



iPROCEEDS

Project on targeting crime proceeds on the Internet in
South-eastern Europe and Turkey

www.coe.int/cybercrime

Version 21 December 2017

Training Course for Judges and Prosecutors

Advanced Course on the Search, Seizure and Confiscation of Online Crime Proceeds

Self-Guided Training Manual

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

Contact:

Alexander Seger
Cybercrime Division
Directorate General of Human Rights and
Rule of Law
Council of Europe,
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int

Disclaimer:

This technical report does not necessarily reflect official positions of the Council of Europe or of the donor funding this project.

Table of Contents

1	Introduction	6
1.1	Aim of the Course	8
1.2	Target Student Group.....	8
1.3	Summary of Content	9
1.3.1	Online Investigative Challenges.....	9
1.3.2	Cross-border Investigations	9
1.3.3	Virtual Currencies.....	9
1.3.4	Practical Work/Case Studies.....	9
2	Online Investigative Challenges.....	10
2.1	Typologies and Money Laundering Online.....	10
2.1.1	Use of Internet Banking	10
2.1.2	Use of other Internet Financial Services	11
2.1.3	Use of Internet Communication Services	13
2.1.4	Bulletproof Hosting	15
2.1.5	Underground Economy	16
2.2	Identification of the Perpetrator	17
2.2.1	Network Address Translation (NAT)	17
2.2.2	Carrier Grade Network Address Translation (CGN)	19
2.2.3	The use of Anonymisers	20
2.2.4	Botnets/malware/remote control of a PC	23
2.2.5	The use of open, public or stolen WiFi	23
2.2.6	Identification of the Owner of an IP address.....	24
2.3	Engagement with ISPs.....	25
2.3.1	Type of data being requested	25
2.3.2	The EU Data retention Directive declared invalid by the decision of the CJEU	27
2.3.3	National ISPs	29
2.4	Multinational Service Providers	30
2.4.1	Jurisdiction	31
2.4.2	General position	31
2.4.3	Preservation requests	31
2.4.4	Emergency requests	32
2.4.5	Request scope.....	32
2.4.6	Notification of subject of request	32
3	Financial Investigations.....	34
3.1	Introduction	34
3.2	Financial Investigations and Online Crime Proceeds.....	34
3.2.1	Elements of Financial Investigation	35

3.2.2	Cybercrime Aspects of the Financial Investigation.....	35
3.2.3	Financial investigation in the European Union.....	36
4	Cross-border Cooperation	38
4.1	Summary.....	38
4.1.1	Relevant Networks and Organisations for Exchange of Information and for Mutual Legal Assistance.....	39
4.1.2	International Legal Instruments	40
4.1.3	Provisions on International Cooperation	42
4.2	Evaluations of the Application of Provisions on International Cooperation	45
4.2.1	Evaluation related to targeting crime proceeds.....	45
4.2.2	Evaluation related to cybercrime	47
4.3	Use of Templates and Forms for Mutual Legal Assistance	55
5	Virtual Currencies	57
5.1	Basic Course Recap	57
5.2	Introduction to Virtual Currencies	58
5.2.1	More Virtual Currency Terminology	58
5.2.2	Virtual Currency Participants.....	60
5.2.3	Bitcoin	60
5.3	Virtual Currency Risks	63
5.4	Investigative challenges	65
5.4.1	Knowing that Virtual Currencies have been used	65
5.4.2	Transaction Anonymity.....	65
5.4.3	Identification of Source of Funds	65
5.4.4	Cash out/realisation and conversion of proceeds	66
5.5	Freezing/seizing challenges.....	67
5.5.1	Virtual Currency as Proceeds of Crime.....	67
5.5.2	Identifying the Existence of Virtual Currency.....	67
5.5.3	Freezing/Taking Control of Virtual Currency	67
5.5.4	Asset Management	68
6	Practical Work/Case Studies.....	69
6.1	Literature Search	69
6.2	Case Study 1: Consideration of Legal Basis for Actions	69
6.3	Case Study 2: Consideration of FIU/Law Enforcement Interaction	72
6.4	Case Study 3: Consideration of Cybercrime/Money Laundering Interaction.....	75
7	Appendix: List of Relevant Reading.....	77
7.1	Council of Europe.....	77
7.2	European Union	78
7.3	United Nations.....	80
7.4	Financial Action Task Force	80

7.5	Jurisprudence	80
7.6	Other References	81

1 Introduction

The issues of cybercrime, electronic evidence, crime proceeds and money laundering cut across different institutions and involve, in particular, cybercrime units, financial investigation units, Financial Intelligence Units (FIUs) and prosecution services. However, cybercrime investigations are rarely accompanied by financial investigations and vice versa, investigations of financial or other crimes are rarely accompanied by cybercrime investigations. To this end there is a need for more effective inter-agency cooperation between all these institutions, which is expected to have the strongest impact on the search, seizure and confiscation of online crime proceeds.

Cybercrime and the criminal money flows on the Internet do not stop at geographical borders. Therefore, to address these phenomena in a comprehensive way, investigative activities should span across the borders and also operate within different jurisdictions. Effective international cooperation is also crucial for the search, seizure and confiscation of online crime proceeds. Linking up, tracing of proceeds of crime, anti-money laundering and countering terrorist financing measures with investigations on cybercrime and computer forensics offers added opportunities. For example, provisional measures to freeze assets should be accompanied by requests for the expedited preservation of electronic evidence.¹ This is one of the reasons that Recommendation 36 of the Financial Action Task Force proposes implementation of the Budapest Convention on Cybercrime and the Warsaw Convention of the Council of Europe.

As the use of and reliance on information technology becomes ever more pervasive in society, the targeting and exploitation of computer systems has also become increasingly common. Offences involving computers have grown rapidly both in number and in sophistication, but there has been a time lag in developing effective countermeasures. Bringing offenders to justice requires evidence of guilt beyond a reasonable doubt, but evidence derived from electronic devices is volatile, often intangible and probably in another jurisdiction. This means the importance of effective, legally compliant and robust procedures for the identification, collection and preservation of electronic evidence is vital. Criminal proceedings increasingly entail cybercrime or electronic evidence found on computer systems or storage devices. In a similar way this applies also to crime proceeds.

Given the reliance of societies worldwide on information and communication technologies, judges and prosecutors must be prepared to deal with cybercrime and electronic evidence. While in many countries, law enforcement authorities have been able to strengthen their capacities to investigate cybercrime and secure electronic evidence, there has been less focus on the requirements of judges and prosecutors. Experience suggests that in most cases, judges and prosecutors encounter difficulties in coping with the new realities of the cyber world. Particular efforts are therefore required to enable judges and prosecutors to prosecute and adjudicate cybercrime and make use of electronic evidence through training, networking and specialisation.

A concept to support such efforts has been developed by the Council of Europe under the Project on Cybercrime in cooperation with the Lisbon Network of judicial training institutions in cooperation with a multi-stakeholder working group in the course of 2009.

¹ See paragraph 317, Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction, of MONEYVAL Research Report, March 2012. Available at: [http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL\(2013\)6_Reptyp_flows_en.pdf](http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6_Reptyp_flows_en.pdf)

The purpose of the concept was to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors and to integrate such training in regular initial and in-service training.

The objectives of a training concept for judges and prosecutors are:

- To enable training institutes to deliver initial and in-service cybercrime training based on international standards
- To equip the largest possible number of future and practicing judges and prosecutors with basic knowledge on cybercrime and electronic evidence
- To provide advanced training to a critical number of judges and prosecutors
- To support the continued specialisation and technical training of judges and prosecutors
- To contribute to enhanced knowledge through networking among judges and prosecutors
- To facilitate access to different training initiatives and networks.

In this context, through the Joint Regional Project of the European Union and Council of Europe CyberCrime@IPA (Regional Cooperation in Criminal Justice: Strengthening capacities in the fight against cybercrime)² training materials on cybercrime and electronic evidence have been developed to be used by training institutions.

Considering the success and demonstrated value of the basic and advanced training for judges and prosecutors on cybercrime and electronic evidence, through the European Union and Council of Europe Joint Project iPROCEEDS³ a further two training modules: a basic and an advanced module on the investigation, search, seizure and confiscation of online crime proceeds were developed.

In general terms, the activities of criminals and criminal organisations are designed to generate profits. According to United Nations estimates, the total amount of criminal proceeds in 2009 was approximately USD2.1 trillion, or 3.6% of global GDP, but only a very small proportion of those funds was ever recovered⁴. Targeting proceeds of crime by conducting a financial investigation in parallel with the criminal investigation might also reveal evidence of the money laundering offence. Money laundering allows criminal organisations to benefit from their illegal activities and maintain their operations.

The financial impact of cybercrime and the size of related proceeds are hard to quantify in the absence of reliable data and research, but cases show that the proceeds from cybercrime are laundered through sophisticated schemes involving both traditional and new payment methods⁵. However, cybercrime investigations are rarely accompanied by financial investigations and vice versa, investigations of financial or other crimes are rarely accompanied by cybercrime investigations.

³ The European Union and Council of Europe Joint Project "Targeting crime proceeds on the internet in South Eastern Europe and Turkey" – iPROCEEDS aims at strengthening the capacity of authorities in the IPA region to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet. <http://www.coe.int/en/web/cybercrime/iproceeds>

⁴ Explanatory memorandum to the Proposal for an EU directive on countering money laundering by criminal law (22.12.2016). Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0826>

⁵ Criminal Money Flows on the Internet – methods, trends and multi-stakeholder counteraction, MONEYVAL Research Report, March 2012.

Organised crime groups hide and reinvest assets in states other than the one where the crime originating the property was committed. This makes it much more complicated for competent authorities to fight cross-border serious and organised crime. In the same vein, cybercrime and criminal money flows on the Internet do not stop at geographical borders. To address this phenomenon in a comprehensive way, investigative activities should span across the borders and also operate within different jurisdictions. Therefore, effective international cooperation is also crucial for the search, seizure and confiscation of online crime proceeds.

The concept of targeting online crime proceeds presented in this training course brings together the approaches of cybercrime, financial and money laundering investigations with the purpose of increased efficiency and success of criminal investigations and criminal proceedings from the perspectives of both prosecuting a criminal and targeting proceeds of crime.

1.1 Aim of the Course

This course is intended to facilitate the continued education of an interested judge or prosecutor, who has completed the basic course on investigation, search, seizure and confiscation of online crime proceeds and wishes to continue their education in this area. The aim is to enhance the knowledge of the interested judge or prosecutor with regards to the legal and technical landscape as they apply to online crime proceeds. This is achieved through a more detailed study of selected topics of interest in this area.

The course will cover in more detail selected topics in the following areas:

- The legal and technical challenges of investigations involving online criminal money flows.
- The practicalities of cross-border investigations.
- Criminal use of, and risks associated with, virtual currencies.

This is followed by practical work in the form of literature search and case studies for the student to consider.

1.2 Target Student Group

This course is designed for judges and prosecutors that have already completed a basic course on the search, seizure and confiscation of online crime proceeds. It is expected that the users of this manual will already have knowledge of:

- The meaning of cybercrime and the nature of a cybercrime investigation
- The nature of financial investigations
- The money laundering offence and the role of a Financial Intelligence Unit (FIU)
- Basic technical knowledge such as the nature of an IP address.
- Basic understanding of the particularities of electronic evidence.

All of these prerequisites can be met through completion of the Council of Europe's "Basic Course on the Search, Seizure and Confiscation of Online Crime Proceeds".

1.3 Summary of Content

1.3.1 Online Investigative Challenges

In the basic course, a number of online criminal money flows and money laundering typologies were introduced. The purpose of this section is to discuss in more detail some of the investigative challenges that can be experienced with a selection of the typologies described there. This includes discussion of the investigative challenges associated with identification of a perpetrator online, identification of the online crime proceeds, as well as the challenges associated with engagement with national, international and multinational Internet Service Providers (ISPs).

1.3.2 Cross-border Investigations

The concept of targeting online proceeds of crime brings together the approaches of cybercrime, financial and money laundering investigations with the purpose of increased efficiency and success of criminal investigations and criminal procedure from the perspectives of both prosecuting a criminal and targeting and confiscating proceeds of crime.

While mutual legal assistance is still considered as the principal means to enforce court orders and to gather evidence abroad, the length of the procedure represents an important obstacle. However, the use of joint investigations and joint investigation teams might address some of the challenges of efficiency. Law enforcement (police and prosecutors) cooperation and exchange of information is indispensable in cross border cases. Relevant networks play an important role in this respect.

For the purpose of this advanced course it is useful to highlight some of the recent findings on obstacles that have been identified by international organisations in application of international standards in domestic legislation and practice, as well as relevant recommendations that could be used as a source of inspiration.

1.3.3 Virtual Currencies

Following on from the basic terminology relating to virtual currencies that was discussed in the introductory course, this course elaborates further on the participants in the virtual currency ecosystem, including virtual currency exchanges, wallet services and so on. The operation of the Bitcoin virtual currency is described and this is followed by an explanation of the risks and challenges associated with investigations involving the use of virtual currencies as well as search, seizure and their asset management.

1.3.4 Practical Work/Case Studies

To assist students with mapping the information provided in this course into the context of their national legislation, a guided literature search and several case studies are provided to allow students to, in their own time, further investigate the issues raised here.

2 Online Investigative Challenges

2.1 Typologies and Money Laundering Online

In the basic course, a number of online criminal money flows and money laundering typologies were introduced. The purpose of this section is to discuss in more detail some of the investigative challenges that can be experienced with a selection of the typologies. There are two very large, and commonly encountered, issues that will be discussed separately in their own sections of this course; the investigative challenges associated with identification of a perpetrator online (see Section 2.2) and the myriad of challenges related to the use of virtual currencies (see Section 5).

2.1.1 Use of Internet Banking

Several of the typologies discussed in the basic course rely on a criminal having access to a bank account. In particular this relates to the typologies of wire transfers, bank account takeover and international transfers. The regulatory requirements on financial institutions in terms of customer due diligence, records keeping, etc. are well understood⁶. However, criminals rely on the non-face-to-face nature of the online banking environment to attempt to bypass these controls⁷. Without the need for direct customer contact, it is possible for a criminal, for example, to impersonate a legitimate banking customer (e.g. by stealing or using online banking credentials) in a way that is much more difficult for a financial institution to identify.

There are three main leads to be followed when investigating such cases:

- The way the bank account was compromised (e.g., phishing, malware infection). Evidence on that could be obtained from the owner of the account, which most probably is the victim.
- Login information regarding the compromised bank account. This information can be provided by the financial institution.
- Bank account(s) used to transfer the money from the compromised account. This information is in the possession of the financial institution and could help in the identification of the individuals (money mules) involved and in tracing the money for the final seizure.

In the remainder of this section, certain investigative issues that are made more complex through the use of online banking services will be discussed.

Firstly, it is more difficult to establish the nature of the relationship, if any, between the owner of the bank account and the suspect. For example:

1. Is the owner of the bank account aware of the activity of the suspect?
2. Does the suspect have direct control over the bank account or is the suspect directing the activities of the owner of the bank account?

⁶ International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, the Financial Action Task Force (FATF) Recommendations, 2012. Available at: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

⁷ FATF Report, Money Laundering Using New Payment Methods, October 2010. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>

3. Is it possible to identify the person who performed a particular transaction on the account?

With these questions and many others, it should be clear that the non-face-to-face nature of the online banking environment makes establishing the facts in an investigation more challenging.

Secondly, the use of online banking services also introduces some challenges with identification of the suspicious activity itself. In a branch, when a suspect presents themselves and attempts to perform a transaction, there is at least an opportunity for a teller to identify whether the activity being performed is obviously suspicious. In the online environment the processing of transactions is largely automated. Combined with the structuring of funds to avoid reporting limits, this can lead to an increased risk that suspicious transactions might be missed. To combat this, financial institutions often deploy automated transaction monitoring software, the function of which is to detect transactions that deviate from the profile of transactions commonly carried out on a particular account.

Some, but not all, fraud monitoring software will also check the IP address that a particular online banking account is allegedly logging in from. If, for example, the IP address is one that the account has never logged in from before, this can be used to raise the suspicion that the online banking account might have been compromised. However, from a practical point of view for financial institutions, there is a tricky balance to strike between detecting and preventing fraud on the one hand and not interfering with the legitimate banking activities of globally mobile customers on the other.

Further, even if a customer's online banking account has been compromised, it will not always be apparent from the IP address being used to log in. This is because in the case where the customer's PC has been infected with a malware, it is possible that the criminal will have control of a customer's PC. This will allow the criminal to perform a login on the customer's account that will be from the IP address of the customer's PC, thus preventing the triggering of an alert due to a login from an unusual IP address.

Thirdly, there is the issue of what additional evidence is required to demonstrate the activities of the suspect, and whether that evidence is available. The IP addresses from which a particular account logged in will most likely have been recorded by the financial institution, but not always in a readily accessible way. Significant effort may be required to identify which IP addresses were used for which logins by which accounts. This is due to the complexity of an online banking infrastructure and in particular due to the fact that logs may not be stored or correlated in a way that offers easy access to the required information. Additionally, if and when the IP address that has been used can be identified, associating the suspect with that IP address is a separate challenge.

2.1.2 Use of other Internet Financial Services

Other (non-banking) Internet financial services play a role in several of the typologies discussed in the basic course. In particular the use of Internet payment systems, purchases through the Internet and the use of online gambling/trading platforms. Once again, the non-face-to-face nature of the relationship between the service and the user of the service introduces the opportunity for criminals to exploit these types of services.

Eventually these services will need to have some form of interaction with the traditional financial services sector. This is most commonly through the use of payment cards, which are used to "charge up" an account with the Internet financial service provider. Once funds

have been transferred from a payment card to the service provider, the nature of the subsequent interactions between the user and the Internet financial service provider are opaque to the traditional financial system. Therefore, it is recommended that Internet payment services are subject to compliance obligations and oversight⁸. The nature of this regulation may vary from jurisdiction to jurisdiction.

Consider, for example, the concept of micropayments⁹. It would not make financial sense for an Internet payment service to immediately charge every micropayment to the credit card of the user because the payment card fees would erase any profit for the payment service in the transaction. Instead, the payment services typically aggregate a number of payments for a period of time and submit a single charge for all user activity within a particular time period. The payment service is therefore accepting some fraud risk but since the amounts of money involved in individual payments is typically very small, the overall losses tend also to be small.

A micropayment model is also sometimes offered by mobile phone operators. In these cases, the user makes micropayments using their phone or phone number and the charges are placed on the user's next mobile phone bill.

In these cases the most important for the investigator is to clarify the nature of the illegal activity (frauds, unauthorised access), types of data which can be gathered and from where in order to prove the criminal activity and to trace the money flow.

In the majority of the cases victims are alerted at a later stage about the frauds involving their bank accounts or credit cards. Nevertheless, the payment services providers are able to identify illegal activities and preserve the data, which can be later provided to the investigators.

The main challenges that arise through the use of Internet payment services relate to the fact that the required records typically reside in a different jurisdiction. The involvement of multinational service providers and the mutual legal assistance process can significantly slow down and increase the complexity of an investigation.

Similar problems arise with the use of platforms that facilitate purchasing through the Internet. As discussed in the basic course, purchasing goods or services through the Internet, which are then shipped to the criminal or to a mule, is a good way of converting stolen payment credentials into real-world value. In these cases, the investigation is completely reliant on the records keeping of the purchasing platform, and on their ability to identify suspicious activity. Once again, most investigations will find that most of the large online purchasing platforms are headquartered in another jurisdiction. Collecting evidence from these organisations will require a mutual legal assistance treaty request to be submitted to the jurisdiction in question.

Online gambling platforms also present some unique challenges that arise principally from the inconsistent regulation of these entities across the world. For example, in some jurisdictions online gambling is illegal so cooperation with the operator of an online gambling company in these cases may indicate recognition of the entities and can therefore present legal challenges. Within the EU, for example, 20 EU member states allow online gambling and seven do not. Some, by virtue of recent legislation, have decided to

⁸ FATF Report, Money Laundering Using New Payment Methods, October 2010. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>

⁹ <https://en.wikipedia.org/wiki/Micropayment>

allow or prohibit online gambling, while others allow or prohibit it “passively” by continuing to apply legislation established, often many years earlier, for conventional gambling. Of the twenty Member States that allow online gambling, thirteen operate a liberalized market, six operate state-owned monopolies and one has licensed a private monopoly¹⁰.

2.1.3 Use of Internet Communication Services

The Internet is ultimately a communication platform and criminals use the communication services to enable their activity. Within the context of criminal money flows on the Internet in particular, communication services on the Internet enable mule recruitment, communication and management. Services such as email, Internet relay chat, instant messaging and phone services that are available online can be used by criminals to organise their activities.

Technical difficulties can arise both with the identification of the parties to a communication and the identification of the substance of a communication. The issue of identification of suspects on the Internet is discussed in detail in Section 2.2.

The trend in recent years has been towards an increased focus amongst Internet services providers towards assurances of privacy for their users. This has manifested in many cases as in increased use of encryption. Encryption is deployed in, broadly, three different ways¹¹:

- **Full-Disk or Device Encryption:** In the case of a laptop or personal computer, technologies to encrypt the full content of the hard drive have been available for some time. It has also been possible for some time to equivalently encrypt the storage of a mobile device such as a smartphone. In approximately 2014, technology companies such as Apple and Google have begun enabling device encryption by default on their smartphones. Decryption and access to the device typically requires a passphrase or PIN. The legitimate requirement for such encryption is to protect the smartphone owner’s personal data against loss or theft of the device.
- **End-to-End Encryption:** This expression applies to encryption of messages sent across a messaging platform in such a way that they are only readable by the sender and the recipient of the messages. Many messaging services, including iMessage, WhatsApp and Facebook Messenger offer variations on end-to-end encryption of messages. Taking iMessage as an example, the use of end-to-end encryption means that even Apple, the providers of the service, do not have access to the content of messages.
- **Transport Encryption:** This form of encryption refers to data being encrypted for transmission between two parties. Most commonly these days, it is used to refer to the encryption of website traffic. Transport encryption is one of the fundamental security controls of the facilitates the modern world of e-commerce and e-banking, by preventing any attacker from being able to intercept communication between a customer and a bank or e-commerce website.

¹⁰ EU Parliament Study by the Policy Department, Economic and Scientific Policy, titled “Online Gambling, focusing on integrity and a code of conduct for gambling”. IP/A/IMCO/FWC/2006-186/C1/SC2. Available at: [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2008/408575/IPOL-IMCO_ET\(2008\)408575_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2008/408575/IPOL-IMCO_ET(2008)408575_EN.pdf)

¹¹ Encryption a Matter of Human Rights, Amnesty International Report, March 2016. Available at: http://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf

In cases involving the use of transport encryption, special investigative measures such as interception of communication may still be technically possible, with the cooperation of relevant parties such as the website owner and/or Internet Service Provider. Gaining access to an encrypted device or to communication that has been encrypted with end-to-end encryption is more challenging, and will often require access to the suspect's device or PC.

CASE STUDY: APPLE VS. FBI¹²

The FBI sought to unlock an iPhone 5C used by one of the shooters in an attack in San Bernardino, California, that left 14 dead in December 2015.

On 16 February 2016, in response to a request by the US Department of Justice, a federal magistrate judge ordered Apple to create a custom version of its iOS operating system that would allow investigators on the case to get around the phone's security features. Apple's Chief Executive Officer, Tim Cook, responded in an open letter, in which he stated that the government's demands constituted a "breach of privacy" with "chilling" consequences. Cook said:

"When the FBI has requested that that's in our possession, we have provided it. Apple complied with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal...But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone."

Apple appealed the court order and a federal court hearing was due on 22 March 2016. Numerous independent technology experts, law professors, technology companies and human rights organisations have supported Apple's stance on this matter. A widely held view among those opposing the FBI's request, including Amnesty International, is that if Apple was compelled to modify its software to unlock this phone, it would set a precedent that could allow the US government – and potentially other governments – to compel technology companies to weaken or otherwise circumvent their encryption by providing a 'backdoor' to intelligence and other security agencies.

In response to the case, the UN High Commissioner for Human Rights stated that: "A successful case against Apple in the US will set a precedent that may make it impossible for Apple or any other major international IT company to safeguard their clients' privacy anywhere in the world---it is potentially a gift to authoritarian regimes, as well as to criminal hackers. There have already been a number of concerted efforts by authorities in other States to force IT and communications companies such as Google and Blackberry to expose their customers to mass surveillance."

On March 28, the FBI said it had unlocked the iPhone with the help of a third party and the Department of Justice withdrew the case.¹³

¹² *Ibid.*

¹³ FBI says it has cracked terrorist's iPhone without Apple's help, CNN, 29 March 2016, <http://money.cnn.com/2016/03/28/news/companies/fbi-apple-iphone-case-cracked/index.html>

2.1.4 Bulletproof Hosting

The terms of service of most Internet and web hosting services disallow illegal activities on their networks or services. They will therefore usually cooperate with law enforcement requests for information and also with requests to take down domains or websites that are illegal.

Bulletproof hosting, on the other hand, is the name given to hosting services that do not cooperate with law enforcement requests for information or for websites to be taken down. Often these services are geographically located in other countries (relative to the country where the investigation is taking place). In most of the cases the bulletproof hosting companies will try to defend themselves by not having legal responsibilities for the criminal activities conducted by their clients using their infrastructure.

These services are often used to distribute illegal material, to generate spam email, as command and control servers for malware and for other forms of criminal infrastructure^{14, 15, 16}.

Phishing websites that target customers of online banking (and other) services often use bulletproof hosting to create websites that look similar to the legitimate websites. These are often taken down, or blocked, on the basis of unauthorised use of the financial institution's trademark. Websites that do not use the trademark of a legitimate organisation can be more difficult to take down.

The legislation in some countries supports the blocking by national ISPs, using various technical filtering techniques, of content that is known to be illegal¹⁷.

Information provided by the bulletproof hosting companies to the authorities on their users and services is not of much use for an investigation due to the fact that details of these individuals are most of the time fake. However, the payment method for the rented services could be an important lead that might assist in the identification of the source of a criminal activity.

On the legislative side there are also difficulties in establishing the jurisdiction for the committed illegal activities as there might be being more sources, destinations or other coordination places/entities involved.

In countries where there is a bulletproof hosting interception could be used during an investigation. This will assist in gathering information on the source, destination and nature of the criminal activity.

¹⁴ <http://www.cio.com/article/2428317/infrastructure/in-china---700-puts-a-spammer-in-business.html>

¹⁵ http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658_2.html?sid=ST2008111801165&s_pos=

¹⁶ https://en.wikipedia.org/wiki/Bulletproof_hosting

¹⁷ T-CY(2006)04 Strengthening Co-operation between law enforcement and the private sector, examples of how the private sector has blocked child pornographic sites, February 2006. Available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e6ed1>

2.1.5 Underground Economy

The underground economy is the name given to services used by criminals to trade services and information with each other. There have been many examples of underground forums, such as Silk Road and DarkMarket.¹⁸

Underground economy is organisationally structured to commit crimes. They often use a business model named Crime-as-a-Service.

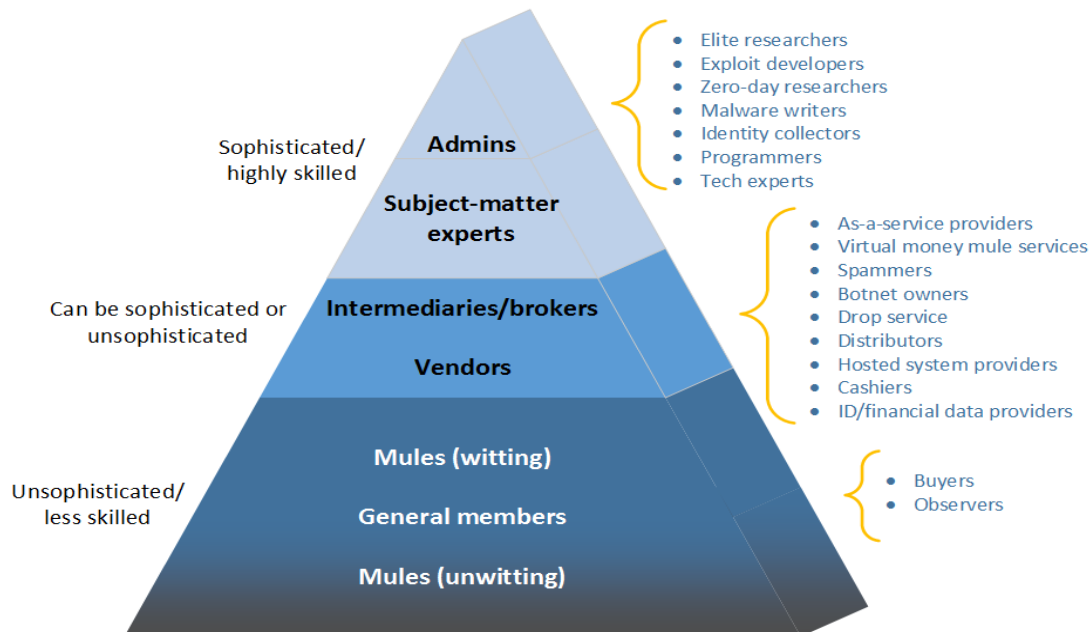


Figure 1: Participants of the Criminal Business Model on the Darkweb

Picture Impact training

Underground forums that are dedicated predominantly to credit card fraud and the sale of stolen credit card data are often referred to as carding forums.

In most of the cases these forums are open only for restricted “clients” based on passwords or other security measures.

The investigations into these types of forums are often very long and complex, with undercover agencies often slowly infiltrating the forums and moving to positions of authority from where they will gain access to information that will enable charges to be brought against the administrators and operators of the forum. The fact that such complex investigations are required means that for most investigations it will not be possible to infiltrate an underground forum to collect evidence for an individual online criminal act or money laundering investigation.

Also, from the investigative perspective it is important to have relevant legislation in place that incriminate these illegal activities, allow undercover activities to be conducted and evidence obtained to be admissible in court. This investigation is a mixed of classic investigative techniques and online techniques.

¹⁸ To find information about the Darknet markets see: <https://www.deepdotweb.com/>

In cases where the owners or operators of a known underground forum are present within the national jurisdiction, or where the underground forum is hosted within the national jurisdiction, relevant substantive provisions in national legislation can be used as the basis of a criminal proceeding in such cases. The relevant provisions will depend on the particularities of the case but could be equivalent to, for example, Article 6 of the Budapest Convention.

SELF-REFLECTION QUESTIONS

1. **What conditions must be met before monitoring of a suspect bank account could be authorised?**
2. **What balance is necessary to protect the interests of a potentially innocent third party who has had their bank account compromised?**
3. **What provisions are available in your national legislation to compel a suspect to decrypt an encrypted device or file?**
4. **What measures are available in your national legislation to compel a national Internet Service Provider to block or filter illegal content?**

2.2 Identification of the Perpetrator

Recall from the basic course that the key characteristic that is used to identify a suspect on the Internet is their IP address.

The purpose of this section is to describe in more detail some of the practical challenges that can arise when trying to associate a particular IP address with an individual. In other words, in situations where you can associate some online criminal activity with a particular IP address and you are trying to identify the real-world person who had control of that IP address at the time the online criminal activity took place.

The converse question may, of course, also arise whereby you have a real-world suspect and you are trying to identify the IP address being used by this individual online. In many respects this situation is easier to deal with and traditional investigative techniques (such as special investigative measures) can be used.

2.2.1 Network Address Translation (NAT)

In order to communicate on the Internet, a source and destination IP address are required. In the past (before the introduction of NAT), each computer needed to have a unique IP address allocated. The problem with this is that IP addresses have been inefficiently allocated and are therefore running out. The long-term solution to the shortage of IP addresses is the introduction of a version of IP, IP version 6, that has a much larger number of available IP addresses. In the meantime, several techniques are used to extend the lifetime of IP version 4, one of which is NAT.

There are certain ranges of IP addresses that are reserved. In other words, they are not supposed to be used on the Internet. Instead, it is intended that they will be used in private networks, such as internal offices ranges. The reserved ranges are:

1. 10.0.0.0 – 10.255.255.255
 - a. In other words, any IP address starting with “10.”
2. 192.168.0.0 – 192.168.255.255
 - a. In other words, any IP address starting with “192.168.”
3. 172.16.0.0 – 172.31.255.255
 - a. In other words, any IP address starting with “172.” and followed by a number between “16” and “31”.
 - b. This reserved range is less frequently used than the other two.

The most common application of NAT involves an organisation assigning IP addresses from one of these ranges to all of their office PCs. Then, when one of the PCs on their network wants to communicate with an IP address on the Internet, their router replaces the internal IP address with one of a small range of real, Internet, IP addresses. In most cases, the outcome of this process is that all IP data from all PCs on the office network appears to the rest of the Internet as if it is coming from a single IP address.

The use of NAT is also extremely common, virtually ubiquitous in fact, in home broadband Internet setups. This means that a home user can use multiple devices on their home network but their Internet Service Provider only needs to assign a single IP address to their connection.

Many excellent technical descriptions of how NAT works are available online^{19, 20, 21}. The interested reader is encouraged to review some of these references for further information if required.

It is worthwhile to consider the implications of the use of NAT on online investigations. It may be possible to identify the public IP address in use during a certain criminal activity but if NAT is in use, this IP address may represent the online activity of many independent users. Therefore an additional investigative step is required to establish the link between the online activity and an individual user’s PC using a reserved IP address behind the NAT router.

There is a remote possibility that an organisation using NAT may have logs of incoming and outgoing traffic that could be used to establish which internal IP address was responsible for generating a specific piece of traffic, which is the subject of the investigation. However, this is unlikely. Further, in cases such as small offices or home users, using standard equipment and services provided by their ISP, such records are not available.

The investigation must therefore use an alternative mechanism to associate the suspect IP address with a particular computer. There may be certain characteristics of the traffic that allow the identification of the internal IP address. For example, certain applications include the internal IP address of the PC generating the traffic in the traffic itself. Alternatively, there may be other distinguishing characteristics, apart from the IP address, that can be used. These would include usernames, email addresses, technical information about the source device, and so on. Through detailed analysis by an expert, it may be possible to identify the source of the traffic in this way.

¹⁹ <http://computer.howstuffworks.com/nat.htm>

²⁰ <http://www.faqs.org/rfcs/rfc1631.html>

²¹ <https://www.youtube.com/watch?v=QBqPzHEDzvo>

If the criminal activity is taking place in real-time, special investigative measures may be applied to intercept outgoing traffic and identify the internal PC in that way. In such cases, the cooperation of the organisation might be required to identify the appropriate location on their network to install a monitoring station. This will typically involve the cooperation of the IT/system administration staff and it must be borne in mind that there is no way to know, in advance, that the suspect is not one of the IT/system administration staff who would then become aware of the investigation.

In summary, NAT presents a challenge for the association of a particular IP address with the activity of a real-world user. Additional information (apart from the IP address) gathered from analysis of the online activity or, alternatively, further investigative measures will typically be needed to complete the investigation and identify the suspect.

2.2.2 Carrier Grade Network Address Translation (CGN)

Additional challenges are presented by the use of carrier grade NAT, or CGN. CGN is a technique by which an ISP can use NAT to translate a large number of subscriber IP addresses into a small number of real Internet IP address.

In these cases, CGN means that, apart from the NAT that might take place while traffic moves from a small or home office to the ISP's network a second NAT might take place within the ISP's network before it is forwarded to the Internet^{22, 23}.

CGN differs from "simple" NAT described in the previous section because not only is the private (internal) IP address replaced with a public (external) IP address, but also the private (internal) TCP/IP port number is replaced with a public (external) port number. In essence, CGN maps TCP or UDP sessions from an internal address space to an external address space. This technique allows CGN to overcome some of the scaling issues with "simple" NAT, but introduces a problem from an investigative point of view, namely that in the overwhelming majority of cases, organisations will log the IP address from which they receive connections but will not log the incoming port number. Since CGN allows for potentially many thousands of users to be using the same public IP address, the IP address alone will not be sufficient to associate the activity with a particular user.

Therefore, presuming the port number is not available; other additional information (apart from the IP address) gathered from the analysis of the online activity would be required to identify the suspect.

Europol, in their 2016 Internet Organised Crime Threat Assessment, makes several recommendations for addressing the investigative challenges raised by CGN, as follows²⁴:

- In order to be able to trace back in individual end user to an IP address on a network using CGN, law enforcement must request additional information from the service providers via legal process:
- Source and destination IP address
- Source port number
- Exact time of the connection (within a second).

²² Background information, further links can be found at: https://en.wikipedia.org/wiki/Carrier-grade_NAT.

²³ <http://www.networkworld.com/article/2237054/cisco-subnet/understanding-carrier-grade-nat.html>

²⁴ Internet Organised Crime Threat Assessment (IOCTA), Europol, 2016. Available at: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016> and 2017 at : <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>

- However, the lack of harmonised data retention standard requirements in Europe means that content service, internet service and data hosting providers are under no legal obligation to retain this type of information, meaning that even a more elaborate request from a law enforcement agency would not yield useable information from the provider.
- Regulatory/legislative changes are required to ensure that content service providers systematically retain the necessary additional data (source port) law enforcement requires to identify end users.
- Alternatively, practical solutions can be developed through collaboration between the electronic service providers and law enforcement. Some electronic providers in Europe do store the relevant information (source port). A European-wide portal could maintain an updated list of those providers and a list of contact points to address in case an investigation is stalled by CGN.

2.2.3 The use of Anonymisers

An anonymiser is a tool that attempts to make activity on the Internet untraceable. It acts as an intermediary between a PC and the rest of the Internet and accesses the Internet on the user's behalf while hiding the user's identifying information.

Anonymisers fall into two broad categories;

- **Protocol-specific anonymisers:** These work only with one particular protocol. An example would be an anonymous remailer for email or an anonymising web proxy.
- **Protocol independent analysers:** These work by creating an IP tunnel through which all user traffic will be forwarded. From the perspective of the receiving user, the IP traffic will look like it comes from someone other than the original sender. An example would be Tor (formerly "The Onion Router").

Some examples are discussed in the case studies below.

In investigations where an anonymiser has been used and the service provider is unwilling or unable to provide support to the investigation, alternative (non-technical) investigative measures may be required to make progress.

CASE STUDY: ANONYMOUS REMAILER

The purpose of an anonymous remailer is to receive messages, remove identifying information and then forward them on to the intended recipient in such a way that the recipient cannot tell where they originally came from.

There are several ways in which this can be achieved:

- **Pseudonymous remailers;** Take away the email address of the sender, give a pseudonym to the sender and sent the message to the intended recipient. The recipient will be able to reply by sending an email to the pseudonym, which the remailer will forward back to the original sender.
- **Cypherpunk remailers (a.k.a. Type I):** Send the message to the recipient while stripping away the sender's address. The recipient cannot respond

to emails sent via this type of remailer. Usually the sender of the message will submit the message to the remailer in encrypted form. The remailer will decrypt it and send it to the recipient. These types of remailers do not keep logs of transactions.

- **Mixmaster remailers (a.k.a. Type II):** The sender composes an email and sends it to the remailer. The message is forwarded multiple times through a peer-to-peer network of remailers until it eventually arrives at the recipient. The recipient cannot respond to the email, unless a reply address is provided in the body of the email. Special software needs to be installed on the user's PC to use a Mixmaster remailer.
- **Mixminion remailers (a.k.a. Type III):** These are similar to Mixmaster remailers but certain technical issues have been addressed. In particular, it is possible for the recipient to respond via the remailer network, without knowing who the sender was.

It is possible to chain multiple remailers together so that even the remailers do not know who is sending the message. It is also possible that a web-based interface to a remailer may be used, as opposed to using a standard or custom email application installed on the user's PC.

CASE STUDY: ANONYMISING WEB PROXY

An anonymising proxy server attempts to anonymise the web browsing activity of a user. Typically an anonymising proxy will accept requests from users and pass them on. From the perspective of the web server that is receiving the request, the request looks like it is coming from the anonymising proxy. Unless the anonymising proxy has the records available to associate the outgoing requests with specific source IP addresses, this will not be possible from analysis of the IP data.

The use of a web proxy is supported in virtually every standard browser, because there are many legitimate reasons why users might want to configure a proxy²⁵. The use of these services typically requires little more than configuration of a small number of options in standard browser software.

However, the content of the web traffic itself may still contain details that could help to identify a suspect. For example, if a suspect were to log in to a website via an anonymising proxy, the IP address that they were logging in from might not be available but analysis of the web traffic might reveal the username and/or password being used.

²⁵ For example, an organisation may want to block employees from viewing certain websites during business hours. In such cases, a proxy can be configured on employee PCs and direct web access to the Internet is then blocked by a firewall. All web requests must therefore pass through the proxy and the proxy is then in a position to block or allow requests according to an organizationally defined policy.

CASE STUDY: TOR (FORMERLY “THE ONION ROUTER”)

Tor is a software tool that directs Internet traffic through a network of PCs, owned by volunteers and operated for free, consisting of several thousand relays. The purpose of this is to make it difficult for Internet activity to be traced back to the original user.

The routing is implemented by multiple layers of encryption and then forwarding of the traffic through multiple, randomly selected relays. Each relay decrypts a layer of encryption, which reveals only the next layer of relaying and passes the remaining encrypted data on to it. The final relay decrypts the innermost encrypted data and sends it on to its intended destination without revealing, or knowing, the source IP address. The routing of the communication is therefore partly concealed from every hop in the Tor network, meaning that there is no single point at which communicating peers can be traced in a way that relies on, or identifies, the source and destination of the communication.

A user of the Tor network installs special software on their PC that will intercept some or all outgoing network traffic and forward it to the Tor network, rather than directly to the intended destination. Once the traffic is within the Tor network, it is sent from router to router until it reaches the last router in the network (where the final decryption takes place and the original traffic is revealed). This router is known as the exit node. From the perspective of the destination, the traffic appears to be originating from the exit node.

From the description above, it may appear that the Tor network only allows anonymisation of client-initiated communication. However, Tor also supports the running of servers via the Tor network in such a way that the server’s IP address is not visible to the users of that server. To achieve this, special addresses are given to servers, known as onion addresses, and these can be accessed via the Tor network in a way that does not reveal the location of the server²⁶. A hidden service advertises its existence and then the Tor network establishes “rendezvous points” in a decentralised way to allow connections between hidden services and users without either knowing the other’s identity.

While direct identification of the IP address of a suspect using the Tor network is virtually impossible, there are specialist techniques available to identify other information that may progress the investigation. For example, it is possible that server misconfiguration may reveal information about the true source of the hidden service. The error pages generated by many common web servers (i.e. the error message presented to a user whenever their request causes an error) include the IP address of the server, meaning that by generating an error condition on the server it may be possible to reveal the IP address.

²⁶ Further detail on the operation of hidden services can be found at:
<https://www.torproject.org/docs/hidden-services.html>

2.2.4 Botnets/malware/remote control of a PC

When a person's PC is infected with a malware, it is possible that software might be installed on the PC that allows someone a suspect to control the PC and use it to conduct criminal activity. Amongst other possibilities, the suspect might install a proxy on the compromised PC and forward all of their traffic via this proxy.

In these cases, the Internet traffic that is associated with the criminal activity will appear as if it is coming from the IP address of the innocent party. However, technical measures are possible that might allow identification the true source of the traffic. For example, by monitoring the IP traffic travelling to and from the compromised PC, it may be possible to identify the IP address of the suspect who is controlling the PC. This is most likely in cases where a criminal has compromised a small number of PCs and is individually communicating with them.

However, the complexity of the command and control (C&C) infrastructure that criminals use to operate networks of compromised PCs (sometimes known as botnets), should not be underestimated. Many techniques are used by operators of botnets to conceal their activity^{27, 28} and to enable their control traffic to pass through firewalls²⁹.

Analysis of the person's PC might reveal the presence of malware, supporting the assertion that the PC might have been controlled remotely by a third party. However, it is also not beyond the realm of possibility that a suspect may deliberately infect their PC with malware in order to rely on a defence that they were not responsible for the actions performed on, or with, the PC. Therefore, the challenge of "putting the suspect at the keyboard" may require further non-technical measures such as surveillance to establish with a degree of certainty which individual performed which actions, or equivalently, to rule out a particular individual as having performed the criminal acts.

Investigators also face challenges in relation to the way to alert the user about the infection and the proper instruments to be used to remove the malware. The moment to make the users aware of their infected PCs is important and has to be decided based on the status of the investigation. The removal of the malware from the infected machines should be done in a way to avoid illegal access or interception of communication without proper consent/authorisation.

2.2.5 The use of open, public or stolen WiFi

Open WiFi networks are specifically set up to allow anyone to connect to them and use the Internet. Open WiFi networks present a risk of criminal use of the Internet connectivity in such a way that it may not be possible to associate their activity with anyone other than the source of the open WiFi. Some, but not all, open WiFi networks require registration and/or will record logs.

A similar problem arises in cases where it is possible for an attacker to guess or crack the WiFi password of a closed WiFi network. One commonly cited scenario that arises with the use of hacked WiFi access points and/or stolen WiFi access is for an attacker to park in a

²⁷ https://en.wikipedia.org/wiki/Fast_flux

²⁸ https://en.wikipedia.org/wiki/Domain_generation_algorithm

²⁹ http://www.pcworld.idq.com.au/article/417011/malware_increasingly_uses_dns_command_control_channel_avoid_detection_experts_say/

car outside an office building and use their WiFi to conduct criminal activity. In such cases, it is unlikely that any identifying records of the connection to the WiFi network will be available (particularly for smaller businesses) and therefore no way to continue the investigation to locate the suspect. It is possible that a suspect may use the same location on multiple occasions, in which case surveillance of the location may lead to identification of the suspect.

A related problem arises due to the fact that there are many locations where Internet access is available in a relatively anonymous fashion, such as libraries, universities or cybercafés.

The defining characteristic of this problem is the ability for a suspect to gain virtually anonymous access to the Internet through the use of Internet connectivity and, in some cases, computers that are owned by a third party.

Similar to the argument made at the end of the previous section, analysis of the person's network might reveal the presence of open WiFi, supporting the assertion that the WiFi might have been used by a third party. However, it is also not beyond the realm of possibility that a suspect may deliberately leave their WiFi open in order to rely on a defence that they were not responsible for the actions performed via the WiFi. Once again, further non-technical measures such as surveillance may be required to establish with a degree of certainty which individual performed which actions, or equivalently, to rule out a particular individual as having performed the criminal acts.

Internet interception is another technique which can be used to establish the involvement of different individuals in the criminal activities.

2.2.6 Identification of the Owner of an IP address

WHOIS is a free service that provides information about the owner of a domain name, including name, surname and contact references.

According to ICANN³⁰, the worldwide domain name administrator, "the WHOIS service is a free, publicly available directory containing the contact and technical information of registered domain name registrants. Anyone who needs to know who is behind a website domain name can make a request for that information via WHOIS.

The data is collected and made available by registrars and registries under the terms of their agreements with ICANN. WHOIS is not a single, centrally managed database. Rather, registration data is held in disparate locations and administered by multiple registries and registrars. They set their own conventions for WHOIS service, consistent with the minimum requirements established in their contracts with ICANN".

WHOIS is used to find out to whom a particular IP address has been assigned. The problem is that the database of WHOIS information is not always accurate. Registrars are required to periodically send communication to those registered with them but there is no onus on them to confirm the accuracy of the data provided by the registrant. This is a problem in particular when trying to identify who owns a particular domain name.

³⁰ Internet Corporation for Assigned Names and Numbers, the international organization in charge of defining policies and related contracts with Internet registries and registrars.

In the case of IP addresses, a further systemic problem has been identified, which is the sub-allocation of IP addresses³¹. The problem arises if a provider to whom a range of IP addresses have been assigned in turn assigns some of those IP addresses to a sub-provider but does not keep accurate or up-to-date information about who is using what IP addresses. In particular, the provider might not always report the sub-allocation to the WHOIS database registry, meaning that the WHOIS database will not contain accurate information about the ultimate controller of the IP address in question.

WHOIS data can be regarded as a specific form of subscriber information data, publicly available on the Internet with unlimited access. However, in the light of the entry into the effect of the EU General Data Protection Regulation (GDPR) on 25 May 2018 access to WHOIS will change to ensure compliance with the GDPR.³²

SELF-REFLECTION QUESTIONS

- 1. Can an order to monitor an IP address be formulated such that it will not impact on the rights of innocent third parties?**
- 2. How might it be possible to establish whether the activity associated with a particular IP address was performed by the holder of that IP address or remotely due to the fact that their PC was infected with malware?**
- 3. What conditions must be satisfied to obtain an order that would enable the identification of the IP address in use by a particular real-world suspect?**
- 4. What conditions must be satisfied to obtain an order that would enable the identification of the real-world holder of an IP address that is involved in criminal activity?**

2.3 Engagement with ISPs

2.3.1 Type of data being requested

For the purposes of a criminal investigation, three types of data may be needed:

- Subscriber information
- Traffic data
- Content data.

In many jurisdictions, conditions to access for subscriber information tend to be lower than for traffic data and the strictest regime applies to content data. The type of data being requested will obviously influence the nature of the request that needs to be made to a multinational service provider in order to gain access to the data. Some, but not all, multinational service providers have a form of expedited voluntary cooperation by which subscriber information can be provided, pending receipt of formal legal process.

³¹ <https://blog.apnic.net/2016/11/28/sub-allocation-system-undermines-integrity-whois-accuracy/>

³² For further reading on access to WHOIS see: <https://www.icann.org/news/blog/data-protection-privacy-update-seeking-input-on-proposed-interim-model-for-gdpr-compliance>

2.3.1.1 Subscriber Information

Subscriber information is the most commonly sought information in domestic and criminal investigations and, without this information, it is often impossible to proceed with an investigation³³. The term subscriber information is defined in Article 18.3 of the Budapest Convention as:

"For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

- a. The type of communication service used, the technical provisions taken thereto and the period of service;*
- b. The subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;*
- c. Any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement."*

Subscriber information is likely to be held by service providers although the information may actually be stored on servers in other jurisdictions. It may thus not always be clear to whom to address a request for subscriber information.

2.3.1.2 Traffic Data

Log files that record activities of the operating system of a computer or of other software or of communications between computers are essential for cybercrime cases and may also be equally important in cases involving online crime proceeds. "Traffic data" is defined in Article 1.d of the Budapest Convention as:

"Traffic data means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service"

2.3.1.3 Content Data

Finally content data is also often required in criminal investigations. According to paragraph 209 of the Explanatory Report of the Budapest Convention:

"Content data is not defined in the Convention but refers to the communication content of the communication; i.e. the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)."

A distinction should also be made between "stored" content data, that is already available on a computer system and "future" content data that is not yet available and needs to be gathered, for example, through the interception of communication. Interception may be carried out upon a court order either by the police or by a specialised body directly, or with the assistance of a service provider. Its use is often restricted to serious crimes.

³³ T-CY Report on Rules on obtaining subscriber information adopted at the on 12th plenary, 2-3 December 2014. Available at: <https://rm.coe.int/16802e7ad1>

2.3.2 The EU Data Retention Directive declared invalid by the decision of the CJEU

As described above, the identification of perpetrators in the cyber-world many times depends on access to the data held by private Internet service providers. The connection of an IP address with data of a person (subscriber to an IP address, email or Facebook account) and the suspect's interaction with other possible suspects (traffic data) and even content of such interaction is an essential part to discover the perpetrator, other suspects and to secure evidence of a crime.

All this is possible only if the private company retains the necessary data (subscriber data, traffic data and/or content data). The legal obligation for data retention for law enforcement purposes has been challenged before the Court of Justice of the European Union (CJEU)³⁴. In its decision in Joined Cases C -93/12 and C - 594/12 (Digital Rights Ireland and Seitlinger and Others) the Data Retention Directive 2006/24/EC³⁵ has been declared invalid. This decision led to the subsequent annulment of relevant national legislation in some EU countries, where there was an obligation for the providers to retain the traffic data for a period varying from 6 months to 2 years.

The result is that the ISPs are not obliged any more to store (retain) the traffic data for the purpose of investigation of serious crime for the period previously requested by national legislation, but they store data only for the period, necessary for the billing or other commercial use. In practice this would mean about 1-3 months. The EU has not adopted a new legal instrument yet and many states are still defining appropriate legal solutions to address the legal concerns. It seems however that is a particularly challenging to address the Court's expectation to avoid covering, in a generalised manner, all individuals, all means of electronic communication and all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime,

One of the possible approaches could be regulating the production order to store (traffic) data after the legal request for a limited period of time is issued.

Since the reasons for derogation were based on the court's views that the directive exceeded the limits of the principle of proportionality, as it interfered in a serious manner with the fundamental rights to respect for private life and to the protection of personal data, this decision might have impact also to non-EU member states, especially if the national legislation would be challenged at the national constitutional courts or in case of individual complaint to the European Court of Human Rights for violation of Article 8 of the Convention on Human Rights.

The main highlights of the court decision might therefore be of a relevance to the national legislator. The court found that the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data. It is also likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance.

³⁴ Court of Justice of the European Union Judgement in Joined Cases C-293/12 and C-594/12. Digital Rights Ireland and Seitlinger and Others. Available at:

<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>

³⁵ Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. (*Invalid*)

The court noted that the directive does not regulate the content of the communications and that the retention of data for the purpose of their possible transmission to the competent national authorities genuinely satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security. However legislature has exceeded the limits imposed by compliance with the principle of proportionality, noting that the review of the discretion of legislator should be strict.

Although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, the wide-ranging and particularly serious interference of the directive with the fundamental rights to respect for private life and to the protection of personal data has exceeded the limits imposed by compliance with the principle of proportionality, as:

- It is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary,
- It covers, in a generalised manner, all individuals, all means of electronic communication and all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime,
- There is no objective criterion for the competent national authorities to have access to the data and can use them only for the purposes of prevention, detection or criminal prosecutions concerning offences that may be considered to be sufficiently serious to justify such an interference. It simply refers to 'serious crime',
- The access to the data is not made dependent on the prior review by a court or by an independent administrative body,
- It imposes a retention period of at least six months, without making any distinction between the categories of data on the basis of the persons concerned or the possible usefulness of the data,
- The period is set at between a minimum of six months and a maximum of 24 months, but there is no objective criteria on the basis of which the period of retention must be determined to be limited to what is strictly necessary,
- It lacks of sufficient safeguards to ensure effective protection of the data against the risk of abuse,
- It does not ensure the irreversible destruction of the data at the end of their retention period.

For further reading on impact of the decision, Franziska Boehm and Mark D. Cole have pointed out some of the relevant aspects in their article Data Retention after the Judgement of the Court of Justice of the European Union from 30 June 2014³⁶. They emphasised that the statements of the Court not only refer to the singular case of the Directive, but also establish general principles for similar data retention measures. These principles encompass the following points:

- The collection, retention and transfer of data each constitute infringements of Article 7 and 8 and require a strict necessity and proportionality test.

³⁶ Data Retention after the Judgement of the Court of Justice of the European Union, Prof. Dr. Franziska Boehm et al., Munster/Luxembourg, 30 June 2014. Available at: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

- The Court clearly rejects the blanket data retention of unsuspecting persons as well as an indefinite or even lengthy retention period of data retained.
- The Court sees a sensitive problem in data originally collected for other purposes later being used for law enforcement purposes. It requires a link between a threat to public security and the data retained for such purposes.
- The required link significantly influences the relationship between private and public actors. Law enforcement is only allowed to access data collected for other purposes in specific cases.
- The Court explicitly demands effective procedural rules such as independent oversight and access control.
- The collection and use of data for law enforcement purpose entails the risk of stigmatisation stemming from the inclusion of data in law enforcement databases. This risk needs to be considered and should be taken into account when reviewing other existing or planned data retention measures at law enforcement and Member States level.

In order to address the issues raised by the CJEU ruling, on 29th November 2016, the UK passed the Investigatory Powers Act 2016. Amongst other important techniques, it places an obligation on ISPs to retain 'connection data' for 12 months. This is a lesser form of intrusion than recording all the browsing data and it is designed to accommodate the CJEU concerns about disproportionate intrusion. It also creates new powers that allow, with the authority of a warrant, the directed monitoring and retention of a suspect's browsing, etc.

2.3.3 National ISPs

The data that Internet Service Provider (ISPs) retains is important for the identification of the perpetrator and his accomplices, their connection in time and space and for the evidence on the content of communication (e-mail content, posts on social platforms such as Facebook).

The obligations of ISPs are regulated by national provisions on retention of (traffic) data and the conditions to access and use of those data for the purpose of criminal investigation. The data can be categorised as subscriber data, traffic data and content data.

The subscriber data is considered as less privacy sensitive and intrusive than traffic data and content data. It is the most often sought information in domestic and international criminal investigations relating to cybercrime and electronic evidence. Without this information, it is often impossible to proceed with an investigation.

Subscriber data is usually held by private ISPs and can be obtained by police or prosecutor production order. However in case of dynamic IP addresses, many states require court order, as some traffic data is involved. In most states court order is requested for: access to traffic data (for the question of data retention see the previous section); for preservation order (to store traffic data onwards); for monitoring traffic data and; for access to content data and in particular for the interception of communications (the later usually considered as most invasive and therefore subject to specific safeguards, conditions and principle of proportionality).

In addition to legal requirements the practical and technical arrangements for transfer of data between ISPs and law enforcement authorities are also important, particularly in case of live monitoring and transmitting of data, which allows for quick processing of data.

Another area of cooperation between law enforcement authorities and ISPs is the question of blocking and take down of Internet pages in case of criminal offence or criminal content. The child pornography material is most frequently mentioned in this context, but also other forms might be relevant, such as hate speech and public provocation to commit terrorist offence or violation of intellectual property rights. While usually a court order for such measure would be required, the “voluntary” action of the owner or editor of the Internet page is being promoted, for the reason of breaching the internal code of conduct. While such approach might be most efficient, especially in the case of prima facie violation (such as pornographic material), it might raise some concerns related to possible interference with freedom of speech, as identified in the Council of Europe Study on filtering blocking and take down of illegal content on the internet in 2016³⁷.

SELF-REFLECTION QUESTIONS

1. What is meant by the term “subscriber information”?
2. What is meant by the term “traffic data”?
3. What is meant by the term “content data”?
4. What are the implications of the CJEU decision on data retention for the identification of a real-world suspect from an IP address associated with criminal activity?

2.4 Multinational Service Providers

In cases involving online crime proceeds, just as in many criminal investigations of cybercrime, crucial evidence is held by private sector organisations such as Facebook, Google, Microsoft, Twitter, Yahoo! and others. Cooperation between competent authorities and these multinational service providers is therefore essential to secure electronic evidence. It is not possible in a manual like this to provide information about all different multinational service providers that a potential reader might need to engage with; the details of an individual service provider’s process for handling law enforcement requests can usually be found on their websites. Therefore, an effort has been made to categorise the key aspects of the law enforcement policies of multinational service providers.

The aim is to provide a framework within which to consider how to engage with a specific service provider in future. Secondly, it will also help to clarify the factors that multinational service providers will take into account when examining incoming law enforcement requests, and thereby the factors that should be considered when formulating a request to the service provider in order to maximise the possibility of a successful outcome.

The Cloud Evidence Group (CEG) prepared an extensive document on the issue of law enforcement access to data held by multinational service providers³⁸. Many interesting

³⁷ Council of Europe Study on filtering, blocking and take-down of Illegal Content on the Internet, June 2016. Available at:

<https://www.coe.int/en/web/cybercrime/-/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>

³⁸ T-CY (2016)5, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final Report, 16 September 2016. Available at:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

aspects will be elaborated in more detail in Section **Error! Reference source not found..** To highlight some of them:

- The CEG concludes that mutual legal assistance remains the main means to obtain electronic evidence from foreign jurisdictions for use in domestic criminal proceedings. This is particularly true for content data.
- Access to subscriber data is less intrusive and should be lightened. Article 18 on domestic production order should be used also for multinational ISPs operating in the territory of a state – a draft Guidance note nr. 10 on Production orders for subscriber information has been prepared.
- The voluntary direct cooperation of the ISPs from USA with foreign law enforcement authorities has been acknowledged, taking into account also high increase of mutual legal assistance requests.
- The CEG proposed to consider drafting additional protocol in order to address some existing challenges, namely to lighten the regime to access subscriber data and to allow for direct request to ISPs under certain conditions.

2.4.1 Jurisdiction

It is often not obvious to a criminal justice authority which jurisdiction the required data is stored and/or which legal regime applies to data³⁹. A service provider may have its headquarters in one jurisdiction and apply the legal regime of a second jurisdiction while the data is stored in a third jurisdiction. If the location of data determines the jurisdiction, it is also possible that the service provider may not easily know the location of the data. Even if the location of the data is known, it is not clear which rules apply for lawful access by criminal justice authorities. It may be argued that the location of the headquarters of the service provider, or of its subsidiary, or the location of the data or the law of the state where the suspect subscribed to the service, or the location or citizenship of the suspect may determine jurisdiction⁴⁰.

2.4.2 General position

In all cases (except emergency requests, as discussed below), the Mutual Legal Assistance process will need to be followed in order to gain access to content data.

Concerning subscriber data, multinational ISPs can broadly be divided into two categories; those that will respond to legal requests from jurisdictions outside of the United States and those that require a Mutual Legal Assistance treaty request to be served on them by a United States court.

2.4.3 Preservation requests

Some service providers will accept preservation requests and will thereby preserve data for a period of time (usually in the region of 90 days) pending receipt of formal legal documentation. If preservation of longer than 90 days is required, an extension letter should be sent to the service provider before the end of the 90-day period.

³⁹ Discussion paper prepared by the T-CY Cloud Evidence Group, Criminal justice access to data in the cloud: challenges, May 2015. Available at:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59>

⁴⁰ T-CY (2016)5, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final Report, 16 September 2016. Available at:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

2.4.4 Emergency requests

In cases involving imminent risk of harm, death or serious physical injury, most multinational service providers will cooperate with law enforcement requests for information where it can be demonstrated that the service provider has information that may be necessary to prevent the harm, death or serious physical injury. One practical challenge in this respect, highlighted elsewhere in this course⁴¹, is that many countries do not have legislation in place permitting disclosure of data to domestic criminal justice authorities in emergency situations. Notably, and in particular, the USA has such a provision, which allows US-based multinational service providers to respond to emergency requests but in cases where the service provider is not based in the USA, or a small number of other countries, the legal basis for disclosure may present an additional practical challenge.

2.4.5 Request scope

Most multinational service providers will reject requests for information that are overly broad in scope. A definition of acceptable scope is not usually provided except to state, “overly broad or vague requests will not be processed”. Therefore, to stand the greatest chance of a successful response, requests should be formulated with as narrow a scope as possible and refer, whenever possible, to subject accounts by whatever unique identifier is used on the specific platform under consideration.

It may not always be obvious what the unique identifier in use on a particular platform. In many cases, but not always, the username and/or email address associated with a particular account are sufficient.

2.4.6 Notification of subject of request

In many cases, when a law enforcement request is received concerning a user of a multinational service provider, it is the policy of the service provider to inform the subject of the request about the existence of the request. This will be done unless notification is prohibited by law or court order.

Therefore, if notification of the subject might compromise the investigation, the order that forms the basis of the request for information from the service provider must include a prohibition on informing the subject of the request.

Additionally, some service providers further indicate that if a law enforcement request brings to their attention an ongoing violation of their terms of service, action may be taken to prevent further abuse, including actions that may notify the user that the service provider is aware of the conduct.

SELF-REFLECTION QUESTIONS

1. Why is it important to separately order a service provider to preserve data required in a criminal procedure, pending receipt of formal documentation to disclose evidence?
2. What conditions must be in place before an order to a service provider

⁴¹ See Section 4.2.2.2.2

that compels disclosure of information pertaining to a user of that service provider could include a clause to prevent the service provider notifying (directly or indirectly) the subject of the request?

3. What options are available in a scenario where an account of a multinational service provider is known to be associated with criminal activity in your jurisdiction but it is not possible to know, without receiving information from the service provider, whether the holder of that account is present in your jurisdiction or not?
4. Considering the delays involved in the Mutual Legal Assistance process, what options (if any) are available to expedite access to content data held by a multinational service provider?

3 Financial Investigations

3.1 Introduction

The concept of targeting online crime proceeds brings together the approaches of cybercrime investigation, financial investigation and money laundering investigation with the purpose of increased efficiency and success of criminal investigations and criminal procedure from the perspectives of both prosecuting a criminal and targeting and confiscating proceeds of crime.

The basic course manual contains basic and detailed explanations of financial investigation, including defining its scope and elements. The definition of financial investigation as well as its elements and some specifics related to online crime, including cybercrime investigation will be briefly addressed and some more details will be provided on recent development of the concept of financial investigation in the EU.

3.2 Financial Investigations and Online Crime Proceeds

Financial investigation can have several meanings, ranging from investigation of financial crime to, for example, investigation for taxation purpose. International legal instruments do not provide for a definition of financial investigation, but in the framework of freezing and confiscation of proceeds of crime the descriptive definition provided by the Financial Action Task Force (FATF) can be used as an example.

It should also be noted that the term financial investigation might include both investigation for targeting proceeds of crime in the framework of criminal procedure as well as in the (separate) civil (in rem) procedure. It should also be noted that financial investigation can, but does not necessarily, coincide with a money laundering investigation.

Financial investigation is an investigation method and should be conducted in parallel to criminal investigation of a profitable crime or even in the judicial phase with the main (but not exclusive) purpose to trace and freeze proceeds of crime with a view of their final confiscation.

FATF has defined financial investigation⁴² as an enquiry into the financial affairs related to a criminal activity, with a view to:

- Identify the extent of criminal networks or the scale of criminality
- Identify and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation
- and develop evidence which can be used in criminal proceedings.

As the criminal profits tend to be at least partially legalized and re-used in the legal economy, a financial investigation might be related to and/or lead to a money laundering investigation. The financial investigation can lead to the suspicion of a criminal offence of money laundering or alternatively, when a Financial intelligence unit (FIU) is analysing suspicious transactions or investigating the criminal offence of money laundering, proceeds

⁴² FATF (2012), Interpretative Note to Recommendation 30, 2nd paragraph.
See also: FATF Report on Operational issues. Financial investigation guidance, 2012.

from a (predicate) crime could become the subject of confiscation (as an object of a money laundering crime).

3.2.1 Elements of Financial Investigation

Financial investigation can be best defined by defining its elements⁴³ and identifying relevant international and national legal provisions to be applied in practice.

As described in the basic course, the elements of a financial investigation are:

1. Detecting the criminal offence and the perpetrator (parallel to criminal investigation)
2. Establishing the (value of) proceeds of crime
3. Establishing property that can be confiscated
4. Freezing order - temporary measures for securing the confiscation.

The result of a financial investigation and potentially of a freezing order would be the final confiscation of proceeds of crime.

3.2.2 Cybercrime Aspects of the Financial Investigation

As presented in more detail in the basic course, the four elements of financial investigation can also be applied in cybercrime investigations and/or investigations of online crime, involving criminal proceeds on the Internet.

There are some specifics related to investigation of online crime that need to be considered:

- Who is the perpetrator and where is the evidence of the crime?
 - This question relates to issues of identifying a suspect using an IP address, access to subscriber data, electronic communication or social network data, and potentially traffic and content data; cooperation with ISPs, both national and international; creation of requests for preservation of data, and court orders to seize and produce electronic evidence.
- What are the proceeds of crime?
 - This question is related to assets and payment systems such as e-money, virtual currencies (e.g. bitcoins) and Internet banking payments; bank accounts located abroad; multiple transactions of different types, possibly structured to conceal the sources of funds; money laundering typologies.
- What can be confiscated/the property of a suspect?
 - When considering money flows on the Internet, there is also a question of jurisdiction. Victims and perpetrators are often not in the same country. The confiscation of proceeds of cybercrime, through financial investigation or money laundering approach should be considered. The focus and target should at least be on the direct proceeds of crime (extortions paid or fraudulent transactions) and the freezing of value in identified bank accounts used for criminal offence (online extortion, computer fraud).
 - The importance of conducting a parallel financial investigation in cybercrime investigations to detect the proceeds (bank accounts and money flow, virtual currency transfers) and the existing property of the perpetrator.

⁴³ For more details see the Basic Course Manual (1.1.3).

- Freezing order
 - Acting fast is crucial in cases of e-banking and Internet in general. Looking for money laundering offence and the use of powers and international links of the Financial Intelligence Unit might be a possible solution. Court order and mutual legal assistance should follow quickly. Use of INTERPOL channel for mutual legal assistance, Warsaw Convention and additional possibilities of the Budapest Convention, bilateral agreements and reciprocity approach should be considered.
- Confiscation
 - Questions arise in international cases related to mutual legal assistance in relation to different confiscation regimes and asset-sharing.

3.2.3 Financial investigation in the European Union

The 2016 Dutch presidency of the EU has identified the issue of targeting proceeds of crime and financial investigation as one of its priorities. A needs assessment on tools and methods of financial investigation in the European Union has been presented, as well as the 'six need-to-knows about financial investigation'⁴⁴.

The needs assessment⁴⁵ highlighted that:

- **Financial investigations may be applied to any proceeds generating crime:** it is not confined to fighting financial/economic crime, including money laundering, or collecting evidence principally for asset recovery.
- **Financial investigations may be conducted in all phases of criminal investigations and judicial proceedings:** from identifying criminality, developing intelligence, collecting evidence (case building), through to prosecution, conviction, and asset confiscation.

The 'six need-to-knows about financial investigation' highlighted also that as financial profit is often the main motivation for perpetrating crimes the proceeds are spent on goods and laundered into the economy frequently using legitimate companies and facilitators. Financial investigation is an additional investigative instrument in the law enforcement toolbox and can be deployed to get the leading individuals from a criminal organisation behind bars and to take away their money and assets. Depriving the leading people of their finances makes it very difficult for them to continue criminal activities. This makes financial investigation a very effective tool in disrupting organised crime and terrorism.

The 'need-to-knows' also highlights:

- **Financial Investigation can be applied to any type of crime:** financial investigation can and should be applied to all types of serious and organised crime such as human trafficking - and smuggling, fraud, drugs-and arms trafficking and terrorism. A general misconception is that financial investigation is confined to the fight against economic crimes such as fraud, tax crimes, corruption or money laundering.

⁴⁴ Brochure: The 6 need-to-knows about Financial Investigation, February 2016. Available at: <https://english.eu2016.nl/documents/publications/2016/02/10/brochure-the-6-need-to-knows-about-financial-investigation>

⁴⁵ Needs assessment on tools and methods of financial investigation in the European Union, ECORYS, December 2015. Available at: https://www.wodc.nl/binaries/2612-summary_tcm28-74130.pdf

- **Financial Investigation throughout criminal proceedings:** ideally, financial investigations are applied at all stages of criminal investigations and judicial proceedings. From a proactive identification of crime or criminal networks, to case investigations and evidence building, up until prosecution and conviction of offenders and asset confiscation. In many cases however, financial investigators are only brought into a criminal investigation at the final stage in order to trace, identify and confiscate the proceeds of crime. This is a missed opportunity. Financial investigations should start the earliest opportunity possible.
- **Wide-ranging financial awareness is essential:** financial awareness is needed at all levels of the law enforcement system - from basic financial awareness at community policing level to highly specialist forensic accountancy expertise needed to unravel the 'corporate veil' behind complex cross-border money laundering structures. It is important that criminal investigators are aware of the need to collect financial evidence at a crime scene and to call in specialist financial expertise when needed. Moreover, financial expertise among prosecutors and judges is crucial to understand and assess the files prepared by the financial investigators.
- **Cross-border cooperation is key to success in financial investigations:** investigators need to be familiar with both the informal exchange of information (CARIN, Europol, INTERPOL) avenues to pursue investigations and the formal e.g. Mutual Legal Assistance requests.
- **The importance of multidisciplinary cooperation:** when public authorities involved in financial investigations such as law enforcement, public prosecutors, Financial Intelligence Units (FIUs) and tax authorities combine their expertise, work together and share information, the best results are delivered. Moreover, there is an increasing awareness and wish that private parties such as banks, real estate agencies and other professional service providers could and should also provide valuable input in financial investigations.

SELF-REFLECTION QUESTIONS

1. What practical or legal obstacles, if any, can you envision that might prevent a financial investigation being carried out in parallel to a cybercrime investigation?
2. What practical or legal obstacles, if any, can you envision that might prevent the identification of criminal proceeds held in online or virtual forms?
3. At what point in criminal proceedings (investigation, judicial, etc.) can a financial investigation be initiated?
4. What conditions must be met before an order to freeze property can be granted?

4 Cross-border Cooperation

4.1 Summary

The Internet, besides its positive aspects, provides opportunities for abuse by criminals who can act in almost invisible ways, rapidly and anonymously, concealing their identity, evidence and traces of criminal profits. This characteristic represents a challenge for law enforcement agencies.

It is important to recognise the benefits of different possibilities for international cooperation by combining the three aspects of an online crime proceeds investigation: cybercrime investigation, parallel financial investigation and money laundering investigation⁴⁶. The Council of Europe Warsaw Convention and the Budapest Convention are important tools to address these aspects.

The Basic Course contains the presentation of the main aspects of international cooperation, such as the advantages of combining international cooperation avenues in the field of cybercrime and electronic evidence as well as financial investigation and money laundering prevention and investigation, distinguishing international cooperation on exchange of (operational) information from mutual legal assistance for evidential purposes, relevant international networks and organisations for exchange of information, relevant provisions of the Budapest and Warsaw conventions, etc.

At the same time, there are a number of challenges related to international cooperation and particularly to mutual legal assistance that need to be considered.

The Budapest and Warsaw conventions introduce avenues for international cooperation to be applied when combining parallel (cyber)crime investigation and financial investigation. However, international cooperation is facing specific legal and practical challenges, pertinent to each of the treaties, as a result of practical circumstances, such as the nature of electronic evidence, cloud technology, but also identification of proceeds of crime, seizure and confiscation of property abroad, taking into account different confiscation regimes and legal differences among parties. These challenges have been identified and addressed by relevant Council of Europe bodies, such as the Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC) and Cybercrime Convention Committee (T-CY).

When combining the aspects of cybercrime investigation, financial investigation and money laundering prevention and investigation it is useful to be aware of all these different aspects, the benefits and the existing challenges of the avenues for cooperation offered by the Budapest and Warsaw conventions.

While mutual legal assistance is still considered as the principal means to enforce court orders and to gather evidence abroad, the length of the procedure represents an important obstacle. However, the use of joint investigations and joint investigation teams might address some of the challenges of efficiency. Law enforcement (police and prosecutor) cooperation and exchange of information is indispensable in cross-border cases. Relevant international networks and organisations play an important role in this respect and also

⁴⁶ It should be noted however that despite the possible efficient tools to prevent and combat money laundering in several countries, the prosecution of money laundering is still a challenge.

help to build trust. The channels for cooperation and instruments offered by them are essential for exchanging information and evidence in criminal investigations.

4.1.1 Relevant Networks and Organisations for Exchange of Information and for Mutual Legal Assistance

International Cooperation – Exchange of (Operational) Information Police to police, prosecutor to prosecutor	
24/7 Network	Network (police and/or prosecutor contact points) Article 35 of Budapest Convention
EGMONT Group	Network of FIUs – money laundering prevention, postponement of suspicious transactions. Article 46 of Warsaw Convention
CARIN Network	Camden Asset Recovery Inter-Agency Network Network of experts for confiscation of proceeds of crime
INTERPOL	Channel for exchange of information and for transmission of MLA requests
Europol (EC3)	EU and relevant agreements with non-EU countries
Eurojust	European Judicial Cybercrime Network (2016) EU and relevant agreements with non-EU countries
International Cooperation – Mutual Legal Assistance (MLA) Formal cooperation – evidence	
MLA: formal cooperation, the result of an MLA request can be used as evidence in court. Usual channels of communication are through the designated central authorities, often Ministries of Justice or Ministry for Foreign Affairs.	
Direct cooperation: judge to judge, prosecutor to prosecutor (EU, bilateral agreements) Warsaw (Article 34) and Budapest (Article 27/9) conventions also provide for direct cooperation between responsible judicial and prosecution authorities in urgent cases, with formal request transmitted through the central authorities as well.	
Other options	JITs Parallel investigation Transfer of proceedings.

Criminals hide (or hold) their property abroad. In the investigation of online crime committed by international crime groups it is necessary to verify whether the offenders have any property abroad. In such cases **police and prosecutor cooperation** is very important. A contact person at foreign police can advise as to what data on property can be obtained from public sources, through police cooperation or by a letter rogatory. Such information can make the acquisition of data considerably easier and faster. Such cooperation is operational and execution of court orders is excluded.

Operational contacts and cooperation can lead also to establishment of joint investigation teams, which in principle can also facilitate a more effective mutual legal assistance

approach. It can also lead to arrangements of parallel investigations in cross border cases with more perpetrators and victims.

Mutual legal assistance is formal cooperation and the result of a request can be used as evidence in court. Usual channels of communication are through the designated central authorities, often Ministries of Justice. The possible channels can also be Ministry of Foreign Affairs or through INTERPOL, Europol or Eurojust in urgent cases.

Within the EU, mutual legal assistance is running directly between responsible authorities (prosecutor/court). Warsaw (Article 34) and Budapest (Article 27/9) conventions also provide for such approaches in urgent cases, with formal requests transmitted through the central authorities as well.

4.1.2 International Legal Instruments

Cybercrime	Financial Investigation
Council of Europe	
Budapest Convention on Cybercrime and Protocol on Xenophobia and Racism ⁴⁷	Warsaw Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism ⁴⁹
T-CY Guidance Notes ⁴⁸	1990 Strasbourg Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime ⁵⁰
EU	
Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA ⁵¹	Directive 2014/42/EU on the freezing and confiscation of instrumentalities of crime in the European Union ⁵²
Directive 2016/1148 of the European Parliament and of the Council of July 2016 concerning measures for a high common level of security of network and information systems (NIS Directive) ⁵³	Joint Action 98/699/JHA on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime ⁵⁴

⁴⁷ Convention on Cybercrime, ETS 185, 21.11.2001 and Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS 189, 28.01.2003.

⁴⁸ <https://www.coe.int/en/web/cybercrime/guidance-notes>

⁴⁹ Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CETS 198, 16.05.2005.

⁵⁰ Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, Strasbourg, ETS 141, 08.11.1990.

⁵¹ The Directive introduces new rules harmonising criminalisation and penalties for a number of offences directed against information systems. It also calls for EU countries to use the same contact points used by the Council of Europe and the G8 to react rapidly to threats involving advanced technology. Available at: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>

⁵² Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0042>

⁵³ NIS Directive available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG

Council of the European Union Conclusions on improving criminal justice in cyberspace and Conclusions on the European Judicial Cybercrime Network ⁵⁵ , June 2016	Framework Decision 2001/500/JHA on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime ⁵⁶
	Directive amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and amending Directive 2009/101/EC ⁵⁷
	Framework Decision 2005/212/JHA on confiscation of crime-related proceeds, instrumentalities and property ⁵⁸
	Framework decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence ⁵⁹
	Framework Decision 2006/783/JHA on the application of the principle of mutual recognition to confiscation orders ⁶⁰
	Council Decision 2007/845/JHA concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime – (introduced the obligation to establish Asset Recovery Office(s) (AROs)) ⁶¹

⁵⁴ To improve cooperation between European Union (EU) countries in the fight against organised crime, this joint action provides for the preparation, within the scope of operations of the European Judicial Network, of user-friendly guides on identifying, tracing, freezing or seizing and confiscating of instrumentalities and proceeds from crime. Available at: <http://eur-lex.europa.eu/legal-content/NLN/TXT/?uri=uriserv:l33073>

⁵⁵ The conclusions focus on: cooperation with service providers that allows for quick disclosure of data; less rigorous legal processes could be envisaged for obtaining specific categories of data, in particular subscriber data. Mutual Legal Assistance (MLA) procedures related to electronic data should be accelerated and streamlined; the volume of MLA requests between competent authorities could be reduced by enhancing cooperation with service providers. Mutual recognition procedures should be efficiently used to ensure effective securing and obtaining of e-evidence. Establishing connecting factors for enforcing jurisdiction in cyberspace, including in cases where the location of data is not (yet) known or volatile. Available at: <http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/>.

⁵⁶ Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (OJ L 182, 5.7.2001, p.1). Available at: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001F0500>

⁵⁷ It is aiming also at regulating virtual currencies by obliging providers of exchange services and custodial wallet providers to *inter alia* cooperate with their national Financial Intelligence Unit (FIU). Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0450:FIN%20>

⁵⁸ Council Framework Decision 2005/212/JHA of 24 February 2005 on confiscation of crime-related proceeds, instrumentalities and property (OJ L 68, 15.3.2005, p.49). Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0049:0051:en:PDF>

⁵⁹ Council Framework Decision 2003/755/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196, 2.8.2003, p.45). Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577>

⁶⁰ Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders (OJ L 328, 24.11.2006, p.59). Available at: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783>

⁶¹ The Decision establishes the requirements for the setting up of national Asset Recovery Offices (AROs) in EU countries. Available at: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0845>

	Directive 2014/41/EU on the European Investigation Order in criminal matters ⁶²
UN	
Resolutions on Combating the Criminal Misuse of Information Technologies (Resolutions 55/63 and 56/121) ⁶³	1988 UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances ⁶⁴
UN General Assembly Resolution 64/211 (March 2010) on the creation of a global culture of cybersecurity ⁶⁵	2000 UN Convention Against Transnational Organised Crime ⁶⁶
	2003 UN Convention Against Corruption ⁶⁷
Others (regional treaties)	
African Union Convention on Cyber Security and Personal Data Protection ⁶⁸	
Arab Convention on Combating Information Technology Offences ⁶⁹	
Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information ⁷⁰	
Shanghai Cooperation Organization Agreement in the Field of International Information Security ⁷¹	

Within the EU, the principle of mutual recognition, as opposed to mutual assistance, has been introduced since 2003 for the execution of freezing orders and in 2006 for confiscation orders. The scope to refuse the execution was also restricted with derogations to the principles of double criminality and double freezing. The EU has made further steps to facilitate cooperation by introducing the European Investigation Order.

4.1.3 Provisions on International Cooperation

International legal instruments deal with aspects of criminalisation of conduct, procedural (investigation tools) and international cooperation, including legal basis for mutual legal assistance (MLA). Warsaw and Budapest conventions provide for avenues that can be used and combined in order to achieve most effective results when conducting parallel financial and (cyber)crime investigation. Cooperation is subject to national provisions with safeguards for postponement or refusal of requests (Warsaw Convention, Section 5, Article

⁶² The European Investigation Order (EIO) directive sets up a comprehensive new system that allows EU countries to obtain evidence in other EU countries, for criminal cases that involve more than one country. Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041>

⁶³ Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf

⁶⁴ United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Vienna, 19.12.1988 (Article 5).

⁶⁵ Available at: <https://ccdcoe.org/sites/default/files/documents/UN-091221-CultureOfCSandCI.pdf>

⁶⁶ United Nations Convention Against Transnational Organised Crime, New York, 15.11.2000 (Articles 12-14).

⁶⁷ United Nations Convention Against Corruption, New York, 31.10.2003 (Articles 31, 54-57).

⁶⁸ <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

⁶⁹ http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences

⁷⁰ http://itlaw.wikia.com/wiki/Agreement_on_Cooperation_Among_the_States_Members_of_the_Commonwealth_of_Independent_States_in_Combating_Offences_Relating_to_Computer_Information

⁷¹ <https://ccdcoe.org/sco.html>

27 and Budapest Convention, Article 25/4 and 27/4 and 5). The main areas of cooperation are highlighted below:

Provisions on International Cooperation	
Budapest Convention	Warsaw Convention
Basic Principles	
<p>(Articles 23-25)</p> <p>The parties shall afford mutual assistance for the purpose of investigation or proceedings concerning:</p> <ul style="list-style-type: none"> - cybercrime (Articles 2-10) - or for the collection of evidence in electronic form of a criminal offence. 	<p>(Article 15)</p> <p>The parties shall mutually co-operate for the purpose of investigation and proceedings aiming at the confiscation of instrumentalities and proceeds.</p> <p>Request for:</p> <ul style="list-style-type: none"> - confiscation of specific items - or to pay a sum of money corresponding to the value of proceeds - and for investigative assistance and provisional measures with a view to confiscation.
Spontaneous Information	
<p>(Article 26)</p> <p>A Party may, within the limits of its domestic law and without prior request, forward to another party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this convention or might lead to a request for cooperation by that party under this chapter.</p>	<p>(Article 20)</p> <p>Similar provision</p>
Provisional Measures	
<p>(Articles 29-30)</p> <p>Expedited preservation of stored computer data.</p> <p>Expedited disclosure of preserved traffic data.</p>	<p>(Articles 21-22)</p> <p>Freezing or seizing, to prevent any dealing in, transfer or disposal of property and provide spontaneously all information relevant for provisional measure.</p>
Investigative Assistance	

<p align="center">(Articles 31-34)</p> <p>Mutual assistance regarding investigative powers:</p> <ul style="list-style-type: none"> - Access to stored computer data; - Trans-border access to stored computer data with consent or where publicly available; - Real-time collection of traffic data; and - Interception of content data. 	<p align="center">(Articles 16-19)</p> <p>Parties shall assist in the identification and tracing of instrumentalities and proceeds, which includes securing evidence as to the existence, location or movement, nature, legal status or value of the aforementioned property. Such assistance comprises also requests for:</p> <ul style="list-style-type: none"> - information on bank accounts; - on banking transactions; and - monitoring of banking transactions.
	<p align="center">Confiscation</p>
	<p align="center">(Articles 23-25)</p> <ul style="list-style-type: none"> - Enforce a confiscation order; or - submit the request to its competent authorities for the purpose of obtaining an order of confiscation and enforce it including request to pay a sum of money corresponding to the value of proceeds, or confiscation of a specific item of property.
	<p align="center">(Article 23/5)</p> <p>Measures equivalent to confiscation:</p> <ul style="list-style-type: none"> - non-criminal sanctions (non-conviction based confiscation); - rules for asset sharing (compensation to the victims, legitimate owners).
<p align="center">Networks for Cooperation</p>	
<p align="center">24/7 Network (Article 35)</p> <p>Each Party shall designate a point of contact available on a 24/7 basis, in order to ensure the provisions of immediate assistance for the purpose of</p> <ul style="list-style-type: none"> - investigations or proceedings concerning criminal offences related to computer systems and data, - or for the collection of evidence in electronic form of a criminal offence. <p>Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:</p> <ul style="list-style-type: none"> - the provision of technical advice; - the preservation of data (Article 29 and 30); 	<p align="center">FIU Cooperation (Articles 46-47)</p> <p>FIUs exchange, spontaneously, or on request, any accessible information that may be relevant</p> <ul style="list-style-type: none"> - To the processing or analysis of information, or - To investigation by the FIU regarding financial transactions related to money laundering and the natural or legal persons involved. <p>FIU power to postpone suspicious transactions.</p>

<ul style="list-style-type: none"> - the collection of evidence, - the provision of legal information, - and locating of suspects. 	
---	--

SELF-REFLECTION QUESTIONS

1. What conditions must be met before information can be spontaneously shared with another jurisdiction?
2. What grounds are available in your national legislation for a refusal to cooperate with an international request for assistance?
3. What conditions must be met to obtain an order to expedite disclosure of preserved traffic data?
4. What practical measures are in place to enable management, disposal and sharing of confiscated assets with another jurisdiction? Must these arrangements be made on a case-by-case basis?

4.2 Evaluations of the Application of Provisions on International Cooperation

It is important to take a note and understand the opportunities and obstacles to international cooperation in the area of financial and cybercrime investigations and electronic evidence as identified by international organisations.

4.2.1 Evaluation related to targeting crime proceeds

4.2.1.1 GENVAL

In the EU⁷², in the context of the fifth round of mutual evaluations of “financial crime and financial investigations”, the Working Party on General Matters including Evaluations (GENVAL) in its 2012 final report⁷³ highlighted key challenges pertaining to this area, namely:

1. Case management (including time and resource management) and cooperation between competent authorities, nationally as well as internationally,
2. Complicated and different legal rules and traditions, nationally and at the EU level, coupled with a sometimes weak implementation,
3. Evidence and the issue of electronic data, and
4. Time. Financial investigations often take a long time, and can cost a large amount of resources, in terms of time, manpower and financial means.

⁷²See also: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/financial-investigation/index_en.htm

⁷³ EU GENVAL 2012 Final report on fifth round of mutual evaluation – “Financial crime and financial investigations”. Available at: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202012%20REV%202>

The report contains also a number of recommendations to the Member States and the EU that could be relevant to any jurisdiction:

- Financial investigation should be carried out in all serious and organised crime cases (which include terrorism) beyond the sole economic and financial crime offences. An overarching, financial crime and financial investigations policy should therefore be drawn up, covering all relevant authorities, including prosecution, aimed at speeding up complex and lengthy investigations in the field of financial crime. It should reflect relevant priorities agreed at the EU level and set the basis for proactive investigations. More attention should be paid to potential profits from international cooperation, especially at EU level.
- The financial crime and financial investigations policy should be reflected in a long-term national strategy. Whenever possible, a concept of financial intelligence-led policing should be included in the strategy, to allow pro-active enforcement measures on the basis of analysis products. The strategy needs to be combined with a regular review and an evaluation methodology as well as a sound reporting mechanism for the entities involved. In setting up such a strategy, some basic criteria, rules or guidelines should be considered to clarify the allocation of tasks between different authorities with selective competencies, as well as the inclusion of key priorities including serious international crime cases. The strategy should thus be supported by sound management within the police, in order to promote a proactive, intelligence-led approach.
- The Member States should implement all EU legislation relating to mutual recognition and judicial cooperation in criminal matters. Moreover, a review of the implementation of the relevant Framework Decisions and application of mutual legal assistance mechanisms should be undertaken by the Member States and relevant EU agencies. Through this, the Member States should identify and tackle obstacles to efficient proactive data exchange with foreign law enforcement authorities, EU agencies and other relevant actors. Spontaneous exchange of information in line with Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between asset recovery offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, should be further enhanced and the use of Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU should be promoted.

4.2.1.2 PC-OC Questionnaire

The Council of Europe's Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC) focused its attention on the area of targeting crime proceeds in 2014. The replies to the PC-OC questionnaire⁷⁴ showed, among other, that there are differences among Parties in the application of the provisions of Strasbourg and Warsaw conventions, relevant for international cooperation.

Some of the aspects addressed in the questionnaire were:

- States are not always able to ensure the implementation of a request grounded on a so-called value-based confiscation system. This system is described in both

⁷⁴ Questionnaire on the use and efficiency of Council of Europe instruments as regards international co-operation in the field of seizure and confiscation of proceeds of crime, including the management of confiscated goods and asset sharing, PC-OC Mod (2015) 06Rev4, 19.5.2016. Available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680666607>

conventions as a system with which it is possible to co-operate besides the so-called object basis confiscation system. In both systems, a criminal conviction is necessary. In the value-based confiscation system, the criminal profits are calculated. Ultimately, on the basis of these calculations, the judge imposes an obligation to pay an amount of money which is equivalent to the criminal profits acquired. The confiscation order can then be executed on all assets belonging to the convicted person. In this regard, it is not required to prove that these assets have been obtained directly from the criminal offence.

- Several States recognise the possibility of seizure and confiscation of assets which belong *de facto* to the accused/convicted person but are legally considered as belonging to a third person, mostly a so-called straw man.
- Only some States are in a position to provide mutual legal assistance for the purpose of, or, related to non-conviction based confiscation and other measures (for instance civil forfeiture). This includes the information-gathering phase, during which criminal information is often requested for use within a NCB proceeding, search and seizure and confiscation of proceeds of crime.
- Some States are in a position to provide assistance in criminal, civil and administrative proceedings related to the liability of legal entities for the purpose of seizure or confiscation of proceeds of crime.
- Only some States are in a position to provide assistance in procedures related to virtual currencies such as bitcoins, especially as regards seizure and confiscation.

4.2.1.3 MONEYVAL

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL⁷⁵ is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems.

Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

Evaluation reports are published online.⁷⁶

4.2.2 Evaluation related to cybercrime

4.2.2.1 GENVAL

The seventh round of EU mutual evaluations is devoted to the practical implementation and operation of the European policies on prevention and combating cybercrime. The evaluation reports finalised have been made public and could serve other countries to review their legislation and strategy on cybercrime.⁷⁷

At the same time, the draft final report highlights some problematic aspects related to international cooperation, namely the average timeframe for answering an MLA request

⁷⁵ Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL):

http://www.coe.int/t/dghl/monitoring/moneyval/default_en.asp?expandable=0

⁷⁶ See: <http://www.coe.int/en/web/moneyval/jurisdictions>

⁷⁷ Adopted reports can be found at: <http://www.coe.int/da/web/octopus/blog/-/blogs/genval-evaluation-reports-on-cybercrime>

amounts to several months and may vary depending on whether the MLA is provided on the basis of an international agreement or of reciprocity. In the latter case, the response time is even longer. However, in view of the specificity of cybercrime, "the length of MLA proceedings makes MLA formal channels rather ineffective, with a negative consequence for the conduct and success of the investigations, as digital evidence is volatile and must be handled rapidly and efficiently, as delays can result in data being lost. There is consequently a general need to speed up the handling of MLA requests in cybercrime investigations". Also the draft report notes that international solutions to improve MLA procedures with third States should be found, for example using a form for requests of expedited production order agreed upon by executing authorities in a given state, was mentioned as best practice identified in one Member State. In the same vein, the development of informal and personal contacts with the competent authorities of third States prior to the sending of a MLA request was highlighted as a useful practice that might lead to a better and faster cooperation in the execution of such formal requests.⁷⁸

The following recommendations were put forward to Member States:

- Member States should improve the quality of the MLA requests they send to other countries, in particular to ensure they are sufficiently completed and examine methods of speeding up and enhancing the quality of responses to MLA requests.
- Member States are recommended to strengthen the effectiveness of the communication process with other Member States and third countries by establishing a MLA registration system and a MLA management system making it possible to follow a case from registration to the answer being sent to the requesting country.
- Member States are encouraged to make more frequent use of Eurojust, EJN and Europol tools and to develop informal contacts with the competent foreign authorities in order to obtain faster responses to MLA requests from third countries.
- The EU should consider coordinating efforts to establish an effective way of communicating and executing MLA requests from its Member States to non-EU countries, or establishing a framework for direct cooperation with relevant non-EU ISPs.
- The EU should work on solutions to improve and speed up the communication process between Member States and third countries, in particular the United States, specifically with regard to the exchange of operational information and to MLA requests and their execution.

4.2.2.2 T-CY

The Council of Europe Cybercrime Convention Committee (T-CY) is monitoring the implementation of the Budapest Convention on Cybercrime and develops further standards and guidance notes, aimed at facilitating the effective use and implementation of the Budapest Convention, also in the light of legal, policy and technological developments.

4.2.2.2.1 Mutual legal assistance

Mutual legal assistance remains the principal means to obtain evidence from foreign jurisdictions for use in criminal proceedings. In December 2014, T-CY completed an assessment of the functioning of mutual legal assistance provisions of the Budapest

⁷⁸ Draft Final report of the seventh round of mutual evaluations on "The practical implementation an operation of the European policies on prevention and combating cybercrime", June 2017. See pp. 82-88. Available at: <http://data.consilium.europa.eu/doc/document/ST-9986-2017-INIT/en/pdf>

Convention.⁷⁹ It concluded, among other things, that the mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence.

The Assessment Report furthermore concluded that not all types of data are needed with the same frequency or urgency: in terms of the type of data requested, subscriber information has been singled out as the most often sought information. The large amount of requests for such information puts a heavy burden on authorities responsible for processing and executing MLA requests and slows down – and often prevents – criminal investigations. This suggests that solutions to the challenge of subscriber information would render MLA more efficient.

The T-CY report identified the following problems encountered:

- Time, workload and the complexity of procedures required to prepare or execute MLA request
- Delays (6 – 24 months) in responses to requests in general or in relation to specific countries
- Delays in providing subscriber data
- Refusal to cooperate for “petty” offences by some countries
- Refusal to cooperate or no reply by some countries
- Problem of cooperation with 24/7 contact points
- No receipt that MLA request has been received or that data has been preserved
- Unclear criteria for “urgent” requests
- Problem of language, quality of translation, terminology used
- Requests received too broad, for a large amount of data
- Discrepancies between legal systems, such as regarding investigative powers
- Legal restrictions (data protection)
- Refusal of cooperation by foreign State without MLA request. However, MLA request requires sufficient information and evidence which cannot be obtained without cooperation by foreign State (vicious circle)
- Request may not meet legal threshold or formal requirements of the requested State or request not complete or threshold/standard required too high
- Inadequacy of laws
- Dual criminality requirement not met
- MLA request not preceded by preservation request to ensure that data is still available
- Data not preserved in foreign State in spite of preservation request
- Data not available anymore in foreign or own State
- Different policies by providers to make data available
- Contact person in emergency cases or the competent authority in foreign State not known Challenging to identity the authority concerns, e.g. web hosting provider
- Overburdened by too many requests
- Limited technical skills and understanding regarding electronic evidence in requested State.
- Limited power of judicial police

⁷⁹ T-CY(2013)17rev, 3 December 2014, T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime. Available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>

- “Probable cause” threshold.

The T-CY adopted a set of recommendations to make the MLA process regarding cybercrime and electronic evidence more efficient through more effective use of existing provisions of the Budapest Convention on Cybercrime and other agreements but also by proposing additional solutions⁸⁰, such as:

- Parties should fully implement the preservation powers of the Budapest Convention (Rec1), monitor the effectiveness of the MLA process (Rec 2), allocate more and better trained staff and more resources for MLA (Rec 3 and 4), strengthen the role and capacities of 24/7 points of contact (Rec 5), establish procedures for emergency situations (Rec 8) and so on.
- Parties should consider – possibly through a Protocol to the Budapest Convention – allowing for the expedited disclosure of subscriber information (Rec 19), the possibility of international production orders (Rec 20), direct cooperation between judicial authorities (Rec 21), addressing the practice of directly obtaining information from foreign service providers (Rec 22), joint investigations and/or joint investigative teams between Parties (Rec 23), allowing for requests to be sent in English language (Rec 24).

4.2.2.2 Additional practical challenges

Some additional challenges and aspects, related also to the international cooperation, will be further elaborated:

Conditions to access content data from the live suspect’s computer, even if data is stored abroad, and related question of consent and jurisdiction

In the final report of the T-CY Cloud Evidence Group (CEG) on Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY⁸¹ it was noted that as a rule, law enforcement powers are normally determined by the principle of territoriality. Under this principle, no state may enforce its jurisdiction in the territory of another sovereign state. Criminal justice access to data on servers or computer systems in general located in other jurisdictions without the involvement of the authorities of those jurisdictions raises concerns.

However, in situations where a computer on a crime scene or of a person being investigated is “live” (that is operating and active), criminal justice authorities could technically access data (including those stored on cloud servers) without knowledge of the jurisdiction in which the server is located and the data is stored. Article 32b of the Budapest Convention offers a solution only for very limited situations as described in the Guidance Note adopted by the T-CY in December 2014.⁸²

Due to the limitations of the Article 32b of the Budapest Convention (voluntary consent of suspect to access the email account during “live” investigation) some states pursue

⁸⁰ See pp. 125-127 of the T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime.

⁸¹ T-CY (2016)5, 16 September 2016, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY. Available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>

⁸² T-CY Guidance Note # 3 on Transborder access (Article 32), 3 December 2014, Available at: <https://rm.coe.int/16802e726a>

unilateral solutions in practice. It seems to be widespread practice that law enforcement in a specific criminal investigation access data not only on the device of the suspect but also on connected devices such as email or other cloud service accounts if the device is open or the access credentials have been obtained lawfully even if they know that they are connecting to a different, known country.

CEG looked into the long-arm doctrine of EU anti-trust law (Cases *ICI* 48/69; *Woodpulp* 89/85) and noted that the European Commission recommend that competition authorities within the European Union shall obtain access to servers anywhere in the world to gather evidence in anti-trust proceedings. To have effective powers to gather electronic evidence, it is important that authorities are able in the exercise of their inspection powers gather digital information which is accessible to the undertaking or person whose premises are being inspected irrespective of where it is stored, including on servers or other storage media located outside the territory of the respective national competition authority or outside the European Union. Conditions and safeguards for such access to data should be defined in a protocol.

CEG concluded that a framework on transborder access will need to define conditions and safeguards for such access to data in order to protect the rights of individuals and prevent prejudice to the powers or rights of other governments or their subjects.

Access to subscriber data

Subscriber data is less privacy sensitive, and most frequently requested. The police or prosecutor production order suffice in many states, however some of them require court order in case of dynamic IP, as some traffic data is included.

The final report of CEG on Criminal justice access to electronic evidence in the cloud therefore recommended:

- As subscriber information is less privacy sensitive than traffic data and content data, conditions for production orders for subscriber information should be subject to lesser safeguards than for other types of data or for other types of intrusive powers.
- A lighter regime for the production of subscriber information will facilitate domestic investigations and international cooperation in a cloud context.

Conditions to use a domestic production order (Article 18 of the Budapest Convention) for subscriber data in case of multinational service providers, offering service in the territory of a state, regardless of its seat abroad and location of data, have been explored.

A criminal justice authority can either establish jurisdiction to enforce by focusing on the location of the computer system or storage device (this is covered by the search and seizure provisions of Article 19 of the Budapest Convention) or of the natural or legal person (including service providers) in possession or control of the data sought.⁸³ The latter is covered by Article 18 on production orders.

Mutual legal assistance presupposes that the location of the data sought is known and that it is thus feasible and known to which State and to which competent authority to address an MLA request. However, it is often not obvious for criminal justice authorities in which jurisdiction the data is stored and/or which legal regime applies to data. A service provider may have its headquarters in one jurisdiction and apply the legal regime of a second

⁸³ See for example, European Union Directive 2016/1148 on the security of network and information systems ("NIS Directive") of 6 July 2016, Article 18 Jurisdiction and territoriality.

jurisdiction while the data is stored in a third jurisdiction. Data may be mirrored in several or move between jurisdictions. If the location of data determines the jurisdiction, it is conceivable that a cloud service provider systematically moves data to prevent criminal justice access.

As the Internet has no borders as such, subscriber information needed in an investigation may be held by a service provider “offering its services in the territory” of a Party although the provider may actually be located and the information sought may be stored on servers in other jurisdictions.

The CEG is of the opinion that a logical interpretation of Article 18.1.b of the Budapest Convention offers a solution. The competent authorities of a Party should be able to request subscriber information from a service provider offering a service in its territory irrespective of where the information is stored and where the provider is located. The Guidance Note # 10 on Production orders for subscriber information⁸⁴ that was adopted by T-CY promotes such interpretation and application of Article 18 of the Budapest Convention. Such application effectively avoids the MLA request.

The Guidance Note highlights that Article 18.1.b order can be applied in specific cases with regard to specified subscribers, if the service provider is in possession or control of the subscriber information and if the service provider is “offering a service in the territory of the Party”, that is when:

- The service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services); and
- orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), or makes use of the subscriber information (or associated traffic data) in the course of its activities, or interacts with subscribers in the Party and
- the subscriber information to be produced is relating to services of a provider offered in the territory of the Party.

Also the decision of the Supreme Court of Belgium confirmed such an interpretation by ruling that the service provider operating on the territory of a state is subject of and bound by applicable national legislation. The Supreme Court of Belgium in the case of Yahoo!⁸⁵ ruled that an order for the production of subscriber information to a provider offering and thus being “present” in the territory of a Party is a domestic order (as is Article 18.1.b) and not a matter of international cooperation or exercise of extra-territorial jurisdiction. Yahoo! Inc. had appealed against an earlier decision of the Court of Appeals of Antwerp of 20 November 2013, among other reasons that under international customary law a State has no extraterritorial jurisdiction to enforce.

The Belgian Supreme Court ruled that:

- In general, a State can enforce coercive measures only on its own territory and would otherwise violate the sovereignty of another State.

⁸⁴ Guidance Note #10: Production orders for subscriber information (Article 18 Budapest Convention), adopted by written procedure by T-CY on 28 February 2017. Available at: <https://rm.coe.int/doc/09000016806f943e>

⁸⁵ Supreme Court of Belgium ruling in the case of *Yahoo!* On 1 December 2015, the Belgian Supreme Court issued a final decision that Yahoo! Inc. registered in California, USA, is obliged to produce subscriber information and is thus subject to the coercive measure of Article 46bis of the Belgian Rules of Criminal Procedure.

Available at in Dutch: http://iure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1

- "A State imposes a measure of coercion on its own territory as far as there is, between that measure and that territory, a sufficient territorial link."
- Article 46bis §2 of the Belgian Rules of Criminal Procedure "only intends to enforce upon operators and suppliers active in Belgium a measure with a view to obtain mere identification data on the occasion of a crime or offence, the investigation of which falls within the competency of the Belgian prosecution authorities. This measure does not require a presence abroad of the Belgian Police or Magistrates, nor of agents acting on their behalf. This measure neither requires any material action or act abroad. The measure therefore has a restricted scope and bearing, the execution of which does not require any intervention outside of Belgian territory".
- Yahoo! Inc., "as a supplier of a free webmail service, is present on Belgian territory and voluntarily subjects himself to Belgian law as he actively participates in Belgian economic life, by specifically using the domain name 'www.yahoo.be', the use of the local language, showing publicity based on the location of the users of his services and his reachability in Belgium for these users by installing a complaint box and FAQ desk."
- "The Public Prosecutor does not require anything in the United States from an American subject, but requires something in Belgium from an American subject offering services on Belgian territory".
- There was, therefore, no exercise of extraterritorial jurisdiction.

Direct cooperation with multinational service providers

Cooperation with the USA is of particular importance as many of multinational service providers have their seat there and the number of MLA requests is increasing. The final report of CEG on Criminal justice access to electronic evidence in the cloud highlights that US service providers may disclose subscriber information and traffic data to foreign authorities based on legal request and that this is in line with the intent of Article 18.1.b of the Budapest Convention. However, it noted that the volatility of provider policies⁸⁶ and unpredictability of disclosure leads to lack of foreseeability for law enforcement as well as customers and raises issues related to rule of law.

In case of European providers such cooperation is not possible due to data protection rules and the MLA request has to be presented.

US service providers accept requests for preservation of any data directly received from foreign authorities in the expectation that this will be followed by a request for disclosure via MLA. European providers do not accept preservation requests received directly from law enforcement authorities in other jurisdictions.

Emergency procedures

Recommendation 8 of the T-CY Assessment Report on mutual legal assistance states that Parties are encouraged to establish emergency procedures for requests related to risks of life and similar exigent circumstances. A survey conducted by the CEG⁸⁷ in 2016, in which 33 States participated, shows that:

⁸⁶ For an overview of various providers' policies see Criminal justice access to data in the cloud: cooperation with "foreign" service providers, T-CY Cloud Evidence Group, May 2016. Available at: <https://rm.coe.int/168064b77d>

⁸⁷ Emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers, T-CY Cloud Evidence Group, May 2016

- The majority of Parties do not have legislation in place permitting disclosure of data to domestic criminal justice authorities in emergency situations;
- less than 20% have procedures in place permitting domestic competent authorities to disclose data to foreign authorities in an expedited manner;
- only two Parties permitted service providers in their territory to disclose data to foreign competent authorities in emergency situation.

The CEG proposed to address Recommendation 8 also through a Protocol to the Budapest Convention.

Additional Protocol to the Budapest Convention

CEG recommended starting negotiation of an additional Protocol to the Budapest Convention on Cybercrime in order to allow for more effective mutual legal assistance, to facilitate direct cooperation with service providers in other jurisdictions when needed and subject to conditions and safeguards, to frame and establish conditions and safeguards regarding existing practices of trans-border access to data and to establish data protection requirements.

A Protocol to the Budapest Convention might:

- Clarify the procedures and conditions for direct cooperation with service providers in other jurisdictions, and the admissibility of data received in criminal proceedings;
- Establish a legal basis for direct preservation requests to foreign service providers. This is already a practice accepted by US service providers;
- Provide for emergency procedures permitting direct cooperation with service providers in foreign jurisdictions in specific exigent situations.

Possible elements of a Protocol:

- Provisions for more effective mutual legal assistance:
 - a simplified regime for mutual legal assistance requests for subscriber information;
 - international production orders;
 - direct cooperation between judicial authorities in mutual legal assistance requests;
 - joint investigations and joint investigation teams;
 - requests in English language;
 - audio/video hearing of witnesses, victims and experts;
 - emergency MLA procedures.
- Provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests.
- Clearer framework and stronger safeguards for existing practices of transborder access to data.

- Safeguards, including data protection requirements.

The Terms of Reference for the preparation of a draft 2nd Additional Protocol to the Budapest Convention on Cybercrime were adopted at the 17th plenary of the T-CY in June 2017.⁸⁸

4.3 Use of Templates and Forms for Mutual Legal Assistance

MLA requests vary, even if they are based on international legal instruments, as they depend on national legislation of the sending State as well as the legislation and practical expectations of the receiving State. Forms for MLA request might help States to a certain extent and therefore some efforts have been made to develop model templates.

The Council of Europe Committee PC-OC developed, in 2016, a Model request form for mutual assistance in criminal matters⁸⁹.

T-CY in its 2014 Assessment Report on the mutual legal assistance provisions of the Budapest Convention on Cybercrime in Recommendation 17 stated that the Council of Europe should – under capacity building projects – develop or link to standardised multi-language templates for Article 31 requests⁹⁰.

EU Council conclusions on improving criminal justice in cyberspace (June 2016) called, among others, on the Commission, in association with Member States, Eurojust and third countries, to consider and make recommendations on how to adapt, where appropriate, existing standardised forms and procedures to request the securing and obtaining of e-evidence.

An example of a form for confiscation order can be found in the Council Framework decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders⁹¹.

Another example is Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters⁹².

Finally, the UNODC has developed a Mutual Legal Assistance Request Writer Tool⁹³.

It is evident that traditional MLA approaches are not adequate any more in a global world with online crime. Awareness of the possibilities and challenges under both instruments of the Council of Europe: the Budapest Convention (e.g. access to data in the cloud) and the

⁸⁸ T-CY(2017)3 Terms of Reference for the preparation of a draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, June 2017. Available at: <https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-protocol/168072362b>

⁸⁹ See the documents from 69th meeting (May 2016): Draft model request form on MLA and practical guidelines for practitioners: <http://www.coe.int/en/web/transnational-criminal-justice-pcoc/pc-oc-69th-meeting>
<http://www.coe.int/en/web/transnational-criminal-justice-pcoc/model-request-form-for-mutual-assistance-in-criminal-matters>

⁹⁰ The mutual legal assistance provisions of the Budapest Convention on Cybercrime, 3.12.2014 (T-CY(2013)17rev).
(<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>)

⁹¹ <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006F0783&from=EN>

⁹² <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041>

⁹³ <https://www.unodc.org/mla/en/index.html>

Warsaw Convention (execution of freezing and confiscation orders) will contribute to better results when combining the cybercrime investigation and parallel financial investigation.

5 Virtual Currencies

Cryptocurrencies, specifically Bitcoin, remain the currency of choice for much of cybercrime, whether it is used as payment for criminal services or for receiving payments from extortion victims. Even so, key members of the Bitcoin community, such as exchangers, are increasingly finding themselves the victim of cybercriminals⁹⁴. Following on from the introduction to virtual currencies that was provided in the basic course, the advanced course provides some more detailed information about the operation of virtual currencies (Bitcoin in particular) and a discussion of the risks associated with the use of these virtual currencies. The section concludes by introducing some of the investigative and freezing/seizing challenges that have been experienced with virtual currencies.

5.1 Basic Course Recap

Based on the FATF definitions⁹⁵, the basic course defined the following terms and categories relating to virtual currencies:

- Virtual currency
- Electronic money/e-money
- Digital currency
- Convertible vs. non-convertible virtual currency
- Centralised vs. decentralised virtual currency

These terms are be recapped in the table below.

Virtual Currency	"A virtual currency is a digital representation of value that can be traded on the Internet and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction"
Electronic money/e-money	"Virtual currency is also distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency."
Digital currency	"Digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and is thus often used interchangeably with the term virtual currency."
Convertible vs. non-convertible virtual currency	Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency. Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, and under the rules governing its use, cannot be exchanged for fiat currency.
Centralised vs. decentralised virtual currency	Centralised virtual currencies have a single administrating authority (administrator) – i.e. a third party that controls the system. An administrator issues the currency, establishes the rules for its use, maintains a central payment ledger, and has authority to redeem the currency (withdraw it from circulation). Decentralised virtual currencies are distributed, open-source,

⁹⁴ The Internet Organised Crime Threat Assessment (IOCTA) 2016, Europol. Available at: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>

⁹⁵ FATF Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

math-based peer-to-peer virtual currencies that have no central administrating authority and no central monitoring or oversight.

5.2 Introduction to Virtual Currencies

5.2.1 More Virtual Currency Terminology⁹⁶

Cryptocurrency	Refers to a math-based decentralised virtual currency that is protected by cryptography – i.e. it incorporates principles of cryptography to implement a distributed, decentralised secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the “block reward” and in some cases, also transaction fees paid by users as an incentive for miners to include their transactions in the next block). Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof-of-work system to validate transactions and maintain the block chain. While Bitcoin provided the first fully implemented cryptocurrency protocol, there is growing interest in developing alternative, potentially more efficient proof methods, such as systems based on proof-of-stake.
Bitcoin	Launched in 2009, was the first decentralised convertible virtual currency, and the first cryptocurrency. Bitcoins are units of account composed of unique strings of numbers and letters that constitute units of the currency and have value only because users are willing to pay for them. Bitcoins are digitally traded between users with a high degree of anonymity and can be exchanged (purchased or cashed out) into US dollars, Euros, and other fiat or virtual currency.
Etherum	The only cryptocurrency (with the exception of its fork Ethereum Classic) that includes a complete programming language. This can be used to create smart contracts – self-executing scripts, where a payment is sent after pre-determined conditions are met.
Altcoin	Refers to math-based decentralised convertible virtual currency other than bitcoins, the original such currency. Examples include Ripple, PeerCoin, Lite-Coin, zerocoin, anoncoin and dogecoin.
Monero	Created in April 2014, is an open-source cryptocurrency that provides arguably the highest amount of privacy using several technologies which render traditional tracing ineffective as both sending and receiving addresses are obfuscated. The transaction amount is hidden. Privacy features of transactions are provided by default.
Node	A client that propagates transactions across the bitcoin network to

⁹⁶ FATF Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

	other nodes.
Private key	The secret key allows to carry on bitcoin transactions and is used to create a signature for a transaction that cannot be forged. The owner of the private key controls the bitcoins.
Public key	A publicly known key derived from the private key.
Bitcoin transaction	Bitcoins are moved from one address to another. When carrying out a transaction the user uses a Bitcoin wallet installed on his computer or an online service offering the relevant functionalities. A Bitcoin transaction is a one-off transaction that cannot be reversed. Bitcoin transactions are transparent and can be viewed on the internet in various ways. Data can be viewed such as the sender's Bitcoin address, the recipient's Bitcoin address and the amount of bitcoins involved in the transaction.
Seizure	Movement of bitcoins from a suspect's addresses to an address controlled by law enforcement.
Anonymiser (anonymising tool)	Refers to tools and services designed to obscure the source of a Bitcoin transaction and facilitate anonymity.
Mixer (laundry service, tumbler)	Is the name given to a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that make it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular Bitcoin address. The mixing service then "comingles" this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed.
Tor (The Onion Router)	Is the name given to an underground distributed network of computers on the Internet that conceals the true IP address, and therefore the identities of the network's users by routing communication through multiple computers around the world and wrapping them in numerous layers of encryption.
Dark Wallet	Is the name given to a browser-based extension wallet that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymiser (mixer), decentralised trading, uncensorable crowd funding platforms, stock platforms and information black markets and decentralised market places similar to Silk Road.
Cold Storage	Refers to an offline Bitcoin wallet – i.e. a Bitcoin wallet that is not connected to the Internet. Cold storage is intended to help protect the stored virtual currency against hacking and theft.
Hot Storage	Refers to an online Bitcoin wallet, by contrast with Cold Storage.
Local Exchange Trading System (LETS)	Is a locally organised economic organisation that allows members to exchange goods and services with others in the group. LETS use a locally created currency to denominate units of value that can be traded or bartered in exchange for goods and services. Theoretically Bitcoins could be adopted as the local currency used with a LETS.

5.2.2 Virtual Currency Participants

Exchanger (also known as a virtual currency exchange)	Is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa for a fee (commission). Exchangers generally accept a wide range of payments including cash, wire transfers, credit cards and other virtual currencies and can be administrator-affiliated, non-affiliated or a third party provider. Exchangers can act as a bourse or an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.
Administrator	Is a person or entity engaged in the business of issuing (putting into circulation) a centralised virtual currency, establishing the rules for its use, maintaining a central payment ledger, and who has the authority to redeem (withdraw from circulation) the virtual currency.
User	A person or entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment.
Miner	Is a person or entity that participates in a decentralised virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system. Miners may be users if they self-generate convertible virtual currency solely for their own purposes. Miners may also participate in a virtual currency system as exchangers, creating the virtual currency as a business in order to sell it for fiat currency or other virtual currency.
Virtual currency wallet (client)	Is a means (software application or other) for holding, storing and transferring bitcoins or other virtual currency.
Wallet provider	Is an entity that provides a virtual currency wallet for holding, storing and transferring bitcoins or other virtual currency. A wallet holds the user's private keys, which allows the user to spend virtual currency allocated to the virtual currency address in the blockchain. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers and merchants to more easily conduct the virtual currency transactions. The wallet provider maintains the customer's virtual currency balance and generally also provides storage and transaction security.

Various other entities may also participate in a virtual currency system and may be affiliated with, or independent from, exchangers and/or administrators. These include, *inter alia*, web administration service providers (i.e. web administrators), third party payment processors (facilitating merchant acceptance), software developers and application providers.

5.2.3 Bitcoin

Bitcoin is a decentralised, peer-to-peer payment network that is powered by its users with no central authority or middlemen. Satoshi Nakamoto published the first Bitcoin

specification and proof of concept to a cryptography mailing list in 2009⁹⁷. Fundamentally, the purpose and operation of the Bitcoin network is concerned with the management and sharing of a public ledger, known as the “blockchain”. This ledger contains every transaction ever performed and is used to verify the validity of every transaction⁹⁸. The integrity and chronological order of the transactions in the ledger are enforced by cryptography. Bitcoins are a convertible, decentralised virtual currency, also commonly known as a cryptocurrency.

This section provides a description of how the Bitcoin virtual currency works.

5.2.3.1 Transferring Value

The most obvious question about a virtual currency is how do users of the currency transfer value to one another. In the case of Bitcoin, each user has one or more Bitcoin addresses. A user can create as many Bitcoin addresses as they want, even a separate address for every single transaction if they want. In practice, Bitcoin software and services represent a user’s bitcoins as being stored in a “wallet”. A wallet may represent a single Bitcoin address or multiple addresses depending on the specific features of that software or service. The address serves as a unique identifying value that is used to represent ownership of a particular Bitcoin⁹⁹. For Person A to send money to Person B, they broadcast a message to the Bitcoin network containing the sender address ID, the recipient address ID (the “receiving address”) and the amount of the transfer in bitcoins. Every node in the Bitcoin network that receives this message will update their copy of the ledger and then pass along the transaction message to other nodes.

To prevent an attacker, Person C, from broadcasting a message attempting to transfer bitcoins from Person A’s wallet to Person C’s wallet, the authenticity of the transactions is assured due to the presence of a digital signature by Person A. In order to create a valid transaction message transferring bitcoins from Person A’s wallet, the person generating the message must have the password associated with the private key of the wallet.

5.2.3.2 Proving Ownership

How does the recipient, Person B in the example above, know that the bitcoins being received actually belonged to Person A? In order to construct a valid message to transfer bitcoins, the sender of the bitcoins must prove that they are the current owner of those bitcoins.

Suppose Person A is sending five bitcoins to Person B. Person A must include in the transaction, references to previous transactions where the recipient of the transaction was Person A and the total value of the previous transactions was greater than five Bitcoins. These are referred to as the “inputs” to the transaction.

All users of the Bitcoin network maintain a copy of the ledger (“block chain”) that contains the history of all previous transactions. Person B can then verify that the bitcoins referenced in the inputs to Person A’s transaction indeed belong to Person A. To simplify this process, there is a rule that transactions must balance. In other words, the number of bitcoins in the “inputs” to a transaction must equal the number of Bitcoins in the “outputs”

⁹⁷ <https://bitcoin.org/en/faq>

⁹⁸ <https://bitcoin.org/en/how-it-works>

⁹⁹ Strictly speaking, each address is a public/private key pair. The public key is the “address”. The private key is kept secret and is used to digitally sign transactions involving the address and thus to verify the authenticity of the transaction.

of the transaction. If there is an imbalance, Person A can transfer the remaining balance of the inputs to themselves.

5.2.3.3 Double Spending

In a peer-to-peer network like the Bitcoin network, there is no guarantee that the order in which the transactions are received by any particular node in the network represents the same order in which they were created. In practical terms this introduces the possibility of Person A creating a transaction message sending bitcoins to Person B and then simultaneously creating a second transaction message to send Bitcoins to someone else. This is known as double spending. It is entirely possible that some nodes in the Bitcoin network will receive the second transaction first. When the first transaction arrived at these nodes, sometime later, it would be considered invalid because it reuses inputs that have already been used, from their perspective, in another transaction. The key technological advance of the Bitcoin protocol is the mechanism by which this issue is resolved.

Transactions are assembled into groups, known as blocks, and the blocks are linked together to form a block chain. Transactions within a block are considered to have happened at the same time. The blocks are ordered by virtue of the fact that each block refers to the previous block in the chain. Transactions that are not already in a block are called “unconfirmed”. Any node in the network can collect a set of unconfirmed transactions, assemble them into a block and propose them as the next block in the chain. The proposed block must contain the solution to a complex mathematical problem that is computationally difficult to calculate¹⁰⁰. The Bitcoin network dynamically adjusts the difficulty of the mathematical problem so that a new block is added to the block chain on average once every ten minutes¹⁰¹.

Although it is unlikely, it may happen that multiple nodes in the Bitcoin network may propose blocks at around the same time. In this case the blockchain temporarily branches as different nodes in the network append different blocks to the blockchain. The situation is resolved when the next block is added to the chain. As mentioned already, the new block will contain a reference to the previous block in the chain. It will therefore be appended to one of the two possible branches in the blockchain, making one branch longer than the other. The rule of the Bitcoin network is that nodes must switch to the longest available branch and the result is that very quickly the blockchain will stabilise. Further, all nodes will agree on all blocks that are a few back from the end of the chain. It is therefore considered safer to wait a period of time before, say, shipping goods based on a transfer of bitcoins. Since each block takes approximately ten minutes to be added to the chain, waiting for six blocks would mean waiting an hour.

5.2.3.4 Mining

The process described above of building blocks and appending them to the blockchain is known as mining. Whoever solves the block and appends it to the blockchain receives a reward of 25 bitcoins. Every few years the block reward is cut in half until eventually no more bitcoins will be released. A total of 21 million bitcoins will be created.

¹⁰⁰ The node creating the block must find a numeric value that, when combined with the other data of the block, gives the resulting combined data a cryptographic hash with a value below a certain threshold.

¹⁰¹ This is achieved by reducing the threshold value in the hash calculation, meaning there is a smaller number of acceptable answers and thus making the identification of a valid value more difficult.

In addition to the bitcoin reward, miners can also receive a transaction fee that can optionally be included with transactions. Currently the main reward for mining is the block reward but over time transaction fees will become the incentive for mining.

Most mining is not performed by individuals but rather by organised groups of miners, known as mining pools. The reward for computing blocks is divided amongst the members of the pool in proportion to the amount of computational effort each member provided to the pool.

5.3 Virtual Currency Risks

Convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering and terrorist financing abuse for many reasons. This section will describe the risks that have been enumerated with regards to both of these two threats to financial integrity¹⁰².

First, they may allow greater anonymity than traditional noncash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified. Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity.

There is no central oversight body and no anti-money laundering software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or more established online payment systems, such as PayPal. The global reach of virtual currencies likewise increases its potential money laundering/terrorist financing risk.

Virtual currency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for money laundering/terrorist financing compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralised virtual currency technology and business models, including the changing number and types/roles of participants providing services in virtual currency payments systems. Importantly, components of a virtual currency system may

¹⁰² An excellent document has been prepared by the European Banking Authority (EBA), enumerating the risks to the financial system presented by virtual currencies. Available at: <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>

be located in jurisdictions that do not have adequate money laundering/terrorist financing controls. Centralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak money laundering/terrorist financing regimes. Decentralised convertible virtual currencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country.

The FATF risk assessment of virtual currencies¹⁰³ indicates that at least in the near-term, only convertible virtual currency, which can be used to move value into and out of fiat currencies and the regulated financial system, is likely to present money laundering/terrorist financing risks. Accordingly, under the risk-based approach described in the referenced report, countries should focus their money laundering/terrorist financing efforts on higher-risk convertible virtual currencies.

The risk assessment also suggests that money laundering/terrorist financing controls should target convertible virtual currency nodes—i.e., points of intersection that provide gateways to the regulated financial system—and not seek to regulate users who obtain virtual currency to purchase goods or services. These nodes include, inter alia, third-party convertible virtual currency exchangers. Where that is the case, they should be regulated under the FATF Recommendations¹⁰⁴. Thus, countries should consider applying the relevant anti-money laundering/counter-terrorist financing requirements specified by the international standards to convertible virtual currency exchangers, and any other types of institution that act as nodes where convertible virtual currency activities intersect with the regulated fiat currency financial system.

Under the FATF's risk-based approach, countries could also consider regulating financial institutions or other designated entities that send, receive, and store virtual currency, but do not provide exchange or cash-in/cash-out services between virtual and fiat currency.

The amended to the 5th Anti-money Laundering Directive¹⁰⁵ will bring virtual currency exchange platforms and wallet providers under the ambit of anti-money laundering regulations imposed by the Directive defining 'obliged entities'.

SELF-REFLECTION QUESTIONS

- 1. Where does the exchange from virtual currency to real currency take place?**
- 2. How are parties to a transaction identified in the Bitcoin virtual currency system?**
- 3. What fundamental feature of decentralised virtual currencies makes them**

¹⁰³ Virtual Currencies – Guidance for a risk-based approach, Financial Action Task Force, June 2015. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

¹⁰⁴ For avoidance of doubt, the FATF Recommendations – International standards on combating money laundering and the financing of terrorism and proliferation, Financial Action Task Force, February 2012. Available at: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

¹⁰⁵ http://www.consilium.europa.eu/register/en/content/out?typ=SET&i=ADV&RESULTSET=1&DOC_TITL=&CONTENTS=&DOC_ID=15849%2F17&DOS_INTERINST=&DOC_SUBJECT=&DOC_SUBTYPE=&DOC_DATE=&document_date_from_date=&document_date_to_date=&document_date_from_date_submit=&document_date_to_date_submit=&MEET_DATE=&meeting_date_from_date=&meeting_date_to_date_submit=&meeting_date_to_date_submit=&DOC_LANCD=EN&ROW_SPP=25&NRROWS=500&ORDERBY=DOC_DATE+DESC

difficult to regulate?

4. What is the name given to the public ledger of Bitcoin transactions?

5.4 Investigative challenges¹⁰⁶

5.4.1 Knowing that Virtual Currencies have been used

The first challenge presented by investigations involving virtual currencies is identifying the use of the virtual currency and/or whether criminal assets are being held in the form of virtual currency. In virtual currencies, the representation of value is almost always held in a totally electronic form¹⁰⁷.

Therefore, there must be awareness on the part of the investigators of the possibility that criminal funds have been converted into virtual currency. Digital forensic analysts must also have the technical capacity and capability to understand where/how to look for the use of virtual currency on seized electronic storage media.

5.4.2 Transaction Anonymity

Since the inception of distributed virtual currencies one frequently mentioned feature of their operation has been the purported anonymity of transactions. Therefore, perhaps the key investigative challenge involving Bitcoin is associating the activities of a particular Bitcoin wallet with a real-world individual.

Despite the fact that all Bitcoin transactions and wallet contents are visible for anyone to see in the blockchain, unless you have possession of the private key you cannot transfer Bitcoin to another account holder¹⁰⁸. However, the real-world individual who has possession of a particular private key is not revealed through the performance of a Bitcoin transaction.

Techniques have been identified that allow, in certain circumstances, IP addresses associated with particular transactions¹⁰⁹. One of the first identification techniques was described in an academic paper published by Philip and Diana Koshy in 2014¹¹⁰. They build their own version of Bitcoin software that downloaded a copy of every single packet of data transmitted by every computer on the Bitcoin network. Through analysis of this data the Koshys were able to identify certain patterns of data that allowed identification of the IP addresses behind particular Bitcoin transactions. However, for the time being, such techniques are not likely to be available to the majority of criminal investigations due to computational challenges they pose.

5.4.3 Identification of Source of Funds

¹⁰⁶ Note that the discussion that follows refers in places to Bitcoin as an example of a decentralized virtual currency. The challenges described here are applicable to the vast majority of virtual currencies, particularly decentralized virtual currencies.

¹⁰⁷ There are some organisations that sell physical representations of virtual currency value, but these are extremely uncommon and not widely used. See, for example <http://www.coindesk.com/10-physical-bitcoins-good-bad-ugly/>

¹⁰⁸ See Bitcoin case study above for a description of how Bitcoin works.

¹⁰⁹ <http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin>

¹¹⁰ An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, Koshy et al
http://fc14.ifca.ai/papers/fc14_submission_71.pdf

In investigations where it has been established that virtual currencies have been used, it may be necessary in some cases to establish that the funds were obtained illegally. The suspect may be questioned on this point but in cases where the suspect is not cooperative and/or the suspect is not yet aware that they are under investigation, it may be difficult to establish how the virtual currencies were purchased.

In this context, the assistance from the private sector is crucial. Virtual currency exchangers that are compliant entities¹¹¹ would be able to provide information on individual clients, typically storing names, verified contact details, IP logs, activity logs, all virtual currencies addresses used by the user on the exchange, personal messages, payment information, a proof of ID and proof of home address.

The use of procedural powers provided by the Budapest Convention on Cybercrime would also allow access to data held by exchangers and other participants in the virtual currencies ecosystem (e.g. through preservation orders, real-time collection of traffic data, etc.)

The challenge of identifying the source of funds in a Bitcoin transaction is also made more difficult through the use of a mixing service. These services work by accepting transactions from multiple people, dividing the transferred funds into small amounts and mixing the funds together with funds transferred by other users of the service. This means that, from the perspective of the recipient of the funds, the original source of the funds is heavily obfuscated at least and potentially completely anonymised¹¹².

5.4.4 Cash out/realisation and conversion of proceeds

The point at which value represented in virtual currencies is converted to fiat currency, there is an opportunity for law enforcement. This conversion typically takes place in a virtual currency exchange, and hence the FATF recommendations concerning virtual currencies, briefly discussed and referenced in Section 5.3, focus on regulation of virtual currency nodes. "Nodes" in this context refers to points where the virtual currency world touches the traditional financial world, which includes, inter alia, virtual currency exchanges.

Where virtual currency exchanges are regulated they must undertake due diligence measures to identify their customers. In the specific case of Bitcoin, all transactions are publicly available on the block chain. This means that, in cases where law enforcement agencies are aware of a particular virtual currency address that is under the control of a suspect, it can be possible by analysing the transactions carried out by the suspect to identify the use of a specific virtual currency exchange. In these cases, law enforcement authorities can then serve a court order on the relevant virtual currency exchange to reveal the customer details such as an ID, home address, IP addresses, email addresses, phone number, transaction history, deposit and withdrawal addresses, bank name, bank account number and transaction information.

In January 2016, for example, ten men were arrested in the Netherlands as part of an international raid on online illegal drug markets. The men were caught converting their Bitcoins into Euros in bank accounts using commercial Bitcoin services, and then withdrawing millions in cash from ATM machines. The trail of Bitcoin addresses allegedly linked the money to online illegal drug sales tracked by FBI and Interpol. The FATF, in

¹¹¹ Compliant entities under anti-money laundering / counter terrorist financing legislation are not limited to virtual currency exchangers, payment-processing agents, online wallets, gaming sites and other online services can also assist investigations.

¹¹² https://en.bitcoin.it/wiki/Mixing_service

their 2014 report on virtual currencies ("Virtual Currencies: Key Definitions and Potential AML/CFT Risks"), provides examples of several other well-publicised law enforcement actions involving virtual currencies.¹¹³ An interested reader is encouraged to review these case studies for further insight into the scale and complexity of previous investigations involving virtual currencies.

However, as discussed elsewhere in this manual, challenges continue to remain due to the worldwide nature of virtual currencies. These challenges range from the fact that virtual currency exchanges are inconsistently regulated across the world to the practical difficulties associated with international investigations.

5.5 Freezing/seizing challenges

5.5.1 Virtual Currency as Proceeds of Crime

Many countries do not need to specify the nature of the proceeds of crime. In such cases, a store of value such as Bitcoin should be regarded as proceeds of crime if the proceeds were derived from criminal activity. However, this needs to be established in your particular jurisdiction.

5.5.2 Identifying the Existence of Virtual Currency

The first challenge is to identify the existence of the virtual currency and to establish that it is under the control by the suspect. Some of the issues arising here have already been discussed in Section 5.4. The existence and control of virtual currency may, for example, be apparent from surveillance, special investigative techniques or even admissions.

5.5.3 Freezing/Taking Control of Virtual Currency

Having identified that crime proceeds as held in the form of virtual currencies, the next question is then to immobilise the virtual currency and to prevent its dissipation. Part of the challenge with freezing virtual currency is their virtual nature, meaning that many copies of the virtual currency wallet may exist. Even in cases where an online wallet has been seized or a wallet held on a suspect's PC has been seized, this is not a basis for confidence that the virtual currency has been moved beyond the control of the suspect. It is not uncommon for a suspect to have backup keys/wallet held elsewhere in the cloud (internet storage space). Therefore, attempts to take control of a suspect's virtual currency wallet cannot give certainty that the assets have been moved beyond the suspect's control.

It has to be highlighted that virtual currencies are not stored on a device as such. In case of bitcoins, it is the private key that allows someone to spend them. There are two main ways to seize bitcoins, namely by gaining access to the suspect's private key or cooperation with the private sector (e.g., exchangers) that control the suspect's private key. Once investigators are in possession of the suspect's private key, to complete seizure, it is required to transfer the funds as the suspect or another person controlling the private key can move the funds to another address. These should be transferred into a Bitcoin address controlled by law enforcement (investigators or public prosecution). Note that procedure will depend on the existing national legislation.

¹¹³ FATF Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

A prosecutor may obtain a legal injunction or separate freezing order preventing the suspect or his agents from dissipating the virtual currency. This will not prevent agents located overseas, where the order may have no effect, from acting to move or dissipate the virtual currency.

If possible the prosecution should seek to liquidate the virtual currency balance as soon as possible (see Section 5.5.4). This requires timely execution of a process to take control of the assets, in case a suspect has access to a back copy of the target virtual currency wallet. Additionally, virtual currencies are often volatile in value and by acting to liquidate and place the balance in a government account you can be sure of preserving the value represented by the virtual at the time of investigation and make it available for eventual confiscation in the event of a conviction.

5.5.4 Asset Management

The recommended best practice is to liquidate the virtual currency store of value. This is based on the need to retain the value of the seized goods (e.g., as with the seized securities and foreign currency in cash). This preserves the value of the asset and insulates against volatility in the market. It also provides reassurance that the virtual currency cannot be moved, transferred or put beyond reach of the courts. Most jurisdictions have provision in their legislation to liquidate assets to preserve value for eventual confiscation but this would need to be established in your particular jurisdiction.

The EU Confiscation Directive¹¹⁴ recommends the establishment of an office to manage seized and confiscated assets¹¹⁵. If such an office is established in your jurisdiction, it may be worthwhile to familiarise yourself with the capabilities of this office to liquidate a store of virtual currency value. Alternatively, if such an office does not exist, the ability to liquidate virtual currency value will depend on the capacity of whatever arrangements are in place for managing assets prior to confiscation.

SELF-REFLECTION QUESTIONS

- 1. Why is it best practice to liquidate virtual currency as soon as possible?**
- 2. Is it necessary in your jurisdiction to establish the illegal source of specific criminal proceeds? If so, how might this be done in the case of virtual currency?**
- 3. What conditions must be met before an order to seize virtual currency can be obtained?**
- 4. What measures can be used to identify the existence or use of virtual currencies? What safeguards are in place to protect the interests of innocent third parties?**

¹¹⁴ Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union.

¹¹⁵ *Ibid* Preamble para 32.

6 Practical Work/Case Studies

6.1 Literature Search

Please provide a reference to the relevant articles of your national legislation and relevant jurisprudence, with a short description, concerning the following points:

1. Confiscation of crime proceeds as an obligation under the Criminal Code and Criminal Procedure Code/special law.
2. Definition of financial investigation, when should a financial investigation take place, who carries out a financial investigation?
3. Access to bank data and monitoring a bank account.
4. Definition and use of special investigative measures.
5. Access to other databases on ownership (land register, car register, etc.)
6. Freezing order.
7. Confiscation decision.
8. Confiscation regime (criminal procedure, value based confiscation, extended confiscation, presumption of imbalance, non-conviction (in-rem) based confiscation).
9. Mutual legal assistance.
10. Specialised institutions.
11. Creation of a Task force (prosecution, police, FIU, tax service, customs).
12. Access to subscriber data (IP address, web page, email account).
13. Access to traffic data and content data.
14. Preservation request.
15. Seizure of electronic evidence.

6.2 Case Study 1: Consideration of Legal Basis for Actions

Your national police have initiated an investigation against suspects A, B and C, who are forming an organised crime group to sell large quantities of marijuana to buyers, D and E.

Using covert measures (covert surveillance and telecommunications surveillance) it has been established that on 15th October 2016 person A delivered 1kg of marijuana to person D, who paid EUR1,000 cash in a suitcase. The postponement of the seizure and arrest has been authorised. On the same day, person A delivered the suitcase with the money to person B. It has further been established that person A has agreed by phone with person E to sell him 2kg of marijuana, for which EUR2,000 will be transferred into bank account number 11.

You decide you need to access the data on the holder of the bank account number 11, including the account holder and data on transactions for the last X months. Also, you decide you need to initiate monitoring of transactions for persons A, B and E accounts.

QUESTION: Describe the legal basis in your national legislation, referring to particular articles, and the conditions for access to bank data, data on transactions and monitoring of accounts.

Through this measure you identify that A, B and E all have bank accounts in your country. You also identify a bank account owned by person B in Austria.

You decide to seek a court order for bank data, transaction data and monitoring of account B in Austria and request mutual legal assistance in this matter.

QUESTION: Provide the legal basis in your national legislation, referring to particular articles, and conditions for mutual legal assistance.

Through analysis of bank accounts of A, B and E it becomes clear that there are frequent transactions between A and B, frequent transactions from E to B and also transactions from B abroad (to another country in the region and also to Luxembourg). You compare and correlate the dynamics of the transactions with the findings of the criminal investigation.

Phone surveillance reveals that B is negotiating with C, who resides between your country and another country in the region, on supply of a bigger quantity of marijuana in one month time on 15th December 2016. C is asking for advance payment, before 1st December 2016 of half of the price (EUR100,000) to bank account 22 (held by legal person DOO), the remaining EUR100,000 is to be paid to bank account 33, held in a bank in Luxembourg.

You decide to find data on the bank accounts of C in your country and in the other country in the region and put a monitoring order in place. You also decide to establish the ownership of the legal person DOO and its bank accounts and to order data on transactions for the last X months and monitoring of DOO's accounts.

QUESTION: Provide the legal basis in your national legislation, including references to articles, and conditions for access to data on legal persons, bank and transaction data of legal persons and tax records of legal persons.

With assistance of the tax service, you decide to establish how DOO conducts business and who the business partners are. You discover that DOO is also trading with industrial cannabis.

You request records for bank account 33 in Luxembourg and find that it belongs to a legal person in your country, owned by C.

QUESTION: Is there a suspicion of money laundering? At what point does the suspicion arise? Should you include the FIU in the investigation task force? What can the FIU help with? What possible money laundering typologies are in use here? Provide the legal basis, elements and conditions in your national legislation for money laundering. Provide the legal basis and conditions in your national legislation for engagement of the FIU.

Phone surveillance establishes that person B has been referring to email communication with person A that contain information about drug transactions and payments in Bitcoin.

You decide you need to identify the email addresses being used by person A and person B and the content of the emails. You determine that person A is using an email address that is provided by a local Internet Service Provider.

QUESTION: Provide the legal basis in your national legislation, including references to articles, and conditions for cooperation with ISPs and access to content of emails.

Through the content of A's email you identify drug transactions to D and E and others and also transfers of cash to bank accounts as well as transfers of value in Bitcoin.

You decide to engage the assistance of the FIU to analyse the bank transactions and seek links and data on holders of relevant accounts abroad (in Austria and Luxembourg as well as in other countries in your region).

QUESTION: Provide the legal basis in your national legislation, including references to articles, and conditions for access to bank data by the FIU and international FIU cooperation.

Through the investigation you identify that a payment is due in Bitcoin from person C to person B on 15 December 2016. You identify that person B's Bitcoin wallet is held by a Bitcoin exchange in Luxembourg.

QUESTION: Provide the legal basis in your national legislation, including references to articles, and conditions for requesting subscriber information from a Bitcoin exchange. Would a Bitcoin exchange in your country be obliged to hold data and cooperate?

QUESTIONS:

- What measures would you take regarding the planned payment on 1st December 2016 into account 22 of the legal person DOO?
- Would you order freezing of the transaction in advance? When is the freezing order disclosed? Would the freezing of the transaction on account DOO endanger the seizure of a large quantity of drugs foreseen for delivery on 15 December 2016?
- After the suspects are arrested, what measures would be taken in relation to the cash payment of 15th December 2016?
- Considering that the group A, B and C have been in the drug business for a long time, how much, and what assets can be confiscated? Provide the basis in your national legislation for your answer.
- Can the legal person DOO be charged with drug trafficking and/or money laundering? If so, provide a legal basis in your national legislation, and conditions for sentencing a legal person. Provide an example of a decision and argumentation relating to confiscation from a legal person.

By analysing the email communication between B and A, you discover that the group is selling drugs also through a specific web page in the darkweb. This is confirmed by one of the buyers who reveals during interrogation how the darkweb ordering and shipping of drugs is functioning and how payment I requested either to the bank account or by bitcoins¹¹⁶.

QUESTION: What would be your actions in relation to the evidence on darkweb activities. Could you engage covert investigation as a buyer and buy drugs, discover the relevant bank accounts and bitcoin wallets and freeze money and property.

¹¹⁶ See for example: <https://www.bitstamp.net/help/what-is-bitcoin/>

6.3 Case Study 2: Consideration of FIU/Law Enforcement Interaction

The Financial Intelligence Unit (FIU) in your country receives a report from a bank indicating that they have a suspicion with some transactions taking place via online banking. The institution has identified that large sums of money were transferred into several customer accounts, where these amounts of money would not be typical for the customers concerned. Additionally, it was noted by the financial institution that the customers appeared to log in to their online banking from IP addresses in Romania, a country that none of the customers have ever logged in from before. This behaviour has been noted in a total of 20 customer accounts and the total value incoming through the 20 accounts is EUR750,000.

The FIU conducts an analysis and identifies other STR's showing suspicious transactions passing through other banks customers' accounts. The FIU prepares a report and passes it to the police.

Research of police intelligence identifies an existing police investigation into the Romanian subjects (actually Moldovan but resident in your country) relating to false identity documents.

The police arrest the subjects and search their premises seizing some laptop computers. Forensic examination of the laptops reveals they have been used to control over 200 bank accounts used to receive and launder money derived from bank accounts of individuals whose computers have been infected by the Trojan 'Dridex'¹¹⁷ which harvested their online bank account credentials. The total sum laundered through these accounts is over €3M.

The suspects are prosecuted and receive jail sentences of 8 and 5 years respectively. No criminal proceeds have been recovered.

QUESTION: What is the legal basis by which the FIU can report the case to the police?

There may be a legislative basis for this interaction, but in many cases, the police and FIU (and other organisations such as tax authorities, customs, etc.) sign a Memorandum of Understanding that allows information sharing to take place. The basis may also depend on the nature of the report made to the police. For example, the information being passed to the police might be considered (by the police) to be intelligence or it might be considered a crime report.

Please investigate the situation in your own country.

QUESTION: What provisions of your criminal procedure code are relevant to the police investigation?

Relating to the area of cybercrime, financial investigations and money laundering there are several actions taken by the police in this case scenario; searches are made of subjects

¹¹⁷ Dridex is an aggressive Trojan mainly used to steal banking credentials. The malware is configured to target the customers of nearly 300 different organizations in over 40 regions. Dridex is heavily focused on customers of financial institutions in wealthy, English-speaking countries, with the majority of targeted organizations located in these countries. The attackers also prioritized other European nations, along with a range of Asia-Pacific regions.

and premises, laptops are seized and forensically examined, evidence is gathered from compromised bank accounts.

The purpose of this question is to consider the legal basis in your criminal procedure code for these actions.

QUESTION: What provisions of your criminal code criminalise the infection of a customer's PC with a virus?

If your country has ratified the Budapest Convention, then infection of a PC with a virus will be criminalised. What is the provision in your Criminal Code that transposes the relevant article from the Budapest Convention?

If your country has not ratified the Budapest Convention, do you have equivalent provisions? How are computer crimes criminalised?

QUESTION: How would you tie the Dridex Trojan activity to the defendants?

The suspects have used a malware to harvest online banking credentials. However, these credentials will have been harvested from the PCs of the victims, not from the PC of the suspects. How, therefore, can you associate the activity of the Trojan with the suspects? Can you form a causal link from the possession of the compromised bank account details (which can be established by their presence on the suspect laptops), to the act of compromising those account details with the Trojan? If yes, how would you approach this? If not, what implications, if any, does this have on the charges that can be brought against the suspects?

QUESTION: How could you establish connections between the Romanians/Moldavians and the controller of the bank accounts where the money has been transferred and the person who disseminated the virus. How could you establish whether there is property of the suspects (in your country or abroad)?

Following on from the previous question, the presence of the bank account details on the suspect laptop may, or may not, demonstrate that the suspects were in control of the bank accounts at the time when the money in question was being transferred. Does this need to be established separately or can it be inferred from the possession of the bank accounts? If not, what else needs to be established?

QUESTION: Can you prosecute for computer facilitated theft?

Computers have been used in this case as a fundamental component of the theft. Is there a provision in your national legislation to criminalise the use of computers as a tool in theft/fraud cases?

QUESTION: What procedural provisions in your national legislation govern the gathering and use of electronic evidence?

In cases such as these, the evidence from the suspect laptops may be crucial. What, therefore, are the provisions in your national legislation that allow for the gathering and use of electronic evidence?

QUESTION: Does your country have a forensic computer capability? How do you engage with the forensic computer capability?

In practical terms collection and management of electronic evidence requires specialist tools and skills. How is this arranged in your country?

QUESTION: Should a financial investigation be carried out in this case? At what point should the financial investigation be initiated?

As described in the scenario, there are clearly significant financial implications associated with the activity of the suspects. In your country, would (and should) a financial investigation be carried out in this case? If so, at what point should the financial investigation be started?

QUESTION: What provisions in your national legislation govern the search, seizure and confiscation of assets in this case? How would you recover the stolen money? Can you freeze it (by FIU or by the police/prosecutor)?

The scenario indicates that the suspects received prison sentences. Do your national provisions require that the asset confiscation component of the proceeding take place after the criminal proceeding, or do they take place in one proceeding?

Do the victims who have been defrauded have any opportunity to recover their stolen funds? Can you compensate victims if you recover some/all of the money? What provisions in your national legislation facilitate this?

QUESTION: What provisions in your national legislation describe the offence of money laundering? Has a money laundering offence taken place?

How is the offence of money laundering defined in your national legislation? Considering the facts of the case as described in the scenario, has a money laundering offence taken place?

QUESTION: Would you prosecute money laundering offence as well as theft/fraud? Why/why not?

When considering this case, would you include a prosecution for the offence of money laundering as well as theft/fraud? If yes, why? If not, why not?

QUESTION: The victims are scattered across many countries, how would you coordinate your investigation with those countries?

Because of the borderless nature of the Internet, virtually all cases with a component of cybercrime also have an international element. In this case, if there are victims in many countries, would you coordinate with those other countries? What if, through your investigations, you identify more victims that were not previously known?

QUESTION: Do you have time limits for submission of evidence and would MLA enquiries exceed those limits? How could you reduce the time delays of MLA requests?

If there is an international component involved, there may be a need to use the mutual legal assistance process, which can introduce some significant delays into the investigation. Do the times involved in the mutual legal assistance process introduce challenges for investigations in your country? How can the time delays be reduced? Can

you use joint investigation teams, for example? Can you use informal channels of communication to facilitate pre-mutual legal assistance enquiries?

6.4 Case Study 3: Consideration of Cybercrime/Money Laundering Interaction

Several citizens in your country report that their PCs were infected with a malware that encrypted all of their photos and documents. The malware then demanded a payment in Bitcoin before decrypting the photos and documents. In several cases, citizens have paid the ransom.

During the investigation, the police engage with the FIU to assist with the tracing of the Bitcoin. The FIU are able to trace the Bitcoin to the exchange where the Bitcoins are converted into fiat currency. The Bitcoin exchange is located in the United States.

A mutual legal assistance (MLA) request is sent to the United States, requesting details of the accounts that performed the transactions. When the response is received from the United States it is revealed that the value of the Bitcoin has been transferred to bank accounts in your country by individuals using IP addresses in your country.

QUESTION: How would you identify the suspects (IP address)? How can you obtain such data - nationally or abroad? What if the IP addresses were not in your country?

The association between an IP address and a real-world person is one of the most important aspects of any online investigation. If the IP address is in your country, how do you engage with national Internet Service Providers to gain access to that data? What legal provisions enable this access? What obligations are placed on Internet Service Providers to retain and make this data available?

Consider the situation where the IP address is not in your country? What is different? How would you approach the situation in that case?

QUESTION: How can you establish the relation between bank account holders (paragraph three in the scenario) and the holders of Bitcoin wallets and persons who used the malware? Should a financial investigation be carried out in this case?

The response to the mutual legal assistance request indicates the IP addresses and bank account details that were used to convert the Bitcoin into fiat currency. How do you (a) find out which financial institution holds the account, if you don't already know and (b) engage with the financial institution to get information about the holder of the bank account. What legal provisions enable this access? What obligations are placed on financial institutions to retain and make this data available?

Consider again the situation where the bank accounts are held in a different country. What is different and how would you approach the situation in that case?

QUESTION: Should a financial investigation be initiated, and if so, at what point?

As described in the scenario, there are clearly significant financial implications associated with the activity of the suspects. In your country, would (and should) a financial

investigation be carried out in this case? If so, at what point should the financial investigation be started?

QUESTION: What provisions in your national legislation describe the offence of money laundering? Has a money laundering offence taken place?

How is the offence of money laundering defined in your national legislation. Considering the facts of the case as described in the scenario, has a money laundering offence taken place?

QUESTION: The scenario describes joint activity by the police and the FIU to analyse and trace the Bitcoin activity. What legal basis for this cooperation exists?

There may be a legislative basis for this interaction, but in many cases, the police and FIU (and other organisations such as tax authorities, customs, etc.) sign a Memorandum of Understanding that allows information sharing to take place.

Please investigate the situation in your own country.

QUESTION: How are virtual currencies, Bitcoin in particular, regulated in your country?

There are various regulatory regimes in place around the world with regards to Bitcoin. What is the situation in your country?

QUESTION: Are virtual currencies obliged entities and required to report suspicious transactions in your country?

In particular, is there an obligation on virtual currency entities such as exchanges or wallet services to report suspicious activity?

7 Appendix: List of Relevant Reading

7.1 Council of Europe

- Convention on Cybercrime, ETS 185, 23.11.2001:
<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
- Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS 189, 28.01.2003:
<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CETS 198, 16.05.2005:
<http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198>
- Convention on Laundering, Search, Seizure And Confiscation of the Proceeds From Crime, Strasbourg, ETS 141, 08.11.1990:
<https://rm.coe.int/168007bd23>
- MONEYVAL/Global Project on Cybercrime, Criminal money flows on the Internet - Typology research, March 2012:
[http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL\(2013\)6_Reptyp_flows_en.pdf](http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)6_Reptyp_flows_en.pdf)
- Council of Europe Study on filtering, blocking and take-down of Illegal Content on the Internet, June 2016:
<https://www.coe.int/en/web/cybercrime/-/study-on-filtering-blocking-and-take-down-of-illegal-content-on-the-internet>
- Questionnaire on the use and efficiency of Council of Europe instruments as regards international co-operation in the field of seizure and confiscation of proceeds of crime, including the management of confiscated goods and asset sharing. PC-OC Mod (2015) 06Rev4, 19.05.2016:
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680666607>
- Cybercrime Legislation – Country profiles:
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Document/ CountryProfiles/default_en.asp
- The functioning of 24/7 points of contact for cybercrime (discussion paper prepared by the Project on Cybercrime), April 2009:
<https://rm.coe.int/16802fa3be>
- Electronic Evidence Guide - A basic guide for police officers, prosecutors and judges (March 2013). Available subject to request at:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp

- T-CY (2006)04 – Strengthening co-operation between law enforcement and the private sector – examples of how the private sector has blocked child pornographic sites, 20 February 2006:
 - <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e6ed1>
- T-CY(2013)17rev - T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, 3 December 2014:
 - <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c>
- T-CY(2014)17 - Rules on obtaining subscriber information report, December 2014:
 - <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1>
- T-CY(2015)10 - Criminal justice access to data in the cloud: challenges, discussion paper prepared by the T-CY Cloud Evidence Group, May 2015:
 - <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59>
- T-CY(2016)13 - Emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers, T-CY Cloud Evidence Group, May 2016:
 - <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f>
- T-CY (2016)2 – Criminal justice access to data in the cloud: cooperation with “foreign” service providers. Background paper prepared by the T-CY Cloud Evidence Group, May 2016:
 - <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d>
- T-CY(2016)7 - Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, final report of the T-CY Cloud Evidence Group, September 2016:
 - <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>
- T-CY(2015)16 Adopted Guidance Note on Production Orders (Article 18) - Version 01 March 2017 (adopted by written procedure on 28 February 2017):
 - <https://rm.coe.int/16806f943e>

7.2 European Union

- Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union OJ L 127/39, 29.4.2014
 - <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0042>

- Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC:
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849>
- Joint Action 98/699/JHA of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime (OJ L 333, 9.12.1998, p. 1):
<http://eur-lex.europa.eu/legal-content/NLN/TXT/?uri=celex:31998F0699>
- Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (OJ L 182, 5.7.2001, p. 1):
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001F0500>
- Council Framework Decision 2005/212/JHA of 24 February 2005 on confiscation of crime-related proceeds, instrumentalities and property (OJ L 68, 15.3.2005, p. 49):
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0049:0051:en:PDF>
- Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196, 2.8.2003):
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003F0577>
- Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders (OJ L 328, 24.11.2006):
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006F0783>
- Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime (L 332/103, 18.12.2007):
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0845>
- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA:
<http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040>
- European Union Directive 2016/1148 on the security of network and information systems ("NIS Directive") of 6 July 2016:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG

- EU GENVAL 2012 Final report on fifth round of mutual evaluation – “Financial crime and financial investigations”:
<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012657%202012%20REV%202>
- Draft Final report of the seventh round of mutual evaluations on "The practical implementation an operation of the European policies on prevention and combating cybercrime", June 2017:
<http://data.consilium.europa.eu/doc/document/ST-9986-2017-INIT/en/pdf>

7.3 United Nations

- United Nations Convention Against Illicit Traffic In Narcotic Drugs And Psychotropic Substances, Vienna, 19.12.1988:
<https://www.unodc.org/unodc/en/treaties/illicit-trafficking.html>
- United Nations Convention Against Transnational Organized Crime, New York, 15.11.2000:
<https://www.unodc.org/unodc/en/treaties/CTOC/>
- United Nations Convention Against Corruption, New York, 31.10.2003:
<http://legal.un.org/avl/ha/uncc/uncc.html>

7.4 Financial Action Task Force

- International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, the FATF Recommendations, 2012:
<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>
- Money Laundering Using New Payment Methods, October 2010:
<http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf>
- Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014:
<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>
- Virtual Currencies – Guidance for a risk-based approach, Financial Action Task Force, June 2015:
<http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

7.5 Jurisprudence

- European Court of Human Rights (ECtHR) Judgement in K.U. v. Finland, 2 December 2008, on the obligation of Governments to protect individuals against crime, including through criminal law:

[http://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22K.U.%20v.%20Finland%22\],%22documentcollectionid%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\],%22itemid%22:\[%22001-89964%22\]}](http://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22K.U.%20v.%20Finland%22],%22documentcollectionid%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-89964%22]})

- ECtHR case law on Personal Data Protection:
http://www.echr.coe.int/Documents/FS_Data_ENG.pdf
- ECtHR case law on New Technologies:
http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf
- ECtHR case law on Mass Surveillance:
http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf
- Court of Justice of the European Union Judgement in Joined Cases C-293/12 and C-594/12. Digital Rights Ireland and Seitlinger and Others:
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>
- EU Court of Justice of the European Union Judgement in Case C-582/14, 19 October 2016, dynamic IP addresses may qualify as 'personal data' under EU privacy law:
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1034974>
- Court of Justice of the European Union Judgement in Case C-264/14, 22 October 2015, "'bitcoin' virtual currency has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators":
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=160800>
- Supreme Court of Belgium ruling in the case of Belgium vs. Yahoo!:
http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1
- US Court of Appeals ruling in the case of Microsoft vs. United States:
<http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412>

7.6 Other References

- Data Retention after the Judgement of the Court of Justice of the European Union, Prof. Dr. Franziska Boehm et al., Munster/Luxembourg, 30 June 2014:
http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf
- Encryption a Matter of Human Rights, Amnesty International Report, March 2016. Available at:
http://www.amnestyusa.org/sites/default/files/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf
- "Brochure: The 6 need-to-knows about Financial Investigation", February 2016:

- <https://english.eu2016.nl/documents/publications/2016/02/10/brochure-the-6-need-to-knows-about-financial-investigation>
- "Needs assessment on tools and methods of financial investigation in the European Union", ECORYS, December 2015:
https://www.wodc.nl/binaries/2612-summary_tcm28-74130.pdf
- European Banking Authority Opinion on 'virtual currencies', EBA/Op/2014/08, July 2014:
<https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>
- An Analysis of Anonymity in Bitcoin Using P2P Network Traffic, Koshy *et al*, Pennsylvania State University:
http://fc14.ifca.ai/papers/fc14_submission_71.pdf
- The Internet Organised Crime Threat Assessment (IOCTA) 2016, Europol:
<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>
- The Internet Organised Crime Threat Assessment (IOCTA) 2017, Europol:
<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>