 2004 on drug precursors.
- OJ L 63/1. Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA). Referred to as (CD, 2002).
- OJ L 119/1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- OJ L 119/89. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
- OJ L 121/37. Council Decision of 6 April 2009 establishing the European Police Office (Europol). (2009/371/JHA). Referred to as (ECD, 2009).
- OJ L 138/14. Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime.
- OJ L 162/33. Commission Implementing Regulation (EU) 2015/1013 of 25 June 2015 laying down rules in respect of Regulation (EC) No 273/2004 of the European Parliament and of the Council on drug precursors and of Council Regulation (EC) No 111/2005 laying down rules for the monitoring of trade between the Union and third countries in drug precursors.

- OJ L 245/44. Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime.
- OJ L 283/31. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- OJ L. 325/14. Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files.
- OJ L 335/8. Council Framework Decision 2004/757/JHA of 25 October 2004 laying down minimum provisions on the constituent elements of criminal acts and penalties in the field of illicit drug trafficking.
- OJ L 350/60. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
- OJ L 330/30. Regulation (EU) No 1259/2013 of the European Parliament and of the Council of 20 November 2013 amending Council Regulation (EC) No 111/2005 laying down rules for the monitoring of trade between the Community and third countries in drug precursors.
- OJ L 330/21. Regulation (EU) No 1258/2013 of the European Parliament and of the Council of 20 November 2013 amending Regulation (EC) No 273/2004 on drug precursors.
- OJ C 351/1. EU Action Plan on Drugs 2013-2016.
- OJ L 376/1. Regulation (EC) No 1920/2006 of the European Parliament and of the Council of 12 December 2006 on the European Monitoring Centre for Drugs and Drug Addiction (recast). Referred to as EC 2006.
- OJ C 402/1. EU Drugs Strategy 2013-2020.
- Recommendation No. R (87) 15 of the Committee of Ministers to member states regulating the use of personal data in the police sector.
- Single Convention on Narcotic Drugs of 1961 as amended by the 1972 Protocol, United Nations, New York (Vol. 976).
- Trautman, F. (2016). Expert meeting on internet and drugs. Background Paper, European Commission DG Migration and Home Affairs of 7 June 2016.

- United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988, United Nations, New York (Vol. 1582).

Websites

- Barlow, J.P. (1996) "A Declaration of the Independence of Cyberspace". Retrieved from: https://www.eff.org/cyberspace-independence on 20 March 2017.
- Bitcoin Wiki (2016). *Address.* Retrieved from: https://en.bitcoin.it/wiki/Address on 1 June 2017.
- Bitcoin. (2017). *Developer Guide.* Retrieved from: https://bitcoin.org/en/developer-guide#block-chain on 31 March 2017. Referred to as Bitcoin (2017a).
- Bitcoin (2017). *Vocabulary.* Retrieved from https://bitcoin.org/en/vocabulary on 31 March 2017. Referred to as Bitcoin (2017b).
- EMCDDA (n.d.). *Legal aspects of controlled deliveries.* Retrieved from http://www.emcdda.europa.eu/html.cfm/index44352EN.html on 25 May 207.
- European Commission – Migration and Home Affairs (2017). *Cybercrime*. Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en on May 7 2017. Referred to as MHA (2017).
- European Commission – Migration and Home Affairs. (2017). *Drugs policy*. Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/drug-control_en on 21 March 2017 (Referred to as DG HOME).
- European Commission – Migration and Home Affairs (2017). *Public Consultations*. Retrieved from: https://ec.europa.eu/home-affairs/what-is-new/public-consultation/2016/consulting_0032_en on 6 June 2017 (Referred to as EC-MHA)
- Europol. (2013). Press Release: New European Cybercrime Centre (EC3) opens at Europol. Retrieved from: https://www.europol.europa.eu/newsroom/news/new-european-cybercrime-centre-ec3-opens-europol on 24 March 2017.
- Europol. (2014). Press Release: Global action against dark markets on tor network. Retrieved from: https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network on 3 April 2017.
- Global Drug Survey. 2017. Retrieved from: https://www.globaldrugsurvey.com/wp-content/themes/globaldrugsurvey/results/GDS2017_key-findings-report_final.pdf on 1 June 2017.

- Google. (2017). *Google crawlers*. Retrieved from: https://support.google.com/webmasters/answer/1061943?hl=en on March 31 2017.
- Human Rights Watch. (2017). Rethinking the war on drugs. Retrieved from: https://www.hrw.org/blog-feed/rethinking-war-drugs on 31 March 2017. Referred to as HWR (2017).
- ICANN, "What does ICANN do?" retrieved from: https://www.icann.org/resources/pages/what-2012-02-25-en on 19 March 2017
- Leiner, B.M., Cerf, V.G., Clark D.D., Kahn R.E., Kleinrock, L., Lynch, D.C., Postel, J., RobertsL.G. & Wolff. S. (1997). "Brief History of the Internet" retrieved from: www.isoc.org/internet/history/brief.shtml on 31 March 2017.
- Oxford Dictionary. (2017). *Dark web.* Retrieved from: https://en.oxforddictionaries.com/definition/dark_web on 15 March 2017.
- The Tor Project Inc. (2017). *Tor: Bridges.* Retrieved from: https://www.torproject.org/docs/bridges on 17 March 2017. Referred to as (The Tor Project Inc., 2017b).
- The Tor Project Inc. (2017). *Overview.* Retrieved from https://www.torproject.org/about/overview.html.en on 15 March 2017. Referred to as (The Tor Project Inc., 2017a).
- The Tor Project Inc. (2017). *Tor: Hidden Service Protocol.* Retrieved from: https://www.torproject.org/docs/hidden-services on 17 March 2017. Referred to as (The Tor Project Inc., 2017c).
- United Nations Office on Drugs and Crime. (2017). Legal Framework for Drug Trafficking. Retrieved from: https://www.unodc.org/unodc/en/drug-trafficking/legal-framework.html on 31 March 2017. Referred to as UNODC (2017).
- United Nations Office on Drugs and Crime. (n.d). *Operation Onymous*. Retrieved from https://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/xxx/operation_onymous.html on 3 April 2017.