UNODC
United Nations Office on Drugs and Crime

DIGEST OF CYBER ORGANIZED CRIME

UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

DIGEST OF CYBER ORGANIZED CRIME

UNITED NATIONS
Vienna, 2021

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

Acknowledgments

The present publication was developed by the United Nations Office on Drugs and Crime (UNODC), under phase II of the global programme on implementing the United Nations Convention against Transnational Organized Crime: from theory to practice, thanks to the generous support from the Governments of the United Arab Emirates and the United States of America.

The publication was drafted by Marie-Helen Maras, with substantive support from the following UNODC staff members: Colin Craig, Nayelly Noya Marin, Maria Cristina Montefusco, Riikka Puttonen and Adelaida Rivera. UNODC would also like to thank the following persons for contributing case summaries for this digest: Lisa Armberger, Élise Corsion, Margot Denier, Wydiane Djaidi, Lorenzo Picarella, Louise Pichler, Max Menn, Jesper Bay Kruse Samson and Manveer Singh Sandhu.

UNODC also wishes to acknowledge the contributions of numerous experts who attended the online expert group meetings to support the development of this case digest and the following people who provided cases highlighted in the present publication (listed in alphabetical order by country name): Cristina Giordano, María Alejandra Mangano and Franco Pilnik (Argentina); Daniel Soto (Chile); Romel David Arévalo Gómez and Nelly Johanna Molina Alarcón (Colombia); Rodrigo Picado Mena (Costa Rica); Marta Pelechová (Czechia); Patricia Alejandra Padilla (Dominican Republic); Mohamed Khalaf (Egypt); Raymundo Alirio Carballo Mejia (El Salvador); Ihab Al Moussaoui (Iraq); Enrique Juárez Cienfuegos and Hector Javier Talamantes Abe (Mexico); Giselle M. Acosta González (Panama); Seongjin Park (Republic of Korea); Joseph Budd and Charles Lee (United Kingdom of Great Britain and Northern Ireland); and Louisa Marion, Chad McHenry and Kelly Pearson (United States). Marcus Asner also contributed to the development of this case digest in this manner.

CONTENTS

Explanatory notes

Mention of any firm, product, service or licensed process does not imply endorsement or criticism by the United Nations.

Mention of any case in the present publication does not imply endorsement of any kind.

Symbols of United States documents are composed of capital letters combined with figures. Mention of such a symbol indicates a reference to a United Nations document.

The following abbreviations have been used:

ATM	automatic teller machine
COVID-19	coronavirus disease
DNS	Domain Name System
Europol	European Union Agency for Law Enforcement Cooperation
FBI	Federal Bureau of Investigation (United States of America)
ICT	information and communications technology
I2P	Invisible Internet Project
PIN	personal identification number
SHERLOC	Sharing Electronic Resources and Laws on Crime
SIM	subscriber identification module
Tor	The Onion Router
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNODC	United Nations Office on Drugs and Crime

CHAPTER I.

INTRODUCTION

I. INTRODUCTION

The present case digest contains an analysis of cases of cyber organized crime. The digest is global in scope and attempts, to the extent possible, to ensure an equitable representation of cases from different geographical regions and legal systems. On the basis of more than 100 cases from more than 20 jurisdictions, observations are made about the ways in which cyber organized crime is identified in case law and how this illicit activity is investigated, prosecuted and adjudicated across jurisdictions. The case digest examines the structure and organization of cyber organized criminal groups, tools used by perpetrators of cyber organized crime, types of cyber organized crime and procedural issues relating to the investigation, prosecution and adjudication of cyber organized crime cases. The case digest contains summaries of relevant judicial proceedings concerning cyber organized crime, organized according to theme. The ultimate goals of the digest are to identify cases involving cyber organized crime and the manner in which such crime has been investigated, prosecuted and adjudicated in different areas of the world. The digest concludes by identifying challenges to investigating, prosecuting and adjudicating cases involving cyber organized crime, as well as the lessons learned for criminal justice professionals, including some of the challenging aspects of criminal justice responses to such crime.

A. Background

Information and communications technology (ICT) has transformed conceptions of organized crime. Specifically, ICT has had an impact on the nature of organized crime activities and the types of individuals who can participate in organized crime. This transformation includes changes not only in the types of offences committed and the modi operandi used by organized criminal groups, but also the variety of individuals who can participate in organized crime. Some traditional organized criminal groups are gradually expanding from offline criminal activities to cybercrime, although, to date, this has not been observed as a full transition. What has been observed is the movement of certain illict activities and operations of these groups online. Such groups are also increasingly seeking to cooperate with cybercriminals who have the critical and essential skills that these groups can use or actually need to execute certain operations. These individuals can be, for example, coders (i.e., individuals responsible for developing malicious software (malware), exploits and other tools used to commit cybercrime) and hackers (i.e., individuals responsible for exploiting the vulnerabilities of systems, networks and applications).[1]

ICT has also transformed the way in which certain groups are structured and organized. It removes the need for face-to-face contact between individuals and enables individuals who have never met before to work closely together and coordinate their activities from anywhere in the world. Criminals within these groups can collaborate on illicit activities and objectives using aliases; thus, the risk of revealing their identities and locations to other members of the group is relatively low.

In addition to the evolution in the structure of traditional organized criminal groups, what has also been observed is the formation of "new" groups and networks that commit cybercrimes and operate partially, predominantly or fully online. These groups exhibit behaviours similar to those of traditional organized criminal groups – particularly the use of their structure and special procedures, which are designed to preserve the anonymity of their members and evade detection by law enforcement agencies.

Moreover, ICT has further removed the barriers for entry into illicit markets. No longer limited by geographical locations, individuals can be part of organized criminal groups from anywhere in the world. This technology also provides criminals with the infrastructure, goods, personnel and customers needed to engage in activities related to cyber organized crime.[2] For these reasons, ICT has played a critical role in the expansion of illicit markets and networks and has made illicit business models more efficient and effective. Ultimately, cyberspace provides organized criminal groups with a space within which they can conduct their

[1] Steven R. Chabinsky, Deputy Assistant Director, Cyber Division Federal Bureau of Investigation, "The cyber threat: who's doing what to whom?", speech at the GovSec/FOSE Conference, Washington, D.C., 23 March 2010; Roderic Broadhurst and others, "Organizations and cybercrime: an analysis of the nature of groups engaged in cyber crime", *International Journal of Cyber Criminology*, vol. 8, No. 1 (2014), pp. 1–20.

[2] Marie-Helen Maras, *Cybercriminology* (New York, Oxford University Press, 2016).

illicit activities with a degree of anonymity, exploit the gaps in the legal systems throughout the world, conduct operations and access clients anywhere in the world. The problem of transnational organized crime is thus further compounded by ever-increasing global connectivity and the borderless realm of cyberspace.

One of the main challenges is to identify cyber organized crime and cyber organized criminal groups, as well as the extent to which these groups operate exclusively, predominantly and/or partially online. At the present time, little is known about cyber organized crime. While there is a growing body of research into various forms of cybercrime, there is comparatively less research on cyber organized crime. While cyber organized crime is a dimension of cybercrime, it requires separate consideration and study. This separate consideration and study can help to shed light on the serious cybercrimes perpetrated by multiple participants working together to achieve a goal and protect their online criminal activities. Without understanding the exact nature and extent of the threat, States continue to struggle in containing the security threat emanating from cyber organized crime. Moreover, without this information, policymakers and other stakeholders cannot make informed decisions in response to cyber organized crime and identify proper courses of action to respond to or otherwise address cyber organized crime. To remedy this, the present case digest seeks to shed light on cyber organized crime and identify cyber organized crime cases from different regions. It identifies and analyses cyber organized crime cases in an attempt to determine not only key characteristics of this form of crime and the groups that commit such crime, but also gaps in knowledge and criminal justice practices as they relate to the investigation, prosecution and adjudication of cases involving this crime.

There is no consensus on a definition of cyber organized crime. However, for the purpose of this digest, to be considered a cyber organized crime, the illicit act should have a cyber dimension (be either a cyber-enabled crime[3] or a cyber-dependent crime[4]) and involve either an organized criminal group (defined in article 2 of the United Nations Convention against Transnational Organized Crime) or an offence established in accordance with article 5 of the Convention (i.e., conspiracy or criminal association).[5] The digest identifies and analyses cyber organized crime cases from various regions with the objective of finding out the ways in which cases involving such crime are investigated, prosecuted and adjudicated, as well as the limitations of and lessons learned from criminal justice responses to such crime.

B. Methodology

The research for this digest predominantly involved a systematic review of primary sources, supplemented by secondary sources. The research began with the identification of cyber organized crime cases in the case law database of the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal of the United Nations Office on Drugs and Crime (UNODC). The database does not record cases involving cyber organized crime but includes cases that cover both "cybercrime" and "participation in an organized criminal group".

Following the review of the SHERLOC case law database and the identification of cyber organized crime cases in the database, cases were solicited from experts participating in two regional expert group meetings on cyber organized crime that were held online (the first meeting, hosted by the United Arab Emirates, was held from 21 to 24 September 2020; and the second, hosted by El Salvador, was held from 19 to 21 February 2021), as well as from States, volunteers and UNODC staff. Desk research was also performed

[3] Cyber-enabled crimes are traditional crimes that are facilitated (in some way) by information and communications technology (ICT). For cyber-enabled crimes, ICT plays a key role in the method of operation (i.e., modus operandi of the offender or offenders; see also United Nations Office on Drugs and Crime (UNODC), Education for Justice University Module Series, Cybercrime, Module 1: introduction to cybercrime, "Cybercrime in brief". Available at **www.unodc.org/e4j/**.

[4] For cyber-dependent crimes, which include crimes that "can only be committed using computers, computer networks or other forms of information communication technology", ICT is the target of the crime (Mike McGuire and Samantha Dowling, "Cyber-dependent crimes", in *Cybercrime: A Review of the Evidence*, Home Office Research Report 75 (London, 2013), p. 4; see also European Union Agency for Law Enforcement Cooperation (Europol), European Cybercrime Centre, *Internet Organised Crime Threat Assessment 2018* (The Hague, 2018), p. 15).

[5] Organized criminal groups are involved in the commission of cyber-assisted, cyber-enabled and cyber-dependent crimes. Cyber-assisted crimes are those crimes where ICT is incidental to the illicit act (e.g., technology is used to facilitate communication between members). While organized criminal groups utilize ICT to communicate and coordinate activities, the use of this technology in this manner is not considered a cybercrime because it is incidental and not integral to the crime. For this reason, cyber-assisted crimes are excluded from consideration in this digest.

using private case law databases (e.g., LexisNexis and Westlaw), open case law databases (government databases, legal information institutes), secondary literature (e.g., law journals and academic publications) and media sources (wherever needed). Moreover, the digest draws on an earlier work by UNODC, which included some cases of cyber organized crime involving trafficking in persons, particularly the 2021 research brief of UNODC on trafficking in persons and Internet technologies, as well as the cases presented at its supplementary expert group meeting on trafficking in persons and Internet technologies, held in Vienna from 25 to 27 November 2019.

This case digest is primarily based on primary sources and hence access to court documents such as judgments, indictments and/or transcripts was a prerequisite for inclusion in the digest. The guiding principles for selection were: *(a)* representation of a variety of dimensions and issues relating to cyber organized crime; *(b)* representation of a variety of geographical regions and legal systems; and *(c)* conclusion of the cases within the period 2000–2020, which is the period covered by this case digest. Classified information does not appear in the digest, and the names of defendants appear in the digest only if the names appear in the official case citation. The cases referred to in the case digest are not the only ones that concern the subject of this digest. The most relevant cases or those considered to be good examples of cases involving cyber organized crime are cited in this document. At the same time, inclusion of a particular case in this digest does not imply endorsement of any kind by UNODC.

The identification of cases involving cyber organized crime in case law is challenging because the cases are not recorded as cyber organized crime. In many cases involving cyber organized crime, individuals are not charged with organized crime and/or participation in an organized criminal group; and/or cyber organized crime, organized criminal groups and/or participation in an organized criminal group are not explicitly mentioned. For these reasons, the identification of a case involving cyber organized crime requires a thorough examination of the details of the case in court documents. Accordingly, for this digest, court documents were examined and analysed to identify essential elements of cyber organized crime, such as the existence of organized criminal groups or participation in an organized criminal group, and the engagement of defendants in cyber-dependent and/or cyber-enabled crime. Another challenge was obtaining court transcripts and other court documents relating to the cases. These documents were not always publicly available or publicly accessible. A further challenge was identifying cases from a variety of geographical regions and legal systems. Cases from certain developed countries were more readily available. Nonetheless, even in such countries, access to many judicial decisions is restricted by a paywall. In least developed countries, there may be no (or only a limited number of) judicial decisions that are accessible online. Language limitations of the researchers and drafters working on the case digest posed an additional challenge.

Other limitations are inherent in this methodology. The case digest is not a comprehensive review of all judicial decisions dealing with cyber organized crime in all countries. A fully comprehensive review of all countries is well beyond the scope of this digest. Moreover, the use of judicial decisions as a methodology for the development of the publication also has inherent limits. Concluded judicial decisions come at the end of a long process of investigation, prosecution and adjudication of offences. At each stage of this process, various factors affect whether and how a case proceeds to the next stage. First, some types of cybercrime are more likely than others to be reported to authorities for investigation. This may be attributable to a variety of factors, including who the victims are and the size and nature of the harm caused. Secondly, not all offences reported to authorities proceed to the investigation stage. In addition to the aforementioned factors, whether an investigation is opened may also depend on law enforcement priorities and resources. Thirdly, not all offences that are investigated lead to charges being laid. This may be affected by a range of issues such as lack of evidence, difficulties with international cooperation, difficulties with jurisdiction and difficulties with identifying and extraditing suspects. Fourthly, not all cases in which charges are laid will proceed to trial. In some countries, prosecutors have a discretion as to which cases should be brought to trial. Charges may be dropped where prosecution is deemed not to be in the best interests of the community. Charges may also be dropped where there is a lack of evidence or as part of incentives to cooperate with law enforcement. Only a minority of cases will reach the end of this process and be subject to a final judicial decision, whether a conviction or acquittal. Finally, not all cases that are subject to a final judicial decision will be published. The factors that hinder investigation, prosecution, adjudication and publication of cases will vary according to, inter alia, the crime in question and the country in which it takes place. Factors that hinder investigation, prosecution, adjudication and publication are likely to be more pronounced in least developed countries.

Each of the aforementioned factors can have an effect on the type of cases obtained for inclusion in the case digest and on the countries represented in the digest. Accordingly, the case digest cannot be considered a representative sample of all cases involving cyber organized crime in all countries. Nevertheless, within these limitations, the case digest seeks to provide a broad overview of cyber organized crime threats faced in countries throughout the world and the responses of investigators, prosecutors and the judiciary.

C. Target audience

The present digest is designed for a wide audience of readers. It is intended to serve as a reference guide to help criminal justice actors identify and counter cyber organized crime and address the challenges in investigating, prosecuting and adjudicating cyber organized crime. Academics, researchers, practitioners, policymakers, legislators and proponents of legislative reform may also find this digest useful. Ultimately, the digest can be used as a resource on what cyber organized crime entails and the manner in which it is investigated, prosecuted and adjudicated worldwide.

D. Structure of the publication

The publication is divided into five main chapters, in addition to the chapter containing the introduction and the chapter on conclusions and lessons learned. Specific cases involving cyber organized crime are highlighted in boxes in the body of the text. A list of cases involving cyber organized crime appears in the annex.

Subjects covered in the publication include the structure, organization and types of cyber organized criminal groups; tools used by perpetrators of cyber organized crime; types of cyber organized crime; and procedural issues relating to the investigation, prosecution and adjudication of cases involving cyber organized crime.

The types of criminal groups that engage in cyber organized crime include groups that predominantly operate online and commit cybercrime; those that operate offline and online and engage in both offline crime and cybercrime; and groups that predominantly operate offline and engage in cybercrime to expand and facilitate offline activities.

The tools used by perpetrators of cyber organized crime include tools such as the clearnet (or the surface web), licit online marketplaces, social media platforms, the darknet, secure communications platforms, online payment services and digital currencies.

Cyber organized crime includes all forms of cyber-dependent or cyber-enabled crime committed by an organized criminal group and/or those who participate in an organized criminal group. Cyber-dependent crime includes acts against the confidentiality, integrity and availability of computer systems and data (such as illegal access to a computer system and/or computer data, illegal interception of computer data and/or acquisition of computer data, illegal computer system and data interference); and illegal production, distribution, use and possession of computer misuse tools. Cyber-enabled crime includes traditional criminal acts that are facilitated (in some way) by ICT, such as computer-related fraud or forgery; computer-related identity offences; crime involving falsified medical products; counterfeiting; blackmail, extortion and ransom; offences involving child sexual abuse and child sexual exploitation; trafficking in persons; smuggling of migrants; drug trafficking; trafficking in firearms; trafficking in wildlife; trafficking in cultural property; money-laundering; and Internet gambling.

The chapter on relevant procedural issues covers issues relating to jurisdiction; identification, tracing, freezing, seizure and confiscation of proceeds of crime; special investigative techniques (electronic surveillance, undercover operations, controlled delivery and other techniques); the collection and use of electronic evidence (expedited preservation of data, production orders, real-time collection of communication traffic data, and interception of content data); and various forms of international cooperation (extradition, mutual legal assistance, law enforcement cooperation and joint investigations).

Finally, the digest includes a chapter on conclusions and lessons learned in the investigation, prosecution and adjudication of cases involving cyber organized crime.

CHAPTER II.

CYBER ORGANIZED CRIME: WHAT IS IT?

II. CYBER ORGANIZED CRIME: WHAT IS IT?

There is no consensus on the definition of cyber organized crime.[6] For the purpose of this digest, cyber organized crime refers to a cybercrime (a cyber-dependent and/or cyber-enabled crime) that is either: *(a)* committed by an organized criminal group, as defined in article 2, subparagraph (a), of the United Nations Convention against Transnational Organized Crime, adopted in 2000; or *(b)* involving an offence established in accordance with article 5 of the Convention, which covers the criminalization of participation in an organized criminal group. Each of these elements are explored in the sections that follow.

A. Cybercrime

Cybercrime is a complex concept that encompasses an array of illicit activities targeting ICT and/or utilizing ICT in the commission of the offence. The offences that are considered cybercrimes are cyber-enabled and cyber-dependent crimes. Cyber-enabled crimes are traditional crimes that are facilitated (in some way) by ICT. For cyber-enabled crimes, ICT plays a key role in the method of operation (modus operandi) of the offender or offenders.[7] By contrast, for cyber-dependent crimes, which include crimes that can only be committed using computers, computer networks or other forms of information communication technology,[8] ICT is the target of the crime.

B. Cyber organized criminal group

Cyber organized criminal groups are organized criminal groups that commit cybercrimes. An organized criminal group is defined in article 2, subparagraph (a), of the Organized Crime Convention as "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit".

In article 2, subparagraph (c) of the Convention, "structured group" is defined as "a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure". A structured group is thus not necessarily one that is hierarchical. For this reason, a decentralized and/or loosely affiliated group can be considered a "structured group".[9]

The aforementioned definition of an organized criminal group states that the group must exist for a "period of time". This requirement can be interpreted as "any period of time".[10] The organized criminal group must also "act in concert", which means that "members of the organized criminal group act together".[11] The definition also includes the requirement that the group engage in serious crime. The term "serious crime" is defined in the Convention by referring not to particular types of criminal activity but to the applicable penalties. Specifically, "serious crime" is defined in article 2, subparagraph (b), of the Convention as "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty".

---

[6] UNODC, *Comprehensive Study on Cybercrime*, draft (Vienna, 2013); Broadhurst and others, "Organizations and cybercrime"; see also UNODC, Education for Justice University Module Series, Cybercrime, Module 13: cyber organized crime, "Conceptualizing organized crime and defining the actors involved". Available at **www.undoc.org/e4j/**.

[7] See also UNODC, Education for Justice University Module Series, Cybercrime, Module 1: introduction to cybercrime, "Cybercrime in brief".

[8] McGuire and Dowling, *Cybercrime: A Review of the Evidence – Chapter 1,* p. 4; Europol, *Internet Organised Crime Threat Assessment 2018*, p. 15.

[9] See also UNODC, Doha Declaration, Tertiary, Education for Justice University Module Series, Organized crime, Module 1: Definitions of organized crime, "Activities, organization and composition of organized criminal groups". Available at **www.unodc.org/e4j/**; UNODC, Education for Justice University Module Series, Cybercrime, Module 13: cyber organized crime, "Conceptualizing organized crime and defining the actors involved". Available at **www.unodc.org/e4j/**.

[10] UNODC, *Model Legislative Provisions against Organized Crime* (Vienna, 2012), p. 8.

[11] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime* (Vienna, 2016), para, 35.

Finally, to be considered an organized criminal group, the group must commit "serious crimes or offences established in accordance with this Convention"[12] in order to obtain some form of "financial or other material benefit". There is no prerequisite, however, that the predominant aim of the organized criminal group is a "financial or other material benefit". The term "other material benefit" is not limited to financially related or equivalent benefits. According to the *Travaux Préparatoires of the Negotiations for the Elaboration of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto*, the term "should be interpreted broadly, to include personal benefits such as sexual gratification". This is to ensure that groups involved in, for instance, child sexual abuse for non-monetary reasons are not excluded.[13] The requirement that the organized group commit a serious crime to obtain some form of "financial or other material benefit" is not a universal requirement in national legislation on organized crime, however. In the United Kingdom of Great Britain and Northern Ireland, for example, the definition of an organized criminal group (or organized crime group, as it is called in the Serious Crime Act 2015) does not refer to "financial or other material benefit". Instead, the Act refers to a group of "three or more persons who act, or agree to act, together to further" a criminal purpose.[14] Likewise, in Germany, the law's definition of an organized criminal group does not include an element concerning the purpose of obtaining a financial or other material benefit.[15] In a case before the Federal Court of Justice of Germany, a group of seven persons charged with and convicted for inciting hatred and distributing unconstitutional content via an Internet radio show (European Brotherhood Radio) were considered a "criminal organization" (see the box below).[16]

BGH, Beschluss vom 19.04.2011, 3 StR 230/10 (Germany)

In June 2008, the defendants W., P., M. and R. formed a structured association to disseminate inciteful and otherwise criminal songs via an Internet radio stream. W., who had risen to organizer and head of the organized criminal group in the summer of 2007, rented a server and created the website "European Brotherhood Radio". The radio stream could be accessed from this site. Furthermore, instructions for building explosives and explosive devices could be found on the subpage Sprengmeister (demolition expert).

Regarding the technical functioning of the radio shows, W. provided the defendants P. and M, and later also the defendants B., Br. and F., with access that enabled them to control and moderate the radio stream. The defendants W. and P. also moderated their own radio shows, where they – in part together, in part on their own – played right-wing extremist songs and other illegal content. Moreover, they recruited other persons to moderate the shows, including the defendants B., Br. and F., and advertised the positions by using stickers, banners, jingles, etc. on the website as well as on the subpages. On 21 February 2009, they also organized an advertising event for the radio. Defendant M. rented the radio stream through which the shows aired and were heard by 20–50 people. He also moderated a continuous broadcast from 24 to 26 February 2009 where he played right-wing extremist songs with inciteful and otherwise illegal content. Defendant R. invested several small amounts of money, including for the creation of the banner and the rent of the radio stream, and maintained the chat rooms on the website.

[12] The "offences established in accordance with this Convention" that are mentioned in the definition of "organized criminal group" are established in accordance with article 5 (criminalization of participation in an organized criminal group), article 6 (criminalization of the laundering of proceeds of crime), article 8 (criminalization of corruption) and article 23 of this Convention (criminalization of obstruction of justice).

[13] *Travaux Préparatoires of the Negotiations for the Elaboration of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (United Nations Publications, 2006), p. 17; cited in UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime*, para. 34.

[14] United Kingdom of Great Britain and Northern Ireland, Serious Crime Act of 2015, sect. 45 (6).

[15] Germany, Criminal Code, sect. 129.

[16] Germany, Federal Court of Justice Decision No. 3 StR 230/10 of 19 April 2011 (BGH, Beschluss vom 19. April 2011–3 StR 230/10).

BGH, Beschluss vom 19.04.2011, 3 StR 230/10 (Germany) (*continued*)

All of the defendants were convicted of forming a criminal organization. Moreover, the defendants had thousands of right-wing extremist files in their possession in order to make them available to the listeners of the radio shows. For this reason, they were convicted for the offences of incitement of masses, dissemination of propaganda material of unconstitutional organizations, and use of symbols of unconstitutional organizations. Independent of the radio stream, defendant W. was in possession of two objects banned under the Weapons Act, as well as a gun and ammunition requiring a licence, which he did not have.

For more information on this case, see UNODC Sharing Electronic Resources and Laws on Crime (SHERLOC) case law database, Case No. DEUx028.[a]

[a] Available at https://sherloc.unodc.org/.

C. Criminalization of participation in cyber organized crime

Article 5 of the Organized Crime Convention requires States parties to the Convention to adopt legislative and other measures to establish as a criminal offence participation in an organized criminal group as a criminal offence, creating criminal liability for persons who intentionally participate in or contribute to the criminal activities of organized criminal groups.[17] This offence broadens criminal liability beyond criminal activities committed by groups, by holding individual actors responsible for their participation in serious crimes involving these groups. A person can be held accountable for their role in planning, organizing, directing, supporting, facilitating or otherwise assisting in the commission of a serious crime relating to an organized criminal group, even if an offence has not been or has not yet been committed by the person.[18] National laws criminalize participation in a criminal organization. However, those laws diverge in the manner in which participation in an organized criminal group is criminalized.

1. Conspiracy

In common-law countries, conspiracy is used to address criminal participation in an organized criminal group. Conspiracy is a voluntary agreement between two or more persons to commit an illicit act. In article 5, paragraph 1 (a) (i), of the Organized Crime Convention, conspiracy is paraphrased as "agreeing with one or more persons to commit a serious crime for a purpose relating directly or indirectly to the obtaining of a financial or other material benefit and, where required by domestic law, involving an act undertaken by one of the participants in furtherance of the agreement or involving an organized criminal group".

[17] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime*, para. 72; CTOC/COP/WG.2/2014/2, para. 4.

[18] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime*, para. 73; CTOC/COP/WG.2/2014/2, paras. 4–5.

Table 1. Elements of conspiracy in the United Nations Convention against Transnational Organized Crime

Provision in the Convention	*Physical element (actus reus)*	*Mental element (mens rea)*
Article 5, paragraph 1 (a) (i)	Agreeing with one or more other persons to commit a serious crime	The agreement was entered into intentionally. The agreement was made for a purpose relating directly or indirectly to obtaining a financial or other material benefit.

Source: UNODC, *Model Legislative Provisions against Organized Crime* (Vienna, 2012).

The crime that is part of this voluntary agreement does not have to be committed for criminal responsibility to apply. The crime of conspiracy is known as an inchoate crime, which is an illicit act taken towards the preparation to commit and/or the commission of a crime. In some jurisdictions, beyond the agreement, some action must be taken towards the commission of the crime. The crime of conspiracy is distinct from the crime that is the object of the conspiracy (i.e., the crime that the conspirators agree to commit). For this reason, people may be charged with and convicted for both conspiracy and the crime (or crimes) that they agreed to commit.

Regina v. Jake Levene, Mandy Christopher Lowther, Lee Childs (2017), Crown Court Leeds, T20177358 (United Kingdom)

UKBargins (AlphaBay)

Using the computer moniker "UKBargins", the defendants (J.L., M.C.L. and L.M.C.) sold adulterated fentanyl and carfentanil online on AlphaBay, a darknet market. They distributed the drugs domestically, in the United Kingdom of Great Britain and Northern Ireland, and internationally, in Argentina, Canada, the United States of America and other countries, including European countries. The majority of the customers (271 of the 443 identified customers) were overseas.[a] The defendants purchased the equipment and rented premises used to create and package the products they sold (carfentanil and fentanyl mixed with adulterants). The products were mailed to buyers using postal services. The three defendants were charged with and sentenced for conspiracy to evade prohibition of the exportation of controlled substances and conspiracy to provide controlled substances.[b] All three defendants pleaded guilty to their crimes. Two of the defendants (J.L. and M.C.L.) were sentenced to 16 years and 6 months of imprisonment, while the third defendant (L.M.C.) received a sentence of 10 years and 6 months of imprisonment.

For more information on this case, see UNODC, SHERLOC case law database, Case No. GBRx097.[c]

[a] United Kingdom, Crown Court Leeds, *R v. Levene* [2017], T20177358. Amended Sentence Opening. Judgment of 29 May 2018.

[b] The specific charges were: conspiracy to evade prohibition on the exportation of a controlled drug of class A – carfentanyl; conspiracy to evade prohibition on the exportation of a controlled drug of class A – fentanyl; conspiracy to supply a class A drug – carfentanyl; and conspiracy to supply a class A drug – fentanyl. *R. v. Lee Matthew Childs*, Crown Court Leeds, T20177358, Order for imprisonment of 18 January 2019; *Regina v. Jake Levene, Mandy Christopher Lowther, Lee Childs*, Crown Court Leeds, Case No. T20177358, Order for imprisonment of 18 January 2019; and *Regina v. Mandy Christopher Lowther*, Crown Court Leeds, T20177358, Order for imprisonment of 18 January 2019.

[c] Available at https://sherloc.unodc.org/.

2. Criminal association

In article 5, paragraph 1 (a) (ii), of the Organized Crime Convention, criminal association is paraphrased as follows:

(ii) Conduct by a person who, with knowledge of either the aim and general criminal activity of an organized criminal group or its intention to commit the crimes in question, takes an active part in:

a. Criminal activities of the organized criminal group;

b. Other activities of the organized criminal group in the knowledge that his or her participation will contribute to the achievement of the above-described criminal aim.

Table 2. Elements of criminal association in the United Nations Convention against Transnational Organized Crime

Provision in the Convention	*Physical element (actus reus)*	*Mental element (mens rea)*
Article 5, paragraph 1 (a) (ii) a	Through an act or omission, take an active part in criminal activities of the organized criminal group	The act or omission is intentional and undertaken with knowledge of the criminal nature of the group, or of its criminal activities or objectives.
Article 5, paragraph 1 (a) (ii) b	Through an act or omission, take an active part in other (non-criminal) activities of the organized criminal group	The act or omission is intentional and undertaken with knowledge that participation will contribute to the achievement of the criminal aim.

Source: UNODC, *Model Legislative Provisions against Organized Crime* (Vienna, 2012).

Civil-law countries typically criminalize association with a group that has criminal objectives. In such countries, a person can be charged with criminal association for illegal and/or legal activities that they engage in on behalf of and/or for the organized criminal group. The person engaging in these acts must be knowledgeable of the criminal nature, activities and/or objectives of the group.

Cassazione penale, sezione III, 12 Febbraio 2004, No. 8296, & Tribunale di Siracusa, 19 Luglio 2012, No. 229 (Italy)

A case in Italy involved a chat group on MSN ("Foto di Preteen") where child sexual abuse material was shared among members of the community. This case represents one of the first instances in that country where unlawful association (art. 416 of the Criminal Code ("Associazione per delinquere")) was applied to criminal groups operating online. The court determined whether the legal definition of unlawful association could be applied to online criminality.

The court stated that the fact that the interactions between the different members of the group took place in the virtual world did not constitute an obstacle per se to the creation of an organized criminal group. In this case, the court identified the presence of all of the following elements of unlawful association: *(a)* the existence of a bond between at least three persons that was not short term or occasional; *(b)* the existence of a criminal plan that constituted the aim of the organization; and *(c)* the existence of an organizational structure, with a minimum degree of sophistication, that enabled the criminal plan to be carried out. The court held that the website allowed different persons to cooperate for a period of time. The website had a defined structure, with a webmaster who

represented the leader of the criminal association and who established and enforced a set of strict internal rules regulating the organization — rules that all of the subscribers of the group had to follow and abide by (e.g., rules for joining the website and punishment for non-compliance with the rules). In addition, the court held that the organization achieved its objectives through the website, which enabled the collection and distribution of child sexual abuse material. Citing the above-mentioned findings and reasons, the court concluded that the legal definition of organized crime could also be applied to online criminal groups.

CHAPTER III.

CYBER ORGANIZED CRIMINAL GROUPS

III. CYBER ORGANIZED CRIMINAL GROUPS

The structure, organization and types of cyber organized criminal groups vary, as do the roles within those groups. The geographical location and/or concentration or distribution of members of the groups also vary. The same holds true for the gender of members of cyber organized criminal groups and those who participate in cyber organized crime, as well as the gender of victims of cyber organized crime. Each of these issues are explored below.

A. Structure, organization and types of criminal groups that engage in cyber organized crime

The structural complexity and organization of cyber organized crime vary. Cyber organized criminal groups range from those with hierarchical structures, with some form of centralization, division of labour and identifiable leaders, to those that are transient, fluid, lateral, loosely affiliated and decentralized networks.[19] DrinkorDie, a group of copyright infringers/digital pirates, was a hierarchical group with a clear division of labour and roles within the group.[20] By contrast, Dream Market was a decentralized network made up of diffused, loosely structured groups.[21] In some cases, the structure and organization of the groups were not connected to people but to the online site within which they operated. This has been observed on illicit online market sites on both the clearnet (i.e., the visible web) and the darknet.[22]

Cyber organized criminal groups use online forums and platforms to regulate and control their provision of illicit goods and services. Other cyber organized criminal groups have service-providing structures (i.e., they offer crime as a service).[23] For instance, the Shadowcrew, an international organization with approximately 4,000 members, promoted and facilitated a wide variety of criminal activities online, including electronic theft of personal identifying information, credit card and debit card fraud, and the production and sale of false identification documents.[24] These groups are composed in a manner that makes the provision of their services possible by, for example, leveraging multi-skilled members and/or associates who can provide the services. The Shadowcrew divided labour according to specific skills in order to facilitate its operations.

These groups exhibit behaviours similar to those of traditional organized criminal groups, particularly the use of structure and procedures that are designed to preserve the anonymity of members and avoid the attention of law enforcement agencies by deploying operational security measures to hide their identities and activities.[25] For example, the Bayrob group redirected users seeking assistance or seeking to report crime to websites that they controlled, thus evading detection by private organizations, security companies

[19] See also UNODC, Education for Justice University Module Series, Cybercrime, Module 13: Cyber organized crime, "Criminal groups engaging in cyber organized crime". Available at **www.unodc.org/e4j/**.

[20] Federal Court of Australia, *Hew Raymond Griffiths v. United States of America*, 143 FCR 182 (2005), 2005 WL 572006 (DrinkorDie leader); see also United States Department of Justice, "Extradited software piracy ringleader sentenced to 51 months in prison", press release, 22 June 2007.

[21] United States District Court, *United States of America v. Gal Vallerius* (2018).

[22] See, for example, Southern District of New York, *United States of America v. Gary Davis*, Case No. 1:13-CR-950-2, 26 July 2019 (UNODC, SHERLOC case law database, Case No. USAx156)(Silk Road); *United States of America v. Ross William Ulbricht*, Case No. 15-1815 (2d Circuit 2017), 31 May 2017 (UNODC, SHERLOC case law database, Case No. USAx202); Western District of Louisiana, *United States of America v. John Doe #1, Edward Odewaldt, et al*., Case No. 10-CR-00319, Third Superseding Indictment, 16 March 2011, pp. 4–5 (Dreamboard); Western District of Washington, *United States of America v. Brian Richard Farrell*, Case No. 2:15-CR-29-RAJ (Silk Road 2.0), 17 January 2015); United States District Court, *United States of America v. Gal Vallerius* (Dream Market).

[23] Crime as a service refers to criminals' provision of services that facilitate crimes and/or cybercrimes (Maras, *Cybercriminology*); Roderic Broadhurst and others, *Malware Trends on "Darknet" Crypto-markets: Research Review – Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology* (Canberra, Australian National University, Cybercrime Observatory, 2018).

[24] United States District Court, District of New Jersey, *United States of America v. Andrew Mantovani et al*., Criminal Indictment, Case No. 2:04-CR-0078, 28 October 2004, p. 2 (Shadowcrew).

[25] United States, Northern District of Ohio, *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus* **(Bayrob Group),** Case No. 1:16-CR-00224, Indictment, (8 July 2016).

and law enforcement agencies.[26] These groups also take measures to evade law enforcement detection that accord with the type of services they provide. In fact, forums with child sexual abuse material and specialized forums for cybercriminals only commonly have greater security measures than those sites that offer controlled drugs and other illegal goods. For instance, Dreamboard, an illicit site where child sexual abuse material was exchanged, took significant measures aimed at preventing infiltration by law enforcement agencies by requiring all its members to be vetted and to continuously contribute child sexual abuse material to the platform.[27] In addition, the administrator of Card Planet (a "carding" forum where credit card data that were stolen predominantly through computer intrusions were made available for a fee) had also created a site called Cybercrime Forum for elite cybercriminals.[28] Any person interested in using this site had to first become a member, and to do that the person had to be vetted by three existing members and had to pay a fee (usually 5,000 United States dollars as a form of insurance). The existing members of the site would then vote on whether the prospective member should be granted access to the site.[29] The Cybercrime Forum also took other security measures to avoid detection by law enforcement agencies. For example, arrested members were banned from the site to prevent law enforcement agencies from using them and/or their details to access the site.[30]

Typologies have been created on criminal groups that engage in cybercrime based on the structures of these groups and their degree of involvement in offline and/or online activities.[31] Cyber organized criminal groups can be broken down into three types:[32] groups that predominantly operate online and commit cybercrime; groups that operate both offline and online and engage in both offline crime and cybercrime; and groups that predominantly operate offline and engage in cybercrime to expand and facilitate their offline activities. Each of these is explored in the subsections that follow.

1. Groups that predominantly operate online

There are two types of groups that predominantly operate online and commit cybercrime: swarms and hubs.

(a) Swarms

A swarm can be described as the coalescence, for a limited period of time, of individuals to engage in specific tasks in order to commit a cybercrime.[33] Once they complete their assigned task or objectives and/or succeed in committing the cybercrime as a collective, some, most or all of the individuals may go their separate ways and the temporary group that has been formed may disband.[34] This disbanding does not preclude any of the individuals from becoming part of another swarm to engage in a similar or different cybercrime in the future, with some or all of the same individuals or with other individuals.

Swarms are characterized as decentralized networks, typically (though not exclusively) made up of "ephemeral clusters of individuals" with a common purpose and minimal chains of command.[35] A common purpose of a swarm is to commit a cybercrime for ideological reasons and the individuals who join swarms tend to

[26] Ibid.

[27] *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard).

[28] United States, Eastern District of Virginia, *United States of America v. Aleksei Yurievich Burkov* (Card Planet), Case No. 1:15-CR-00245, Superseding Indictment, February 2016.

[29] Ibid., pp. 13–14.

[30] *United States of America v. Aleksei Yurievich Burkov* (Card Planet).

[31] BAE Systems Detica and John Grieve Centre for Policing and Community Safety, London Metropolitan University, *Organised Crime in the Digital Age* (2012) UNODC, *Comprehensive Study on Cybercrime*, draft; Broadhurst and others, "Organizations and cybercrime".

[32] Ibid.

[33] See also UNODC, Education for Justice University Module Series, Cybercrime, Module 13: cyber organized crime, "Criminal groups engaging in cyber organized crime".

[34] In her 2002 article, Susan Brenner discusses the possibility of "swarms" manifesting and operating online (see Susan W. Brenner, "Organized cybercrime? How cyberspace may affect the structure of criminal relationships", *North Carolina Journal of Law & Technology*, vol. 4, No. 1 (2002), pp. 43–45).

[35] Broadhurst and others, "Organizations and cybercrime".

do so for such reasons. An example of the composition of a swarm is the "hacktivist" group Anonymous.[36] While Anonymous does not have a declared leader, the group has some degree of leadership, at least in the sense that there are members of the group who take the initiative in organizing, planning and ultimately making decisions on committing cybercrimes.[37] In 2014, *United States of America v. Gottesfeld*,[38] a self-identified member of Anonymous conducted a distributed denial-of-service attack[39] against the computer network of a children's hospital, purportedly in response to the hospital's handling of a former patient. He was charged with and convicted for conspiracy to damage and for damaging protected computers, was sentenced to 121 months' imprisonment and was required to pay restitution (an estimated US$ 443,000).[40] Nevertheless, in most jurisdictions, swarms are not be regarded as organized criminal groups if they do not engage in cybercrime for a material benefit.

(b) Hubs

A hub is a group that has a core group of criminals who are surrounded by peripheral criminal associates. A hub is more structured than a swarm; it has a command structure that can be identified. Typically, the activities of hubs are profit-driven. Some of the criminal activities corresponding to this organizational structure are phishing, sexual offending and malware operations (worms, viruses, scareware, etc.).[41]

An example of a hub is Dreamboard, a criminal enterprise consisting of an online bulletin board that advertised and distributed child sexual abuse material only to its members. In order to join Dreamboard, prospective members had to provide child sexual abuse material. In order to remain a member of Dreamboard, members had to continuously provide child sexual abuse material or their access to the bulletin board would be revoked. A member's access was revoked if the member went 50 days without posting child sexual abuse material.[42] Dreamboard members had to follow rules, which were available in four languages (English, Japanese, Russian and Spanish). One of the rules was that images on the site must be of girls 12 years old or younger.[43] The administrator of Dreamboard placed its members in separate groups. Members of the SuperVIP group were trusted members of the site who produced and advertised their own child sexual abuse material. SuperVIP group members had greater access to child sexual abuse material than other members.[44] VIP group members and other members had more restricted access to child sexual abuse material. To advance to a higher group level, they needed to produce child sexual abuse material and make it available to other members, post more advertisements for child sexual abuse material or post advertisements for child sexual abuse material that other members did not already have in their possession.[45] A few Dreamboard members were sentenced to life imprisonment for their crimes.[46]

---

[36] Members of Anonymous have been charged with committing various cyber-dependent crimes during their hacktivist operations (see, for example, United States, Northern District of California, *United States of America v. Dennis Collins et al.*, Case No. 11-CR-00471-DLJ (PSG), 16 March 2012). Members of Anonymous were charged for conducting coordinated distributed denial-of-service attacks against PayPal during Operation Avenge Assange). Thirteen members pleaded guilty to charges of violations of the Computer Fraud and Abuse Act of 1986. Most of the defendants pleaded guilty to a conspiracy charge as well (United States Attorney's Office, Northern District of California, "Thirteen defendants plead guilty for December 2010 cyber-attack against PayPal", 6 December 2013.

[37] David S. Wall, "Dis-organised crime: towards a distributed model of the organization of cybercrime", *The European Review of Organised Crime*, vol. 2, No. 2 (2015), pp. 71–90.

[38] United States District Court, District of Massachusetts, *United States of America v. Martin Gottesfeld*, 319 F. Supp. 3d 548, 19 June 2018.

[39] A distributed denial-of-service attack involves the use of multiple computers and other technologies to overwhelm the target's resources.

[40] Nate Raymond, "Massachusetts man gets 10 years in prison for hospital cyberattack", *Reuters*, 10 January 2019.

[41] Broadhurst and others, "Organizations and cybercrime"; see also UNODC, Education for Justice University Module Series, Cybercrime, Module 13: cyber organized crime, "Criminal groups engaging in cyber organized crime".

[42] *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard).

[43] Ibid.

[44] Ibid., p. 6.

[45] Ibid.

[46] United States Department of Justice, Office of Public Affairs, "Third Dreamboard member sentenced to life in prison for participating in international criminal network organized to sexually exploit children", 6 September 2012.

2. Groups that operate offline and online

The groups that operate offline and online and engage in crimes and cybercrimes are known as hybrids.[47] This group includes two subcategories: clustered hybrids and extended hybrids.

(a) Clustered hybrids

A clustered hybrid refers to a group that engages in certain activities and/or uses specific methods to commit a cybercrime. The clustered hybrid has a structure similar to that of the hub. What differentiates them is the clustered hybrid's movement between offline and online activities and its ability to execute its operations both online and offline. These groups are often focused on specific crimes and cybercrimes, use certain tactics, have an identifiable method of operation and/or operate within a specific location.[48] Like hubs, these groups are predominantly profit-driven. A typical example of a clustered hybrid group is one that engages in automatic teller machine (ATM) skimming[49] and then uses the data to make online purchases or sells the data in online carding forums.[50]

Clustered hybrid groups have engaged in other forms of fraud. For instance, an organized criminal group based in the United Kingdom perpetrated an international Internet fraud targeting individuals in the United States of America who advertised rental properties.[51] Specifically, the members of the clustered hybrid group, using fraudulent identities, pretended to be interested renters, contacting the individuals advertising the property and offering them money (i.e., a deposit and rent). If the targeted individuals responded, the perpetrators would send money – in the form of a forged cashier's cheque – in excess of what was being asked. The perpetrators would then contact the individuals and claim that the excess money had been sent accidentally and request that the excess money be sent back to them via a well-known money transfer service. In some instances, the perpetrators convinced the individuals to send by money order the entire amount of the cheque. In other instances, the individuals, realizing that this was a scam, did not send any money.

(b) Extended hybrids

An extended hybrid is more sophisticated and less centralized and has a less obvious core than a clustered hybrid. Extended hybrids are made up of associates and subgroups that commit various criminal activities. They are not as well defined as clustered hybrids and their composition is more complex. Darknet market communities (such as Silk Road, Silk Road 2.0 and Dream Market), which have administrators and moderators (who oversee and run the sites), vendors (who sell illegal goods and services (internationally controlled drugs, counterfeit documents and money, hacking tools and services, etc.)), buyers (who purchase illicit goods and services) and suppliers (who provide the goods to the vendors), are loosely interrelated and could be classified as extended hybrids.[52] This would depend on the nature of the darknet community, the complexity of its operations and structure, and the breadth of its illicit activities. Some darknet communities that focus on one cybercrime and are not as complex in their composition could be considered clustered hybrids.

[47] Broadhurst and others, "Organizations and cybercrime"; BAE Systems Detica and John Grieve Centre for Policing and Community Safety, London Metropolitan University, *Organised Crime in the Digital Age* (2012); UNODC, *Comprehensive Study on Cybercrime*, draft.

[48] See also UNODC, Education for Justice University Module Series, Cybercrime, Module 13: cyber organized crime, "Criminal groups engaging in cyber organized crime".

[49] For further information about automated teller machine (ATM) skimming, see chap. V, sect. B.1.

[50] United States, Eastern District of New York, *United States of America v. Jael Mejia Collado et al.*, Case No. 13 CR 259 (KAM), Superseding Indictment, May 2013; *United States of America v. Ercan Findikoglu*, Case No. 1:13-CR-00440, Indictment, 24 June 2015.

[51] England and Wales Court of Appeal, *Regina v. Sunday Asekomhe* [2010] EWCA Crim 740, p. 1.

[52] See, for example, *United States of America v. Gary Davis*, Case No. 1:13-CR-950-2; *United States of America v. Ross William Ulbricht*, Case No. 15-1815; *United States of America v. Brian Richard Farrell*, Case No. 2:15-CR-29-RAJ; *United States of America v. Gal Vallerius* (Dream Market).

3. Groups that predominantly operate offline

Some organized criminal groups predominantly operate offline and only use ICT to expand or support illicit offline activities and operations. These groups are hierarchical, are typically comprised of traditional organized criminal groups and have sought to expand certain illicit activities online, such as gambling, extortion, prostitution and trafficking in persons.[53] In *United States of America v. Locascio et al.*, members and associates of the "Gambino Family of La Cosa Nostra" carried out an Internet scheme involving adult entertainment websites with the intention of defrauding visitors to those sites. (Free tours advertised on the site were used to lure visitors to ultimately enter their credit card details under the guise that this was needed to verify their age. The credit card details were then used to make fraudulent transactions.)[54] In Italy, associates of the Camorra and 'Ndrangheta ran an Internet gambling ring (Dollaro Poker).[55]

B. Roles within a cyber organized criminal group

Cyber organized criminal groups operate as legitimate enterprises with employees hired in various roles, such as technical and other support personnel, marketing personnel and "employees" in charge of the receipt and distribution of payments to other members; in addition, they have rules and codes of conduct that govern members' behaviour.[56] When a specialized skill or ability is needed, these groups hire others to complete the tasks.[57]

The roles within a cyber organized criminal group vary depending on the cybercrime committed and any offline activities that are involved in the execution of the tasks associated with the illicit acts and/or the achievement of the group's objectives. Perpetrators of interpersonal cybercrimes, such as online child sexual abuse and exploitation, have roles that differ from the roles of groups that predominantly engage in cyber-dependent crimes. Cyber organized criminal groups that mainly commit interpersonal cybercrime assign certain roles to members, such as identifying, recruiting and ultimately enticing a minor to engage in a sex act[58] or identifying, creating, obtaining and sharing child sexual abuse and exploitation material.[59] In contrast, cyber organized criminal groups that conduct cyber-dependent crimes would have certain roles relating to the tools and technology needed to conduct cybercrimes, such as:[60]

(a) Coders. Individuals responsible for developing malware, exploits (programs, or pieces of code, designed to find and take advantage of security flaws or vulnerabilities in an application or computer system) and other tools used to commit cybercrime (e.g., they can build custom exploits for a fee);

(b) Hackers. Individuals responsible for exploiting vulnerabilities in systems, networks and applications;

---

[53] BAE Systems Detica and John Grieve Centre for Policing and Community Safety, London Metropolitan University, "*Organised crime in the digital age*" (2012); UNODC, *Comprehensive Study on Cybercrime*, draft; Broadhurst and others, "Organizations and cybercrime"; see also UNODC, Education for Justice University Module Series, Cybercrime Module 13: cyber organized crime, "Criminal groups engaging in cyber organized crime".

[54] United States District Court, Eastern District of New York, *United States of America v. Salvatore Locascio et al*., 357F. Supp. 2d 536, 28 September 2004.

[55] Italy, Cass., 31 Marzo 2017, No. 43305.

[56] Europol, *Internet Organised Crime Threat Assessment 2020* (The Hague, 2020), p. 31; *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus* (Bayrob Group); Hungary, *Prosecution v. Baksa Timea and others* (SHERLOC Case No. HUNx003).

[57] Ibid.

[58] See, for example, Canada, Provincial Court of Saskatchewan, *R v. Chicoine*, 2017 SKPC 87, 14 November 2017; United States District Court, Eastern District of Michigan, *United States of America v. Caleb Young*, Case No. 18-20128, Sentencing Memorandum, 11 May 2018; **Costa Rica,** Tribunal Penal del Tercer Circuito Judicial de San José, Causa penal número 15-001824-0057-PE & Causa Penal número 19-000031-0532-PE (Operación R-INO).

[59] See, for example, Argentina, Tribunal Oral Federal de Jujuy, Causa FSA 8398/2014/TO1; *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard); Germany, Federal Court of Justice, Decision 2 StR 321/19, of 15 January 2020 (BGH, Beschluss vom 15.01.2020, 2 StR 321/19) (the Giftbox Exchange and Elysium).

[60] Chabinsky, "The cyber threat"; Broadhurst and others, "Organizations and cybercrime"; United States, Western District of Pennsylvania, *United States of America v. Alexander Konovolov et al.,* Case No. 2-19-CR-00104 (GozNym Malware), Indictment Memorandum, 17 April 2019, p. 3.

(c) Technical support. Individuals who provide technical support for the group's operations, including the maintenance of infrastructure and the technologies used;

(d) Hosts. Individuals who host illicit activities either on servers or offline physical locations. Bulletproof hosting services, for example, offer to host illicit activities on servers that are designed to evade law enforcement and security detection and enable illicit activities to continue uninterrupted.

These roles are often identified in organized criminal groups that provide crime as a service (i.e., provide services that facilitate crimes and/or cybercrimes).[61] In addition to hacking, malware and hosting, the illicit services offered include the provision of exploit toolkits or information about system vulnerabilities and ways to exploit those vulnerabilities, as well as tutorials for various cybercrimes.

Cyber organized criminal groups can have members or associates that serve as specialists. These individuals specialize in a specific cybercrime or other crime or in a tactic or method to commit a cybercrime. An example of a specialist is an individual who develops "crypters", software tools that encrypt malware so that it can evade detection by antivirus programs on devices.[62] Organized criminal groups can also have members or associates who are suppliers and distributors of illicit goods and services.[63] In addition, organized criminal groups may use "cashers", who convert illicit goods to money, steal money from targets and distribute it to group members, or otherwise make the proceeds from the group's illicit activities available to group members.[64] The "cashers", who are also known as "runners" or "strikers", may be used to withdraw or transfer money online or at a physical establishment, such as a bank.[65] Furthermore, these groups may use "money mules", who obtain and transfer money illegally upon request and payment,[66] to launder the proceeds of their cybercrimes.[67]

Some of the roles within cyber organized criminal groups are transient and the persons in these roles only participate in the group until they fulfil their purpose. One example of a person in a temporary role is a specialist[68] who can be hired by the organized criminal group to create malware for later distribution by the group. Moreover, all members of the group are not valued equally and/or considered important. Even in certain online illicit forums, members of the forum were ranked; in some cases, VIP status was granted to elite members of the group.[69] Furthermore, some members of the group may be considered expendable. For instance, "money mules" who are solicited online and asked to open bank accounts (or use their own accounts) and receive money from others (or asked to mail or physically move packages by receiving them and forwarding, sending or taking the packages to their destination) are often considered by the group to be expendable (especially if they unwittingly participate in this activity).

[61] Maras, *Cybercriminology.*

[62] *United States of America v. Alexander Konovolov et al.* (GozNym malware), p. 3.

[63] Ibid.

[64] Ibid.

[65] Canada, Ontario Court of Justice, *R. v. Kalonji,* 2019 ONCJ 341, 17 May 2017, para. 7.

[66] Maras, *Cybercriminology*, p. 337.

[67] See, for example, *United States of America v. Alexander Konovolov et al.* (GozNym malware) and *United States v. Aleksei Yurievich Burkov* (Card Planet).

[68] Specialists can also be permanent members of the group.

[69] See, for example, United States District Court, District of Nevada, *United States v. Svyatoslav Bondarenko et al.*, Case No. 2:17-CR-306-JCIVI-PAL (Infraud), Second Superseding Criminal Indictment, 30 January 2018; *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard).

Tribunal de grande instance de Paris, 13e chambre correctionnelle, 20 novembre 2018 (France)

The Federal Bureau of Investigation (FBI) of the United States conducted an operation known as "Operation Card Shop", whereby it established an undercover carding forum (Carder Profit) that was used to identify cybercriminals exchanging illict goods and services relating to "carding" (the use, sale, sharing or otherwise distribution of stolen credit card or debit card data in order to commit cybercrime and other forms of crime).

As a result of the operation, a number of persons were arrested and taken to court in France. Information on that case is provided below.

From 2010 to 2014, the defendant (Z.) ran a criminal enterprise that engaged in online fraud. To this end, Z. used stolen credit card data found on carding forums by himself, P. (the "technical advisor" of the group) and N. (a member of the group in charge of finding credit card data), as well as credit card data stolen by L. from his former employer. The defendants (P. and Z.) would then hack into customer accounts on commercial websites and modify the contact information so that the actual customers would not receive any notifications of purchases and/or deliveries. Z. and N. would buy goods on commercial websites and send them to shipping points. Z. and X. forged fake identification to be used by "mules" to receive the packages at the shipping points. Several persons (Y., M., O., Q., V., T. and R.) were used as "mules". They would each receive the packages, keeping some packages as payment and sending others to Z. so he could sell them on retailer websites. Several people involved in this criminal organization later started using the same techniques to buy goods for themselves. Z. and V. were also found to be in possession of ATM skimmers that they intended to use to obtain more credit card data. The group managed to place about 2,000 orders on online commercial websites for an amount estimated to be €40,000–€60,000.

One of the 15 defendants was acquitted and the other 14 were convicted of several offences, depending on their degree of involvement in the fraud. The convictions ranged from complicity to commit fraud as part of a organized criminal group to participation in an organized criminal group, illegal access to a data system and illegal acquisition of computer data as part of an organized criminal group. For those convicted for their participation in an organized criminal group, the French court highlighted the difference between the notions of "bande organisée" and of "association de malfaiteurs" in French law. According to French law, "bande organisée" is used as an aggravating circumstance to an already existing offence, whereas an "association de malfaiteurs" is a separate criminal offence as such. The acts of defendants cannot be prosecuted as both "bande organisée" and "association de malfaiteurs" if the acts are inextricably linked together. The court held that it could not convict the defendants for both "bande organisée" and "association de malfaiteurs" as it related to the cyber organized crime they had committed. Ultimately, only Z. and V., who had taken part in the ATM skimming scheme, were convicted for participating in an "association de malfaiteurs".

The defendants were given sentences of imprisonment ranging from six months to two years. For all but four of the defendants in this case (Z., V., P. and N.), the sentences were suspended. Z. and V. were sentenced to 2 years and to 15 months of imprisonment, respectively, and were required to pay €3,000 and €2,000, respectively, in fines to the state and €10,200 in compensation to the victims. P. and N. were sentenced to 15 months and to 18 months of imprisonment, respectively, and were required to pay fines of €2,000 to the state and €10,200 in compensation to the victims.

For more information about this case, see UNODC, SHERLOC case law database, Case No. FRAx030.[a]

[a] Available at https://sherloc.unodc.org/.

C. Geographical organization

The perpetrators of cyber organized crime may be part of a group in which the offenders may or may not be in geographical proximity. The cases included in the digest represent a variety of regions. Research has shown that geographical proximity between perpetrators has played some role in the formation and expansion of cyber organized criminal groups.[70] For example, in *HKSAR v Chan Pau Chi*,[71] 15 defendants in Hong Kong, China, were charged with and convicted for a range of offences, including money-laundering and conspiracy relating to the illegal facilitation of prostitution online via websites (i.e., through the advertisement and promotion of services). Nevertheless, other cyber organized criminal groups form and thrive even when there is little or no geographical proximity between their members.[72] There have been a number of cases indicating that the members of a darknet site (administrators, moderators, vendors, buyers and suppliers) can be from anywhere in the world.[73]

Police v. Zhong [2017] WSDC 7 (Samoa)

The case *Police v. Zhong* involved automatic teller machine (ATM) skimming in Samoa undertaken by three nationals of China, two of them being defendants in the case, causing 47,350 tala in damage. On 24 August 2016, an employee reported suspicious activity involving the use of ATMs. Over 30 cards had been used and captured by ATMs at various bank locations. The cards had never been seen before, and their appearance was different from that of normal ATM cards. In addition, when the bank employees examined the trial balance report for the Matautu ATM for the previous day, they noticed a number of complete and incomplete transactions corresponding to the suspicious cards. One of the employees was instructed to check the ATM cameras and obtain video footage of the suspicious transactions. After viewing the footage, the employees contacted the police.

The police officers subsequently went to a location in Matautu, Samoa, that included a restaurant, a shop and accommodations, where the two defendants could be identified. The police called for backup, searched the living quarters of the defendants and found and seized, inter alia, over 100 suspicious ATM cards and three ATM skimming devices. The defendants were arrested. In some of the video footage produced in evidence, a third national of China could be seen participating in the offences. That man had already left the country at the time of the defendants' arrest and was not a party to the proceedings.

The two male defendants (Z.S. and Y.Q.) were charged with several offences involving theft; intentionally accessing an electronic system without authorization; dishonestly accessing an electronic system and thereby obtaining a benefit; and intentionally possessing a card skimming device for the purpose of committing an offence. While some of the theft charges were subsequently dismissed or reduced, on 7 July 2017, the defendants were each sentenced to five years' imprisonment for theft or stealing,[a] accessing an electronic system without authorization,[b] accessing an electronic system for dishonest purpose,[c] and possession of illegal devices.[d]

[a] Samoa, Crimes Act of 2013, paras. 161 and 165 (b).
[b] Ibid., para. 206.
[c] Ibid., paras. 33 and 207.
[d] Ibid., paras. 33 and 213 (a).

[70] Broadhurst and others, "Organizations and cybercrime"; Eric Rutger Leukfeldt, Anita Lavorgna and Edward R. Kleemans, "Organised cybercrime or cybercrime that is organized? An assessment of the conceptualization of financial cybercrime as organised crime", *European Journal in Criminal Policy and Research*, vol. 23, No. 3 (September 2017), pp. 292–293.

[71] Hong Kong, China, *HKSAR v. Chan Pau Chi* [2019] HKEC 1549.

[72] See, for example, *United States of America v. Alexander Konovolov et al.* (GozNym malware).

[73] See, for example, *United States of America v. Gary Davis*, Case No. 1:13-CR-950-2; *United States of America v. Ross William Ulbricht*, Case No. 15-1815; *United States of America v. Brian Richard* Farrell, Case No. 2:15-CR-29-RAJ; *United States of America v. Gal Vallerius* (Dream Market).

D. Gender and cyber organized crime

The demographic characteristics of offenders and victims vary, depending on the type of cybercrime. In the cases included in this digest, the offenders were predominantly male. The members of organized criminal groups were either all male or predominately male, with a few exceptions (in some cases, men and women were more equally represented; in others, however, there were more women than men).[74] The roles of offenders in organized criminal groups vary by gender. Male offenders were predominantly in leadership roles, whereas women primarily served in other roles, such as recruiters, coders, specialists and organizers.[75] There are exceptions to this (see the box below). While the gender of victims was not identified in many of the cases included in the digest, there were exceptions in cases involving trafficking in persons and child sexual abuse and exploitation.[76]

The findings in this section are based solely on the cases included in the digest and are thus not generalizable.

United States of America v. Melissa Scanlan, Case No. 18-CR-30141-NJR-1 & Case No. 19-CR-30154-NJR-1 (S.D. Illinois, 20 October 2019) (The Drug Llama) (United States of America)

M.S. (a female) and another conspirator B.A. (a male) used the computer moniker "The Drug Llama" on a vendor account on Dream Market (a darknet site) to sell counterfeit tablets containing fentanyl and acetyl fentanyl.[a] M.S. was responsible for sourcing the drugs that would be sold using the vendor account, while B.A. was responsible for receiving and fulfilling darknet drug orders, as well as the management of the account.[b] M.S. and B.A. received fentanyl and other drugs from Mexico, predominantly from F.R. and another (unnamed) member of the Mexican cartel. After M.S. and B.A. sold the drugs, they kept a portion of the criminal proceeds and gave the rest to couriers (usually N.D. and A.K., both females). The couriers would transport the proceeds across the border between Mexico and the United States and deliver them to F.R. and another member of a Mexican cartel.[c] It has been estimated that 52,000 counterfeit tablets containing fentanyl and acetyl fentanyl tablets were sold in a single year.[d]

M.S. was charged with and convicted of conspiracy to distribute fentanyl;[e] distribution of fentanyl;[f] sale of counterfeit drugs;[g] misbranding of drugs;[h] international money-laundering conspiracy;[i] and distribution of fentanyl resulting in death.[j] She pleaded guilty and was sentenced to 13 years and 4 months of imprisonment.[k] B.A. was charged with and convicted of conspiracy to distribute fentanyl;[l] distribution of fentanyl;[m] sale of counterfeit drugs;[n] and misbranding of drugs.[o] He pleaded guilty and was sentenced to 9 years' imprisonment.[p]

[74] See, for example, France, Tribunal de grande instance de Paris, 13e chambre correctionnelle, 20 novembre 2018; United States, Southern District of Illinois, *United States of America v. Melissa Scanlan*, Case No. 18-CR-30141-NJR-1 and Case No. 19-CR-30154-NJR-1, Stipulation of facts, 20 October 2019, p. 4; *HKSAR v. Chan Pau Chi* [2019] HKEC 1549.

[75] See, for example, *United States of America v. Dennis Collins* et al., Case No. 11-CR-00471-DLJ (PSG); United States, Eastern District of Virginia, *United States of America v. Daniel Palacios Rodríguez, Alexandra Guzmán-Beato, Elvis Pichardo Hernández, José David Reyes-González, Juan Rufino Martínez-Domínguez, and Fátima Ventura Pérez,* Case No. 1:19-MJ-286, Affidavit in support of criminal complaint and arrest warrant, 24 June 2019.

[76] See, for example, Canada, *R v. Philip Michael Chicoine*; Canada, Nova Scotia Court of Appeal, *R v. Pitts*, 2016 NSCA 78; *United States of America v. Caleb Young*; and Germany, Federal Court of Justice, Decision 2 StR 321/19, of 15 January 2020 (BGH, Beschluss vom 15.01.2020, 2 StR 321/19).

For more information on this case, see UNODC, SHERLOC case law database, Case No. USAx187.[q]

[a] *United States of America v. Melissa Scanlan*, p. 4.
[b] *United States of America v. Brandon Arias*, Case No. 18-CR-30141-NJR-2, Stipulation of Facts (S.D. Illinois, 16 July 2019), pp. 4–5.
[c] *United States of America v. Melissa Scanlan*, p. 5.
[d] Ibid., p. 4.
[e] United States Code, Title 21, sect. 846.
[f] Ibid., sect. 841.
[g] Ibid., sect. 331 (1) (3).
[h] Ibid., sect. 331(A).
[i] United States Code, Title 18, sect. 1956 (H).
[j] United States Code, Title 21, sect. 846; United States, Southern District of Illinois, *United States of America v. Melissa Scanlan*, Plea Agreement, Case No. 18-CR-30141-NJR-1 and Case No. 19-Cr-30154-NJR-1, 30 October 2019, pp. 1–2.
[k] United States Attorney's Office, Southern District of Illinois, "Dark web fentanyl trafficker known as 'The Drug Llama' sentenced to 13 years in federal prison", press release, 12 February 2020.
[l] United States Code, Title 21, sect. 846.
[m] Ibid., sect. 841.
[n] Ibid., sect. 331 (1) (3).
[o] Ibid., sect. 331 (A).
[p] United States Attorney's Office, Southern District of Illinois, "Brandon Aria, a/k/a 'the Drug Llama', sentenced to 9 years for distributing fentanyl on the dark web", 12 November 2019.
[q] Available at **https://sherloc.unodc.org/**.

CHAPTER IV.

TOOLS USED BY PERPETRATORS OF CYBER ORGANIZED CRIME

IV. TOOLS USED BY PERPETRATORS OF CYBER ORGANIZED CRIME

Perpetrators of cyber organized crime leverage ICT to commit a variety of cyber-dependent and cyber-enabled crimes on the clearnet and the darknet. The clearnet refers to the visible (or surface) web and includes websites that are indexed using traditional search engines (Google, Bing, etc.). The deep web is composed of sites that are not indexed by traditional search engines and thus are not easily accessible by the general public. The sites located on the deep web can include intranet sites and password-protected sites, as well as sites that require specialized software to access them, such as the Onion Router (Tor), Freenet or the Invisible Internet Project (I2P). The sites that are part of an overlay network that can only be accessed using specialized software are known as darknet sites.

LG Duisburg, Urteil vom 05.04.2017, 33 KLs – 111 Js 32/16 – 8/16 (Germany)

This case concerns the proceedings of six defendants involved in trafficking illegal goods online. Two so-called underground economy forums, "d.cc" and "g.me" (the latter replaced another forum of the founder and administrator N2, who was separately prosecuted), were established for the purpose of selling and/or purchasing illegal goods and exchanging information that could subsequently be used for committing criminal offences. The illegal goods and data available for sale on the forum mainly included drugs, false documents, counterfeit money and stolen personal data. The forums were accessible by conventional browsers via the clearnet and could be found using popular search engines. In addition, the forums were accessible by a number of special browsers, such as the Tor browser, via the darknet.

In order to register for the forums, users had to provide an email address and username for use on the platform and then contact N2 to activate the accounts. In addition to hosting advertisements for illicit goods, both forums provided a platform to exchange information with other users on topics such as anonymizing and ways to protect against law enforcement detection and the dissemination of malware. Because of mistrust between the anonymous users, some of the transactions in the forums were concluded via escrow service for a fee.

H., G. and X. had leadership roles on the underground economy forums. Defendant H. was responsible for the technical aspects of the forums, such as maintaining servers and the security of the forums. He held the positions of administrator, moderator and trustee, who received fees paid by users of the escrow service. Defendant G. held the position of moderator and was responsible for checking the compliance of user postings with forum rules and sanctioning users where necessary. He also acted as a trustee for three transactions, sold official documents in one case and acquired counterfeit money twice. Defendant X. held the position of "supermoderator" and mainly provided technical support (e.g., the establishment and maintenance of the technical infrastructure of one of the forums). He also created a "scene guide" that provided users with tips on committing criminal offences, as well as information on how to avoid identification by law enforcement officers. The defendant was also involved in the establishment and maintenance of the technical infrastructure of one of the forums ("g.me"). The defendants did not know each other in person but were in close contact for organizational purposes and communicated through areas of the forums that were accessible only to members in leadership positions and through various other encrypted messenger services.

The defendants were charged with and convicted of computer fraud (H.), attempted computer fraud (H.), illegally acquiring narcotic drugs (X.), aiding and abetting illicit trading in narcotic drugs in quantities which are not small (G., H. and X.), aiding and abetting illicit trading in narcotic drugs (G., H. and X.), aiding and abetting counterfeiting of money (G., H. and X.), aiding and abetting

procurement of false official identity documents (G., H. and X.) and counterfeiting of money (G.). The court sentenced H. to 21 months' imprisonment, G. to 12 months' imprisonment and X. to 14 months' imprisonment. The creator of the underground economy forums and several other persons were also charged with and, in separate trials, convicted of crimes relating to the forums.

For more information on this case, see UNODC, SHERLOC case law database, Case No. DEUx025.[a]

[a] Available at https://sherloc.unodc.org/.

Criminals exploit legitimate commercial services to further their illicit ends online.[77] Case law has revealed that perpetrators of cyber organized crime have searched for targets on dating sites, social media platforms and live broadcasting services on the clearnet.[78] Social media platforms have also been used by organized criminal groups to communicate with members, advertise illicit goods and services, exchange illicit goods (e.g., stolen and counterfeit identity documents) and facilitate or carry out illicit activities.[79] Moreover, illicit goods and services have also been advertised on licit online marketplaces and online classified advertisement sites.[80]

United States of America v. Carl Allen Ferrer, Case No. 18 CR. 464 (D. Arizona, 5 April 2018) (Backpage) (United States of America)

Backpage was a classified advertisement website that included a section for advertisements for sexual services. Among the sexual services advertised on Backpage were sexual services by trafficked women and children. Charges had been unsuccesfully brought against Backpage for its facilitation of trafficking in persons and prostitution.[a] A report published by the Permanent Subcommittee on Investigations, the chief investigative subcommittee of the United States Senate Committee on Homeland Security and Governmental Affairs, revealed that Backpage had knowingly sanitized advertisements published on its site in order to conceal crimes.[b] Specifically, the report revealed that Backpage had knowingly facilitated trafficking in persons by editing advertisements that openly advertised human beings for sexual services and posting them online instead of denying them access to the platform.[c]

In April 2018, Backpage was seized by law enforcement authorities in the United States. Founders, higher-level executives and managers of Backpage were charged with offences that included conspiracy to facilitate prostitution and conspiracy to commit money-laundering.[d] The chief executive officer and one of the founders of Backpage, C.F., pleaded guilty to conspiracy to commit offence or to defraud the United States, in violation of Title 18 of the United States Code (sect. 371).[e] In his plea agreement, he acknowledged that the majority of revenue for the site had come from illegal advertisements and that Backpage had used bank accounts for shell companies and cryptocurrency processing companies (i.e., CoinBase, Crypto Capital, GoCoin, Kraken and Paxful) to conceal the source of its revenue.[f] He also acknowledged in his plea deal that he had conspired to sanitize advertisements by removing words and photographs that were indicative of prostitution.[g] As part

[77] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 17.

[78] United States Court of Appeals for the Fifth Circuit, *United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase and Rasaq Aderoju Raheem*, Case No. 17-60397 (5th Circuit, 4 March 2019. The defendants created fake profiles on dating sites to identify targets and lure them into a fake relationship (*United States of America v. Caleb Young* (Bored Group)).

[79] See, for example, United States District Court, Eastern District of Virginia, *United States v. Ramiro Ramirez-Barreti et al.*, Criminal Case No. 4:19-CR-47, Second Superseding Indictment, 14 August 2019, p. 12; United States District Court, Western District of North Carolina, *United States v. Anthony Blane Byrnes,* Case No. 3:20-CR-192.

[80] See, for example, *United States of America v. Daniel Palacios Rodríguez, Alexandra Guzmán-Beato, Elvis Pichardo Hernández, José David Reyes-González, Juan Rufino Martínez-Domínguez, and Fátima Ventura Pérez.*

United States of America v. Carl Allen Ferrer, Case No. 18 CR. 464 (D. Arizona, 5 April 2018) (Backpage) (United States of America) (*continued*)

of the plea deal, C.F. is required to forfeit the company's assets and property, take all the steps in his power to permanently shut down Backpage and testify that Backpage engaged in money-laundering and facilitated prostitution. He has not yet been sentenced. A "sales and marketing director" of Backpage, D.H., also pleaded guilty to conspiracy to facilitate prostitution in a scheme designed to provide free advertisements to sex workers in order to draw them away from Backpage's competitors. The trials of another six persons affiliated with Backpage (M.L, J.L., S.S., J.B., A.P. and J.V), which include the other two founders of Backpage (M.L and J.L.), were postponed until 2021.

The Backpage case held an Internet intermediary liable for its role in the facilitation of serious crimes. Article 10 of the Organized Crime Convention requires States parties to the Convention to establish the liability of legal persons for participation in serious crimes involving an organized group.[h] Where Internet intermediaries with legal personhood are themselves involved in the commission of serious crimes involving an organized criminal group, article 10 requires that States parties have in place legislation under which the intermediaries can be found liable. Furthermore, States parties must ensure that legal persons held liable in accordance with article 10 are subject to effective, proportionate and dissuasive sanctions.[i]

Unlike the aforementioned case of Backpage, in the vast majority of cases, online intermediaries are not themselves involved in the commission of serious crimes, but rather their services are abused by criminals to carry out offences. In such circumstances, cooperation between online intermediaries and law enforcement authorities is critical. The Organized Crime Convention envisions a degree of cooperation between the law enforcement agencies and prosecutors and the private sector in the prevention of organized crime.[j] The Conference of the Parties to the United Nations Convention against Transnational Organized Crime has encouraged the private sector to strengthen its cooperation and work with States parties to the Convention and the Protocols thereto in order to achieve the full implementation of those instruments.[k]

For more information on this case, see UNODC, SHERLOC case law database, Case No. USAx169.[l]

[a] United States District Court, District Court of Massachusetts, *Doe v. Backpage.com LLC*, 104 F. Supp. 3d 149, 15 May 2015; United States, Superior Court of the State of California, *The People of California v. Carl Allen Ferrer, Michael Lacey and James Larkin*, Case No. 16FE024013, 23 December 2016; Marie-Helen Maras, "Online classified advertisement sites: pimps and facilitators of prostitution and sex trafficking?", *Journal of Internet Law*, vol. 21, No. 5 (November 2017), pp. 17–21.

[b] United States Senate, Permanent Subcommittee on Investigations, *Backpage.com's Knowing Facilitation of Online Sex Trafficking* (Washington, D.C., Committee on Homeland Security and Governmental Affairs, 2017).

[c] See also UNODC, Education for Justice University Module Series, Trafficking in persons and smuggling of migrants, Module 14: links between cybercrime, trafficking in persons and smuggling of migrants, "Technology facilitating trafficking in persons". Available at www.unodc.org/.

[d] United States District Court, District of Arizona, *United States of America v. Michael Lacey, James Larkin, Scott Spear, John "Jed" Brunst, Dan Hyer, Andrew Padilla and Joye Vaught*, Case No. 18 CR. 422, Indictment, 28 May 2018.

[e] United States District Court, District of Arizona, *United States of America v. Carl Allen Ferrer*, Case No. 18 CR. 464, Plea Agreement, 5 April 2018, p. 2.

[f] Ibid., pp. 13–14.

[g] Ibid., p. 13.

[h] United Nations Convention against Transnational Organized Crime, art. 10, para. 1.

[i] Ibid., art. 10, para. 4.

[j] Ibid., art. 31, para. 2 (a).

[k] CTOC/COP/2012/15, resolution 6/1.

[l] Available at https://sherloc.unodc.org/.

In its report entitled *Internet Organised Crime Threat Assessment 2020*, the European Union Agency for Law Enforcement Cooperation (Europol) revealed that perpetrators of cyber organized crime communicated via encrypted means (e.g., Protonmail, Tutanota and cock.li).[81] Case law has revealed that unencrypted and encrypted messaging applications were used not only for communications between perpetrators

[81] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 27.

of cyber organized crime, but also to identify and target victims and commit cybercrimes.[82] In addition to the use of mainstream communication platforms and devices, instant messaging, messaging platforms on websites, proprietary communication platforms and tools have been developed and marketed exclusively to criminals (e.g., Phantom Secure (see the box below)).[83]

United States of America v. Vincent Ramos et al., Case No. 18-CR-01404-WQH (S.D. California, 2 October 2018) (Phantom Secure) (United States of America)

Phantom Secure, a company based in Canada, modified existing BlackBerry phones by removing key features that could be used to track and keep under surveillance users of the devices, such as the camera, microphone and Global Positioning System (GPS), and operated an encrypted network that enabled its devices to send and receive encrypted communications.[a] Traffic was routed through international proxy servers that were located in countries that the company believed did not cooperate with foreign law enforcement agencies.[b] These measures were taken to prevent law enforcement agencies from accessing the devices and intercepting communications. The devices were not available to the general public and could be obtained only through a referral from an existing user of the device and only after the person had been vetted (i.e., a background check was conducted using open source resources to verify the identity of the person).[c] To further protect the identities of those utilizing the devices, the real names and other personally identifying information about users were not collected.[d] Moreover, Phantom Secure would wipe devices that had been seized by a law enforcement agency, destroying evidence that the devices contained by making unreadable the data stored on them. Phantom Secure also suspended service and deleted the contents of a device if it was suspected that a law enforcement officer or an informant was using the device as part of a law enforcement investigation.[e] Phantom Secure thus obstructed justice by concealing evidence from law enforcement authorities and destroying it.

The organizational structure of the Phantom Secure criminal enterprise included individuals with roles as administrators, distributors and agents. Administrators included Phantom Secure's corporate executives and staff in the front office who had physical control of the Phantom Secure network, Phantom Secure's books and records and its corporate operations. Administrators could initiate new subscriptions, remove accounts and remotely wipe and reset devices. As the chief executive officer of Phantom Secure, the defendant V.R. was its lead administrator. K.A.R. was also alleged to have served as an administrator of Phantom Secure. An unnamed individual (only identified as Individual A in court documents) was said to have held an integral role in the design and maintenance of the security integrity of Phantom Secure. Distributors coordinated agents and resellers of Phantom Secure devices and received payments for ongoing subscription fees, which they transferred, minus a personal commission, back to Phantom Secure. They also provided technical support and communicated directly with Phantom Secure administrators. Y.N., C.P. and M.G. were all alleged to have been distributors for Phantom Secure. Agents physically sourced and engaged with new customers to sell and deliver Phantom Secure devices. They earned a profit on the sale of the handset and provided first-level technical support to their customers.

[82] See, for example, United States District Court, Eastern District of Virginia, *United States v. Ramiro Ramirez-Barreti et al.*; United States District Court, Southern District of California, *United States of America v. Cristian Hirales-Morales, Marcos Julian Romero and Sergio Anthony Santivanez*, Case No. 19-CR-4089-DMS, Indictment, 10 October 2019; *R v. Philip Michael Chicoine*.

[83] See, for example, *United States of America v. Svyatoslav Bondarenko et al.*, p. 22 (Infraud); *United States of America v. Caleb Young* (Bored Group); *United States of America v. Beniamin-Filip Ologeanu*, Superseding Indictment No. 5:19-CR-10, 6 February 2019, pp. 10–11; United States District Court, Northern District of Ohio, *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus*, p. 6 (Bayrob group); United States District Court, Eastern District of Kentucky, *United States of America v. Andre-Catalin Stoica et al.*, Criminal Indictment No. 5-18-CR-81-JMH, 5 July 2018, p. 16 (Alexandria Online Fraud Network); *United States of America v. Ramiro Ramirez-Barreti et al.*; UNODC, SHERLOC case law database, Case No. DEUx033, LG Leipzig, Urteil vom 14.06.2012, 11 KLs 390 Js 191/11.

***United States of America v. Vincent Ramos et al.*, Case No. 18-CR-01404-WQH (S.D. California, 2 October 2018) (Phantom Secure) (United States of America) (*continued*)**

The defendant was charged with racketeering conspiracy to conduct enterprise affairs in violation of Title 18 of the United States Code (sect. 1962) and conspiracy to aid and abet the distribution of a controlled substance in contravention of Title 21 of the United States Code (sects. 841 (a), para. (1), and 846). The defendant was sentenced to nine years' imprisonment. The defendant was also ordered to be on supervised release for a term of three years following his release from imprisonment. The defendant was further required to forfeit assets and to pay a fine of US$ 100.

This case was significant because it was the first time the United States had prosecuted and convicted an executive of a company for knowingly providing transnational criminal organizations with encrypted infrastructure to conduct the international importation and distribution of narcotic drugs. This case shows how organized criminal groups are adapting to use improved forms of technology to communicate and evade detection and apprehension. It also shows the challenges faced by law enforcement authorities in investigating and prosecuting increasingly sophisticated organized criminal groups.

For more information on this case, see UNODC, SHERLOC case law database, Case No. USAx154.[f]

[a] United States District Court, Southern District of California, *United States of America v. Vincent Ramos*, Case No. 18-MJ-0973, Complaint, 15 March 2018, pp. 5–6.
[b] Ibid., p. 6.
[c] United States District Court, Southern District of California, *United States of America v. Vincent Ramos et al.*, Case No. 3:18-CR-01404-WQH, Criminal Indictment, 15 March 2018, p. 3; *United States of America v. Vincent Ramos*, Complaint, p. 6.
[d] *United States of America v. Vincent Ramos.*
[e] United States District Court, Southern District of California, *United States of America v. Vincent Ramos*, Case No. 18-CR-01404-WQH, Plea Agreement, 2 October 2018, p. 6.
[f] Available at **https://sherloc.unodc.org/**.

Criminals have utilized wire transfers, cashier's cheques, money orders, gift cards and prepaid cards, as well as online payment and money transfer services, to send and receive the proceeds of cybercrime.[84] Other services distribute digital currency[85] either through a single centralized authority or peer-to-peer, without any central oversight. These currencies can be convertible (i.e., they have an equivalent value in fiat currency or they can be used as a substitute for fiat currency) or non-convertible (i.e., they do not have an equivalent value in fiat currency, they cannot be substituted for fiat currency and they can be used only in the domain or domains for which they were created, such as a gaming platform).[86] Case law has revealed that digital currencies, such as Liberty Reserve, were used to conceal crimes and distribute proceeds of crimes between members and associates.[87]

[84] For example, the Alexandria Online Fraud Network received victim payments in the form of reloadable prepaid cards, prepaid debit cards and gift cards of varying types; United States postal money orders; cashier's cheques; money transfer service wires; and bank wires and deposits. For other examples of cases involving groups that used some of these payment options, see Tribunal correctionnel d'Anvers, Antwerpen, 2 mai 2016 (Belgium); *United States of America v. Andre-Catalin Stoica et al.,* p. 4; *United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase and Rasaq Aderoju Raheem*, Case No. 17-60397; *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus*, p. 8; United States District Court, District of South Carolina, *United States of America v. Jimmy Dunbar, Jr. and Mitchlene Padgett,* Criminal Case No. 2:18-1023, Indictment, 14 November 2018, p. 3; and *United States of America v. Rakeem Spivey and Roselyn Pratt*, Case No.: 2:18-CR-0018, Indictment, 14 November 2018, p. 3.

[85] Digital currency can be described as a digital representation of either virtual currency (non-fiat) or e-money (fiat) (Financial Action Task Force, "Virtual currencies key definitions and potential AML/CFT risks" (June 2014)), p. 4). Virtual currencies refer to a digital representation of value that, like traditional coin and paper currency, functions as a medium of exchange (i.e., it can be digitally traded or transferred and can be used for payment or investment purposes) (United States Department of Justice, Office of the Deputy Attorney General, *Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency–Enforcement Framework* (Washington, D.C., 2020), p. 2). The term "e-money" refers to the digital representation of fiat currency used to electronically transfer value denominated in fiat currency (Financial Action Task Force, "Virtual currencies key definitions", p. 4).

[86] United States Department of Justice, Office of the Deputy Attorney General, *Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency*, p. 3.

[87] Infraud used Liberty Reserve, bitcoin and other digital currencies to conceal the nature of their proceeds and move the proceeds among enterprise members and associates (*United States of America v. Svyatoslav Bondarenko et al.*, p. 21); see also United States District Court, Southern District of New York, *United States of America v. Liberty Reserve S.A. et al.*, Case No. 13-CR-368 (DLC), 23 September 2015 (UNODC, SHERLOC case law database, Case No. USA004R).

United States of America v. Liberty Reserve, Case No. 13-CR-368 (DLC) (S.D. New York, 23 September 2015) (United States of America)

Liberty Reserve, registered in 2006 in Costa Rica, was a centralized digital currency service that allowed users to convert euros or United States dollars into a digital currency called Liberty Reserve that was pegged to the value of the fiat currency. Money could not be deposited directly into Liberty Reserve accounts through wire transfers or credit card payment. Instead, third-party exchangers were used, which enabled Liberty Reserve to avoid collecting any information about its users through banking transactions or other activity.[a] Once money was deposited into the accounts of third-party exchangers, a corresponding amount of Liberty Reserve currency was then credited to the user's Liberty Reserve account. The user could then transfer the Liberty Reserve currency to other users. Liberty Reserve currency could be converted back into fiat currency by transferring to the Liberty Reserve account of a third-party exchanger. Liberty Reserve charged a small fee for each transaction and offered to hide Liberty Reserve account information for a small fee (a "privacy fee") when users were transferring funds to other Liberty Reserve users. In addition, when users registered for a Liberty Reserve account, the only personal information that users had to provide during registration was a name, email address and birthdate. According to the criminal indictment, Liberty Reserve was intentionally created, structured and operated as a criminal business venture, one designed to help criminals conduct illegal transactions and launder the proceeds of their crimes.[b] Before Liberty Reserve was shut down in 2013, the number of users worldwide exceeded one million.

The two founders of Liberty Reserve were charged with and arrested for conspiracy-related offences. In 2013, one of the founders, V.K., a citizen of the United States, pleaded guilty to, among other offences, conspiracy to commit money-laundering and conspiracy to operate an unlicensed money-transmitting business and was sentenced to 10 years of imprisonment.[c] The other founder, A.B., a citizen of Costa Rica, was arrested in Spain in 2013 and extradited to the United States in 2014. In 2016, A.B. pleaded guilty to one count of conspiring to commit money-laundering and was sentenced to 20 years of imprisonment and a fine of US$ 500,000.[d]

For more information on this case, see UNODC, SHERLOC case law database, Case No. USA004R.[e]

[a] *United States of America v. Liberty Reserve S.A. et al.,* Indictment No. 13-CR-368, para. 16.
[b] Ibid., para. 8.
[c] Nate Raymond and Brendan Pierson, "Digital currency firm co-founder gets 10 years in prison in U.S. case", *Reuters*, 13 May 2016.
[d] United States Department of Justice, Office of Public Affairs, "Liberty reserve founder sentenced to 20 years for laundering hundreds of millions of dollars", press release, 6 May 2016.
[e] Available at https://sherloc.unodc.org/.

In addition, cryptocurrencies are used by perpetrators of cyber organized crime to further their illicit ends. The most widely used cryptocurrency is bitcoin. Case law has revealed that darknet sites include "tumbling" or "mixing" services to obscure links between buyers' and vendors' bitcoin addresses.[88] These services essentially scramble multiple buyer-seller bitcoin transactions together in order to conceal the bitcoin payments from buyer to seller or commission payments to the administrator.[89] In *Internet Organised Crime Threat Assessment 2020*, Europol revealed that while the most popular cryptocurrency (bitcoin) is still predominantly used, darknet markets have started to offer alternative privacy-enhanced cryptocurrencies for transactions, such as Monero, Dash and Zcash.[90] Case law supports this observation. In particular,

[88] *United States of America v. Gary Davis*, Case No. 1:13-CR-950-2 (SHERLOC case law database, Case No. USAx156).
[89] United States District Court, Southern District of Florida, *United States of America v. Gal Vallerius*, Case No. 17-MI-03241-JG, Criminal Complaint, 31 August 2017, para. 24 (c).
[90] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 58.

the darknet sites included in this digest relied on bitcoin, Monero and Ethereum for financial transactions.[91] The popularity of cryptocurrencies has led to their use in scams to lure unsuspecting investors in fraudulent schemes.[92] Moreover, cryptocurrencies have been used by criminals for money-laundering.[93] Finally, cryptocurrencies are not only a tool used by organized criminal groups, but also the target of these criminals. For example, the so-called Bayrob group engaged in "cryptojacking", malicious "cryptomining" whereby malicious code was used to infect systems and use the resources of the infected systems to "mine" cryptocurrencies.[94]

Seoul Central District Court (Criminal Department I-I), 2 May 2019, 2018NO2855 (Welcome to Video) (Republic of Korea)

Between 8 July 2015 and 4 March 2018, the defendant, a national of the Republic of Korea, operated "Welcome to Video", a darknet website for the exchange of child sexual abuse material.[a] The defendant posted approximately 20 gigabytes of images and videos to the website that had been downloaded from other websites. Website users were able to download child sexual abuse material using bitcoins or "points" that could be earned by uploading other child sexual abuse material to the website. Each user received a unique bitcoin address when creating an account on the website. An analysis of the server revealed the website had more than one million bitcoin addresses, meaning that the website had a capacity for at least one million users.

Germany, the Republic of Korea, the United Kingdom and the United States engaged in a joint law enforcement investigation that led to the arrest of the defendant and the seizure of the server used to operate the website. Specifically, in the United States, criminal investigation agents of the Internal Revenue Service traced bitcoin exchanges to identify IP addresses linked to the website. The agents then analysed the IP addresses to identify the server hosting the website, which was located in the Republic of Korea. Law enforcement officers from the Republic of Korea, the United Kingdom and the United States subsequently raided the location of the server and arrested the website operator, seizing approximately 8 terabytes of child sexual exploitation videos. The law enforcement agencies involved shared the data from the seized server with law enforcement agencies throughout the world, resulting in the arrest of 337 individuals in 12 different countries. According to the National Center for Missing and Exploited Children of the United States, approximately 45 per cent of the seized videos contained child sexual exploitation material that had not been previously identified. Law enforcement authorities seized money in bitcoins and Power Ledger tokens.

The defendant was sentenced to two years' imprisonment for the production and distribution of child pornography[b] and the spreading of pornography;[c] the sentence was ultimately suspended. The defendant was also sentenced to complete a sex offender treatment programme and to perform 200 hours of community service. The appellate court reversed the lower court's judgement in part, holding that the sentence imposed by the lower court was too light and improper. The appellate court decided to sentence the defendant to one year and six months of imprisonment; that sentence was not suspended. The appellate court also ordered the defendant to complete a sexual violence

[91] *Regina v. Jake Levene*, Crown Court Leeds, Case No. T20177358; *Regina v. Mandy Christopher Lowther*, Crown Court Leeds, Case No. T20177358; *Regina v. Lee Childs*, Crown Court Leeds, Case No. T20177358.

[92] A group of five defendants participated in a worldwide Ponzi scheme, the BitClub Network, which defrauded cryptocurrency investors (United States District Court, District of New Jersey, *United States of America v. Matthew Brent Goettsche, Russ Albert Medlin, Jobadiah Sinclair Weeks, Joseph Frank Abel, and Silviu Catalin Balaci*, Case No. 19-CR-877-CCC, 5 December 2019; United States District Court, District of New Jersey, *United States of America v. Silviu Catalin Balaci*, Superseding Information, Case No. 19-877 (2017)).

[93] United States District Court, Southern District of New York, *United States of America v. Ross William Ulbricht*, Case No. 14-CR-068, 4 February 2014.

[94] *United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus*.

treatment programme; in addition, he was subjected to a five-year restriction order on employment in a child- and/or youth-related organization.

The website, Welcome to Video, was one of the first of its kind to use the cryptocurrency bitcoin to monetize child sexual exploitation videos. Prior to being shut down, it was considered to be the largest darknet site containing child sexual abuse material. The combination of the site using cryptocurrencies for transactions and being hosted on the darknet posed challenges for law enforcement authorities.

For more information about this case, see UNODC, SHERLOC case law database, Case No. KORx002.[d]

[a] For more information on child sexual exploitation material, see chap. V, sect. B.6.
[b] Art. 11, para. 2, of the Act on the Protection of Children and Youth against Sex Offenses of the Republic of Korea.
[c] Article 44-7, paragraph (1) 1, and article 74, paragraph (1) 2, of the Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc.
[d] Available at https://sherloc.unodc.org/.

CHAPTER V.

TYPES OF CYBER ORGANIZED CRIME

V. TYPES OF CYBER ORGANIZED CRIME

There are two types of cyber organized crime: cyber-dependent organized crime and cyber-enabled organized crime. Types of cybercrimes that fall under the categories of cyber-dependent and cyber-enabled crimes are examined in the sections below.

A. Cyber-dependent crime

Cyber-dependent crimes target ICT and would not be possible without the use of that technology. Cyber-dependent crimes target the confidentiality (access is restricted to authorized users), integrity (data are correct, trustworthy and valid) and availability (systems and data are accessible on demand) of computer systems and data. Illicit acts against the confidentiality, integrity and availability of computer systems and data include illegal access to a computer system and/or computer data; illegal interception of computer data and/or acquisition of computer data; illegal data and system interference; and illegal production, distribution, use and possession of computer misuse tools. These cybercrimes are committed for a variety of reasons, including financial, ideological, political and personal reasons (such as revenge, personal gratification, to gain status and to obtain recognition among peers).[95]

1. Illegal access

Unauthorized or illegal access to ICT and/or its data is commonly known as hacking. Hacking refers to not only gaining unauthorized or illegal access but also exceeding authorized access. Both of these activities are proscribed by law, but this proscription varies by country and region.[96] Hackers may access or attempt to access systems and data; exceed or attempt to exceed authorized access to systems and data; and/or may utilize this access to steal, modify, disrupt and/or otherwise damage systems and data. With respect to the latter, once hackers gain illegal or unauthorized access to systems, they can view, download, alter and/or steal data, damage the systems and/or interrupt or disable access to the system and/or data by legitimate users.[97]

R. v. Kalonji, 2019 ONCJ 341 (Canada)

The case *R. v. Kalonji* involved six defendants (H.K, T.S.-M., A.G., K.R., B.M. and K.H.), three of whom (H.K., K.H. and A.G.) were charged with and convicted of conspiracy to commit fraud, in particular account takeover fraud (two of the defendants were also charged and convicted of other crimes).[a] To accomplish this fraud, new accounts (so-called "complicit accounts") or joint accounts were opened that were in some way linked to victims' accounts (often identified by hackers that gained illegal access to bank systems or by insiders of the bank).[b] Money was then transferred from the victims' accounts to the joint or complicit accounts and subsequently withdrawn from the accounts by associates. Intercepted communications of one of the defendants (H.K.) revealed that he had used hackers to identify victims' accounts and to manipulate bank accounts for fraudulent reasons (e.g., to transfer money from victims' accounts to complicit accounts).[c]

For more information on this case, see UNODC, SHERLOC case law database, Case No. CANx137.[d]

[a] Canada, Ontario Court of Justice, *R. v. Kalonji,* paras. 110–114.
[b] Ibid., para. 6.
[c] Ibid., paras. 46, 66 and 75.
[d] Available at https://sherloc.unodc.org/.

[95] Majid Yar, *Cybercrime and Society* (Thousand Oaks, California, SAGE Publications, 2006); Samuel C. McQuade III, *Understanding and Managing Cybercrime* (Upper Saddle River, New Jersey, Pearson Education, 2006); David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge, United Kingdom, Polity, 2007); Maras, *Cybercriminology*.

[96] Article 29, paragraph 1 (a), of the African Union Convention on Cyber Security and Personal Data Protection requires States parties to that Convention to criminalize gaining or attempting to gain unauthorized access to part or all of a computer system or exceed authorized access.

[97] Maras, *Cybercriminology*, p. 14.

Tribunal de grande instance hors classe de Dakar, 14 janvier 2020, 30/2020

The computer systems and data systems of a network of savings and credit cooperatives in Senegal, were accessed by unknown individuals for the creation of large and fictitious amounts of money or to steal money from existing accounts of the banking network and transfer it to their accomplices' accounts for withdrawal.

Cheikh Al X, Jeanne AJ Ap and Alioune Ak Z were accused of aiding and abetting fraudulent computer system access by providing the principal offenders – the unknown individuals – with bank accounts to facilitate the deposits of fictitious money.

Following the unknown individuals' orders, Cheikh Al X targeted and facilitated the use of several bank accounts for the receipt of the stolen funds. He also asked Jeanne AJ Ap to facilitate the use of an account of the banking network. Jeanne asked her cousin Ao AG to use her own account to help a friend who needed to receive money from her husband. The money from each account was sent to the unknown individuals and a part of it was shared with the defendants, as well as the bank account owners (such as Ao AG).

The defendants were convicted of fraud and aiding and abetting the access and maintenance of computer systems and the modification or deletion of data; fraudulent interception of computer systems for the purpose of obtaining financial benefits; and modification of data by the introduction, erasure or deletion of data. They were sentenced to two years of imprisonment and to pay to the banking network 3.5 million CFA francs in compensation.

For more information on this case, see UNODC, SHERLOC case law database, Tribunal de grande instance hors classe de Dakar, 14 janvier 2020, 30/2020.[a]

[a] Available at https://sherloc.unodc.org/.

The term "hacking", however, is not included in multilateral, regional and national cybercrime laws. Instead the terms "illegal access" or "unauthorized access" are used. For example, article 2 of the Council of Europe Convention on Cybercrime [98] includes the term "illegal access", which is defined as the intentional "access to the whole or any part of a computer system without right". In the Agreement on Cooperation among the States members of the Commonwealth of Independent States in Combating Offences related to Computer Information, "illegal access" is defined as unauthorized access to computer information.[99] The term "illegal access" is also included in the Arab Convention on Combating Information Technology Offences, adopted by the League of Arab States in 2010; in that Convention, illicit access to, presence in or contact with part or all of the information technology is considered to be a criminal offence. Some laws consider illegal

[98] In this digest, as a way to illustrate the meaning of concepts and variation in the definitions of concepts, the definitions included in multilateral conventions (such as the Council of Europe Convention on Cybercrime) and regional instruments (such as the Agreement on Cooperation among the States members of the Commonwealth of Independent States in Combating Offences related to Computer Information), the African Union Convention on Cyber Security and Personal Data Protection and the Arab Convention on Combating Information Technology Offences), as well as national laws, are used.

[99] Article 1, paragraph (d), of the Agreement on Cooperation among the States members of the Commonwealth of Independent States in Combating Offences related to Computer Information.

access alone to be an offence,[100] whereas other laws require access to be accompanied by a proscribed act in order to be considered an offence.[101]

2. Illegal interception or acquisition

Multilateral, regional and national cybercrime laws proscribe the illegal interception or acquisition of computer data. There is no universal definition of illegal interception or acquisition of computer data and the definitions included in laws vary. In the Arab Convention, the offence of illicit interception is defined as the deliberate unlawful interception of the movement of data by any technical means and the disruption of transmission or reception of information technology data (art. 7). In article 3 of the Council of Europe Convention, "illegal interception" is defined as the intentional "interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data". Instead of using the words "without right", the African Union Convention on Cyber Security and Personal Data Protection, adopted in 2014, holds that interception is illegal if it occurs "fraudulently".[102] Perpetrators of this type of cybercrime seek to intercept data as they traverse networks through, for example, eavesdropping on communications or masquerading as the sender or receiver of communications and/or data.[103]

3. Data and system interference

Interference is broadly understood as including any activity that alters, deletes, inhibits the functioning and/or damages systems and/or data.[104] In article 29, subparagraphs 1 d),[105] 1 e),[106] 1 f),[107] 2 b)[108] and 2 d),[109] of the African Union Convention, data and system interference are considered criminal offences. According to

[100] See, for example, the Arab Convention on Combating Information Technology Offences, which calls for States to criminalize illicit access to, presence in or contact with part or all of the information technology, or the perpetuation thereof (see art. 6, para. (1)); and calls for the provision of enhanced penalties for illicit access leading to the obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries or the acquirement of secret government information (see art. 6, para. (2)). In of the African Union Convention on Cyber Security and Personal Data Protection, States parties to the Convention are required to criminalize: gaining or attempting to gain unauthorized access to part or all of a computer system or exceed authorized access (art. 29, para. 1 a)); and remaining or attempting to remain fraudulently in part or all of a computer system (art. 29, para. 1 c)).

[101] Article 3 (1) (a) of the Agreement on Cooperation among the States members of the Commonwealth of Independent States in Combating Offences related to Computer Information calls for the criminalization of: the illegal accessing of computer information protected by the law, where such act results in the destruction, blocking, modification or copying of information or in the disruption of the functioning of the computer, the computer system or related networks (art. 3, para. (1) (a)); and Agreement the violation of regulations governing the use of computers, computer systems or related networks by a person who has access to those computers, systems or networks, resulting in the destruction, blocking or modification of computer information protected by the law, where such act causes significant harm or serious consequences (art. 3, para. (1) (c)). The African Union Convention on Cyber Security and Personal Data Protection considers the following to be a criminal offence: gaining or attempting to gain unauthorized access to part or all of a computer system or exceed authorized access with intent to commit another offence or facilitate the commission of such an offence (art. 29, para. 1 b)).

[102] The African Union Convention requires States parties to criminalize intercepting or attempting to intercept computerized data fraudulently by technical means during non-public transmission to, from or within a computer system (art. 29, para. 2 a)).

[103] See also UNODC, Education for Justice Module Series, Cybercrime, Module 2: general types of cybercrime, "Computer-related offences". Available at **www.unodc.org/e4j/**.

[104] Ibid.

[105] States parties are required to criminalize hindering, distorting or attempting to hinder or distort the functioning of a computer system (art. 29, para. 1 d)).

[106] States parties are required to criminalize entering or attempting to enter data fraudulently in a computer system (art. 29, para. 1 e)).

[107] States parties are required to criminalize damaging or attempting to damage, delete or attempting to delete, deteriorate or attempting to deteriorate, alter or attempting to change the computer data fraudulently (art. 29, para. 1 f)).

[108] States parties are required to criminalize intentionally inputting, altering, deleting or suppressing computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data are directly readable and intelligible (art. 29, para. 2 b)).

[109] States parties are required to criminalize the fraudulently procuring, for oneself or for another person, any benefit by inputting, altering, deleting or suppressing computerized data or any other form of interference with the functioning of a computer system (art. 29, para. 2 d)).

article 4 of the Council of Europe Convention, data interference is considered a crime when it is "committed intentionally" and involves the "damaging, deletion, deterioration, alteration or suppression of computer data without right". Article 8 of the Arab Convention calls for the proscription of deliberate unlawful destruction, obliteration, obstruction, modification or concealment of information technology data (so-called "offences against the integrity of data").

BGH, Beschluss vom 30.08.2016, 4 StR 194/16 (Germany)

At the time of the crimes, the defendant A.T. had been working for a company producing and operating slot machines for several years. He advised its employees regarding the manipulation protection of the slot machines. He employed his son-in-law, P., as a computer specialist. The brother of the defendant, S.T., had been operating his own gambling halls.

In 2013, A.T. and Dr. C. (the managing director and a shareholder of the firm Ca. GmbH, which had put up slot machines of the firm L. GmbH in their casinos in Germany) decided to manipulate the software of the slot machines for financial gain. P., who knew of the plans, developed cards and dongles (a device similar to USB stick) with which the software of the machines was manipulated to credit the player points (tradable for cash) without previously having initiated a game. This was referred to as the "credit approach". P. also installed a backdoor in the software that was activated by daily codes and manipulated the game in such a way that, instead of the player choosing between red and black without having any indication of the result, the same colour appeared multiple times in a row. This allowed the player to eliminate the usual risk of loss and receive points that could subsequently be traded for money.

The original flash cards used by the slot machines were replaced by cards with the manipulated software developed by P. This swap happened at night, outside of the casinos' business hours. At first, the backdoor was installed on the flash cards with the original software. Later, the backdoor, as well as the manipulated software to perform the credit approach, were installed on a dongle that was inserted into the slot machines.

The credit approach was used 200 times between July 2014 and January 2015 to obtain €4,485,965 in winnings from the slot machines. Between March 2014 and January 2015, the backdoor was used by 43 people instructed by A.T., resulting in proceeds of €214,030. The people later instructed by S.T. obtained a total of €1,218,420 from making use of the backdoor 1,770 times. In one instance, S.T. himself played and retrieved €1,500 by using the backdoor.

The defendant was charged with and convicted of commercially based computer fraud under section 263a of the German Criminal Code, which provides that whoever, with the intention of obtaining an unlawful pecuniary benefit for themselves or a third party, damages the property of another by influencing the result of a data processing operation by incorrectly configuring the computer program, using incorrect or incomplete data, making unauthorized use of data or taking other unauthorized influence on the processing operation incurs a penalty of imprisonment for a term not exceeding five years or a fine. He was also charged with the disclosure of trade secrets. The defendant was sentenced to five years and six months of imprisonment.

For more information on this case, see UNODC, SHERLOC case law database, Case No. DEUx027.[a]

[a] Available at https://sherloc.unodc.org/.

Data compromises (or data breaches), which occur when criminals illegally access data or databases,[110] are an example of data interference. This illicit access may be obtained in variety of ways, such as by using malware (see chap. V, sect. A.4, below) and other tools to exploit system vulnerabilities, as well as social engineering tactics designed to dupe unsuspecting individuals into engaging in acts that the criminals want the targets to engage in (e.g., revealing personal information or clicking on a link infected with malware). Social engineering tactics are used to perpetrate not only cyber-dependent crimes, but also cyber-enabled crimes (for examples of these tactics, see chap. V, sect. B.1, subsect. (a), below).

Legal definitions of system interference, like those of data interference, vary. The African Union Convention simply defines it as hindering, distorting or attempting to hinder or distort the functioning of a computer system.[111] The definition provided in the Council of Europe Convention explains what specific actions constitute interference: inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.[112]

Segundo Juzgado de Instrucción del Distrito Nacional – Proceso No. 058-13-00719 (Dominican Republic)

The Integral Management Protection Center reported the suspicious use of Dominican prepaid telephone lines to make international calls. Technology fraud engineers from the affected company initiated an investigation, which showed that the prepaid telephone numbers fraudulently used to make international calls from the Dominican Republic had been irregularly switched to postpaid. By performing a search on the intranet (the local network of the telephone company), an information security expert from the affected company identified the IP addresses from where the alterations to the prepaid numbers had been made. With this information, the expert requested assistance in the form of forensic analysis from the department of the national police responsible for the investigation of crimes and high-technology crimes. The forensic analyst discovered that the alterations had been made from the older version of the provisioning platform for automated activation of customer services. The telephone company had recently started using an upgraded version of the platform.

Five individuals were accused of violating articles 265 and 266 of the Penal Code and articles 7, 8, 20 and 26 of law 53-09 on high-tech offences against the national telephone company. Three of the defendants, SAGR, IDHP and WSH, were convicted of electronic fraud and sentenced to three years of prison. Their sentences were suspended on the condition of keeping a permanent residence, refraining from carrying any type of weapons and refraining from drinking alcoholic beverages.

For more information about this case, see UNODC, SHERLOC case law database, Case No. DOMx010.[a]

[a] Available at https://sherloc.unodc.org/.

[110] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 14.

[111] Art. 29, para. 1 d).

[112] According to article 5 of the Convention on Cybercrime, system interference is considered illegal when it is committed intentionally and seriously hinders without right the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Examples of cybercrimes that interfere with systems are denial-of-service attacks and distributed denial-of-service attacks. A denial-of-service attack overwhelms the target's resources, resulting in the denial of requests for access from legitimate users.[113] This type of cybercrime targets the availability of the systems and data. A distributed denial-of-service attack, like a denial-of-service attack, seeks to overwhelm the target's resources to prevent legitimate access to the target; however, instead of just one computer or other technology, multiple computers and other technologies are used to overwhelm the target's resources. Distributed denial-of-service attacks can be committed when multiple users utilize their devices to commit coordinated cyberattacks and/or when multiple computers and other technologies infected with malware are leveraged to conduct a cyberattack.[114] The network of digital devices infected with malware that can be used in a distributed denial-of-service attack constitute what is known as a botnet. The malware used to create a botnet enables the monitoring and remote control of the infected digital devices. Data may also be stolen from these infected devices.

Cassazione penale, sezione feriale, sentenza No. 50620, 12 Settembre 2013 (Italy)

Between 2011 and 2012, a hacktivist group operating under the name Anonymous Italia conducted several cyberattacks against the websites of public institutions and well-known companies. This group identified itself as the Italian branch of the Anonymous collective; its aim, according to the view of the prosecutor, was to become a leading group in the Italian hacktivist community and carry out cyberattacks, which it called "operations".

The members of the group mainly communicated using private and public Internet Relay Chat channels. Participation in private channels was limited to the organizers of the cyberattacks. In these channels, the organizers chose the targets, organized and coordinated the operations and prepared public messages claiming responsibility for the attacks. The public channels did not have access restrictions and were used as platforms for discussing topics related to the ideology of Anonymous and for looking for participants for the distributed denial-of-service attacks launched by the organizers of the private channels. Members of the private channels were charged with participation in a criminal association under article 416 of the Italian Criminal Code ("Associazione per delinquere").

The cyberattacks perpetrated by the group consisted of distributed denial-of-service attacks and illegal access to computer systems and data, which sometimes led to the defacement of victims' websites. The modus operandi of these attacks followed a recurrent pattern. First, the members of the criminal group decided on the target of the so-called operation. The targets were chosen on the basis of maximizing prospective media exposure and dissemination of the group's messages. Secondly, when the members of the criminal group conducted distributed denial-of-service attacks, they recruited participants in public Internet Relay Chat channels and made use of botnets. When they sought illegal access to computer systems and data, they scanned the targeted website in order to find flaws in its security system that they could exploit. Thirdly, the members of the group usually gathered in private Internet Relay Chat channels in order to coordinate the cyberattacks and support each other during the operations. Lastly, once an operation had been completed, the group published a message in which they claimed responsibility for the cyberattacks on the blog and the social network accounts related to Anonymous Italia.

[113] Marie-Helen Maras, *Computer Forensics: Cybercriminals, Laws and Evidence*, 2nd ed. (Burlington, Massachusetts, Jones and Bartlett, 2014), p. 7.

[114] Ibid., p. 8.

Cassazione penale, sezione feriale, sentenza No. 50620, 12 Settembre 2013 (Italy) (*continued*)

The defendant appealed the decision of the Tribunal of Rome. The appeal was based on four grounds, one of which was an error in the application of the criminal association offence (art. 416). The Court of Cassazione rejected the appeal. Regarding the criminal association offence, the judges found that the law had been applied correctly. Regarding the mens rea and the stable association bond elements of the criminal association offence, the messages published on the blog and social media profiles of Anonymous Italia in which members of the group claimed responsibility for the cyberattacks showed the existence of a shared goal, the commission of crimes, and shared identity among the members. Moreover, the continuous cooperation of the members of the criminal association in the commission of the cyberattacks between 2011 and 2012 showed the existence of a stable association bond between them. The organization element of the criminal association offence, which requires the existence of a minimum degree of organization between the criminals, was fulfilled by the division of labour among the members. Regarding the organization element, the Court took into consideration the structure of Anonymous, a fluid and flexible network of individuals who share beliefs, without formal leadership. Despite the absence of formal leadership, some individuals in the network take the initiative organizing online operations and become informal leaders. The Court stressed that the entire Anonymous community did not constitute a criminal association; only the small groups of individuals, who planned and executed cyberattacks and, in that way, assumed a leading role in the hacktivist community, could be considered a criminal association under article 416.

Moreover, the basic structure of private Internet Relay Chat channels defined the extension of the criminal association: only those who had access to the private Internet Relay Chat channels could be part of the criminal association. In this sense, the communication tool corresponded to the structure of the criminal association. These remarks about the structure of Anonymous highlight an important feature of the application of the criminal association to online criminal groups. Prosecutors only charged the members of the private Internet Relay Chat channels in which cyberattacks were prepared and coordinated with the criminal association offence contrary to article 416. They did not charge the users who visited the public Internet Relay Chat channels. The characteristic of the private channels is that their access is limited to certain members, a feature that is also common with online communities of paedophiles. Such communities often adopt control mechanisms to select new members. As noted by the Court, Italian case law had applied the offence of criminal association to online communities of paedophiles in the past. The decision of the Court suggests that the application of the criminal association offence to online criminal groups is limited to the ones that constitute a closed online community. This requirement may be seen as the result of the fluidity of the online groups and the interactions that take place on the Internet and the risk of overcriminalization of cyberspace through a broad application of the requirements of the criminal association offence. In an online environment where lines and borders of participation are blurred, it is sometimes difficult to identify who is actually part of an organized criminal group.

This decision represents one of the Italian landmark cases on the application of the criminal association (art. 416 of the Italian Criminal Code) to organized criminal groups operating online. After examining judicial decisions applying article 416 to online communities of paedophiles, the Court set out the requirements for the application of the criminal association to online criminal groups. The elements of the criminal association are: *(a)* the existence of an association bond between at least three persons that shall not be short term or casual; *(b)* the existence of a criminal plan that constitutes the aim of the organization; and *(c)* the existence of an organizational structure, with a minimum degree of sophistication, that allows the criminal plan to be carried out.

Perpetrators of distributed denial-of-service attacks use existing tools to conduct such attacks, combine existing tools, customize existing tools and create new tools. The creation of new tools and use of existing tools were identified in the Europol report *Internet Organised Crime Threat Assessment 2020* as methods

used by criminals to adapt to security measures.[115] The tools used to conduct distributed denial-of-service attacks and even botnets are available for sale or rent online and offered as a part of "crime as a service".[116] These tools can be custom-ordered or existing tools modified to users' preferences. Access to these botnets, as well as other systems and data of targets, are also offered online by criminal groups as a service for a fee (sometimes called "access as a service").[117]

The 2020 Europol report also revealed that Internet of Things[118] devices are vulnerable to distributed denial-of-service attacks.[119] The Mirai botnet brought home the lesson that everyday objects connected to the Internet can be successfully targeted by perpetrators. Specifically, the Mirai botnet, which at some point was composed of hundreds of thousands of infected Internet of Things devices primarily based in the United States, was used to conduct distributed denial-of-service attacks on various targets and provide revenue to those who controlled the botnet.[120] The revenue they obtained was retrieved from renting the botnet to customers for a fee and extorting from hosting companies and others protection money to avoid being targeted by denial-of-service attacks.[121]

4. Misuse of devices

The misuse of devices is considered illegal "when committed intentionally and without right".[122] This cybercrime involves the possession, "production, sale, procurement for use, import, distribution or otherwise making available of" a device, including a computer program, designed or adapted primarily for the purpose of committing illegal access, illegal interception, data interference and/or system interference.[123] An example of such a device is malware. Malware is often distributed through attachments and infected links in emails and websites.[124] However, criminals have also exploited software vulnerabilities to spread malware and infect systems. While the majority of laws criminalize the misuse of such devices, other laws explicitly prohibit the creation, use or distribution of malware.[125]

Criminals have additionally encrypted malware and taken other measures to evade detection by security measures and law enforcement authorities. For instance, the malware created by the Bayrob criminal enterprise would block targets' access to sites associated with law enforcement.[126] Criminals have further offered malware that is made-to-order, or customized according to the buyer's preferences. SpyEye is an example

---

[115] Europol, *Internet Organised Crime Threat Assessment* 2020, p. 32.

[116] Ibid.; Ken Dunham, and Jim Melnick, *Malicious Bots: An Inside Look into the Cyber-criminal Underground of the Internet* (Boca Raton, Florida, CRC Press, 2009), pp. 3 and 57.

[117] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 31.

[118] The Internet of Things is an umbrella term used to describe a network of Internet-connected devices that collect, store, collate, analyse and share a significant amount of information and monitor people, animals, plants and/or objects in order to provide users of these devices with some form of service (Marie-Helen Maras, "Internet of Things", in *Encyclopedia of Security and Emergency Management*, Lauren R. Shapiro and Marie-Helen Maras, eds. (Cham, Switzerland, Springer International Publishing, 2020)).

[119] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 33; for information about security concerns related to Internet of Things devices, see Marie-Helen Maras, "Internet of Things: security and privacy implications", *International Data Privacy Law*, vol. 5, No. 2 (May 2015), pp. 99–104.

[120] United States Department of Justice, Office of Public Affairs, "Justice Department announces charges and guilty pleas in three computer crime cases involving significant DDoS attacks", press release, 13 December 2017.

[121] United States District Court, District of Alaska, *United States of America v. Paras Jha*, Case No. 3:17-CR-00164, Plea Agreement, 5 December 2017, p. 4.

[122] Article 6, paragraph 1 a, of the Council of Europe Convention on Cybercrime.

[123] Ibid. A somewhat similar definition is provided in article 29, paragraph 1 h), of the African Union Convention, in which States parties are required to criminalize unlawfully producing, selling, importing, possessing, disseminating, offering, ceding or making available computer equipment, programs or any device or data designed or specially adapted to commit offences.

[124] Lorine A. Hughes and Gregory J. DeLone, "Viruses, worms, and trojan horses: serious crimes, nuisance, or both?", *Social Science Computer Review*, vol. 25, No. 1 (February 2007), p. 84.

[125] See, for example, article 3, paragraph 1 (b), of the Agreement on Cooperation among the States members of the Commonwealth of Independent States in Combating Offences related to Computer Information. According to the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, of Nigeria, sect. 32, subsect. (3): any person who engages in malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in a public, private or financial institution's computers shall be guilty of an offence and is liable upon conviction to three years' imprisonment or a fine of 1 million naira or both.

[126] *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus*, p. 6. The Federal Bureau of Investigation (FBI) of the United States mentioned that one of these sites was the Internet Crime Complaint Center (**www.ic3.gov/**) (for further information, see United States, Federal Bureau of Investigation, "Romanian hackers sentenced: members of Bayrob criminal enterprise infected thousands of computers with malware, stole millions of dollars", 20 February 2020).

of a customizable malware toolkit that enabled the theft of personal and financial data. Buyers of this toolkit could, for example, customize SpyEye to target and collect specific information from infected systems or specific financial institutions and choose what methods would be used to collect this information (e.g., keylogger).[127]

The misuse of devices may also involve the possession or use of "a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing" illegal access, illegal interference, data interference and/or system interference.[128] An example of this type of misuse of devices involved the deployment, by a cyber organized criminal group, of malware known as GozNym, a Trojan Horse created by combining two others (Gozi and Nymaim) and designed to infect targeted computers and capture financial data (particularly banking login credentials). The financial data were later used by members to commit bank fraud by gaining unauthorized access to the targets' accounts and stealing funds from those accounts.[129]

United States of America v. Vladimir Tsastsin Andrey Taame, Timur Gerassimenko, Dmitri Jegorov, Valeri Aleksejev, Konstantin Poltev, and Anton Ivanov, Case No. 1:11-CR-00878 (S. D. New York, 14 October 2011) (DNS Changer Malware) (United States of America)

The group responsible for the DNS Changer malware, worked with other conspirators to engage in a fraudulent advertisement scheme.[a] In this case, members of the group posed as a legitimate Internet advertisement agency and entered into Internet advertising agreements where they were paid to receive money each time a user clicked on a website link or advertisement. The suspects used rogue Domain Name System (DNS) servers and malware to fraudulently increase traffic and, in turn, increase their revenue. The malware would infect users' systems, alter users' DNS server settings to route activity to the rogue DNS servers, prevent anti-virus software from receiving updates and facilitate click hijacking (whereby clicking on a search result redirects the user to the perpetrators' desired site, which the perpetrators receive payment for) and click fraud (fraudulently replacing advertisements on sites with desired advertisements that perpetrators receive payment for).[b]

Most of the suspects were charged with and sentenced for their crimes. V.T. pleaded guilty to conspiracy to commit wire fraud and conspiracy to commit computer intrusion and was sentenced to seven years and three months of imprisonment, with one year of supervision after release, and was required to forfeit US$ 2.5 million.[c] Other conspirators also pleaded guilty and were sentenced for their crimes (T.M. and V.A. were each sentenced to four years' imprisonment; D.J. was sentenced to three years and eight months of imprisonment; K.P. was sentenced to three years and four months of imprisonment; and A.I. was sentenced to time served). One defendant, A.T., is currently still at large.

[a] United States District Court, Southern District of New York, *United States of America v. Vladimir Tsastsin, Andrey Taame, Timur Gerassimenko, Dmitri Jegorov, Valeri Aleksejev, Konstantin Poltev, and Anton Ivanov*, Case No. S2-11-CR-878, Indictment, 1 November 2011.

[b] United States Attorney's Office, Southern District of New York, "Estonian cybercriminal sentenced for infecting 4 million computers in 100 countries with malware in multimillion-dollar fraud scheme", 26 April 2016.

[c] Ibid.

[127] United States, Northern District of Georgia, *United States of America v. Aleksandr Andreevich Panin and Hamza Bendelladj*, Case No. 1:11-CR-0557-AT-AJB, First Superseding Indictment, 26 June 2013; United States Department of Justice, Attorney's Office, Northern District of Georgia, "Two major international hackers who developed the 'SpyEye' malware get over 24 years combined in federal prison", 20 April 2016.

[128] Article 6 of the Council of Europe Convention on Cybercrime. A similar definition is provided in the African Union Convention (art. 29, para. 1 h)): States parties to the Convention are required to criminalize unlawfully generating or producing a password, an access code or similar computerized data allowing access to part or all of a computer system.

[129] *United States of America v. Alexander Konovolov et al.* (GozNym malware); United States Attorney's Office, Western District of Pennsylvania, "Three members of GozNym cybercrime network sentenced in parallel multi-national prosecutions in Pittsburgh and Tbilisi, Georgia", 20 December 2019.

B. Cyber-enabled crime

Cyber-enabled crimes include traditional crimes where ICT plays a key role in the methods used to commit the crimes and facilitates the crimes. The types of cyber-enabled crime explored in the subsections below include: computer-related fraud or forgery (bank fraud; phishing; advanced fee fraud scam; romance scam; and other fraud-related scams); computer-related identity offences; falsified medical product-related crime; counterfeiting; blackmail; extortion and ransom (e.g., sexual extortion (sextortion), ransom scams and ransomware); child sexual abuse and exploitation offences (e.g., child sexual abuse and exploitation material; child grooming; and live-streaming child sexual abuse); trafficking in persons; smuggling of migrants; drug trafficking; trafficking in firearms; trafficking in wildlife; trafficking in cultural property; money-laundering; and Internet gambling.

1. Computer-related fraud

There are two general categories of cybercrime that are explored in this section: computer-related forgery and computer-related fraud. The first category, computer-related forgery, can be described as an act, committed intentionally and without right, involving the input, alteration, deletion or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data are directly readable and intelligible.[130] This category of cybercrime includes the impersonation of legitimate individuals and/or entities for fraudulent purposes. Here, fraud can be regarded as the misrepresentation of a fact in order to persuade an individual, group, organization or other entity to provide the offender with something desired or valued.

The second category of cybercrime, computer-related fraud, refers to an act, committed intentionally and without right, causing loss of property to another person by any input, alteration, deletion or suppression of computer data, and/or any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.[131] This category of cybercrime involves the use of false or misleading information to obtain something from the target that is considered desired and/or of value to the perpetrator.

There are many cybercrimes that can be considered computer-related forgery or fraud. Some of these cybercrimes, particularly bank and payment fraud, phishing, advanced fee fraud scams, romance scams and other fraud-related scams, are explored in the subsections below.

(a) Bank and payment fraud

Bank fraud is an umbrella term that covers ways in which money, property or assets owned by financial institutions are illicitly obtained. Payment fraud is a type of bank fraud. Payment fraud involves the unauthorized use of an individual's payment data for the financial gain of the perpetrator. Examples of payment fraud include debit card and credit card fraud (i.e., the theft or unauthorized use of credit or debit card data). With payment fraud, financial institutions are not the only victims; merchants and clients are also victims.

Skimming occurs when a device is installed at a card terminal to surreptitiously collect users' credit, debit or bank card data. A skimmer is a type of device that is designed to surreptitiously collect such information. One type of skimmer is an ATM skimmer. This device, a card reader, is attached to the part of the machine where individuals place their cards. When a user places their card in the machine, the information on the magnetic strip is collected and stored. Personal identification numbers (PINs) are also collected by placing cameras directed at the keypad. In one case in Germany, three individuals were accused of skimming

[130] Article 7 of the Council of Europe Convention on Cybercrime; see also article 10 of the Arab Convention on Combating Information Technology Offences, in which forgery is considered a cybercrime when ICT is used as a means to alter the truth of data in a manner that causes harm, with the intent of using the altered data as true data.

[131] Article 8 of the Council of Europe Convention on Cybercrime. See also article 11 of the Arab Convention on Combating Information Technology Offences, which refers to intentionally and unlawfully causing harm to beneficiaries and users with the aim of committing fraud to illicitly realize interests and benefits to the perpetrator or a third party, through: (a) entering, modifying, obliterating or concealing information and data; (b) interfering with the functioning of the operating systems and communication systems or attempting to disrupt or change them; and (c) disrupting electronic instruments, programmes and sites.

magnetic strip data, as well as obtaining the PINs of several cards, using card readers and miniature cameras.[132] After surreptitiously collecting the data, they created duplicates of the cards (i.e., they cloned the cards) and used them abroad to make payments to other accounts. They were convicted of participating in falsifying guaranteed payment cards[133] and computer fraud.[134] In another case,[135] the German court considered whether ATM skimming could be considered a form of data espionage, defined in the German Criminal Code, section 202a (1), as obtaining, for themselves or another, unauthorized access by circumventing the access protection of data that were not intended for them and were specially protected against unauthorized access. The court found that the reading of the information of the payment card saved on the magnetic strip did not fulfil this requirement, since the data on the magnetic strip were not encrypted or otherwise protected. The fact that some data were saved and transferred magnetically, electronically or otherwise not immediately perceptibly was not to be regarded as "access protection". The court came to the same conclusion regarding the acquisition of PINs, stating that only the unauthorized use of the data when using the card was protected, not the illicit access to the card via a reading device. Accordingly, the court held that neither the acquisition of PINs nor the reading of data stored on the magnetic strip of cards to produce cloned cards was a form of data espionage.

Public Prosecutor v. Law Aik Meng [2006] SGDC 243 (Singapore)

This case involved L.A.M., a national of Malaysia, who operated as a member of an organized syndicate in West Malaysia. The syndicate's objective was to skim data from genuine ATM cards in order to manufacture cloned copies and use them to make fraudulent withdrawals. To accomplish this, the syndicate installed skimming devices in ATMs, which would capture card information while a pinhole camera concealed above the ATM monitor would record the victim keying in his or her PIN. Data would then be transmitted wirelessly to a device used for encoding, storing and playing digital video files that was concealed nearby. The cards created in this manner would subsequently be used to withdraw cash throughout the ATM network of Singapore.

L.A.M.'s role in the syndicate was to install the skimming devices in ATMs in Singapore. Once data were captured, he was responsible for removing the skimming devices and transmitting the captured data to West Malaysia. L.A.M. was also responsible for using cloned cards to make fraudulent withdrawals. With L.A.M.'s help, the syndicate successfully withdrew 18,590 Singapore dollars from the post office savings bank. This activity took place over a period of three months in 2006. Some 849 post office savings bank accounts were compromised and a multinational development bank had to block and replace each account. The assistant vice-president of compliance services of the development bank called the police on 24 May 2006 to inform them of skimming devices that had been located. A police investigation ensued, and L.A.M. was subsequently arrested in connection with the case and taken to the commercial affairs department for further investigation. For his crimes, L.A.M. received a sentence of 12 years' imprisonment. No other conspirators were apprehended.

L.A.M.'s case was the first case of its kind in Singapore involving a criminal enterprise perpetrating ATM fraud.

For more information about this case, see UNODC, SHERLOC case law database, Case No. SGPx013.[a]

[a] Available at **https://sherloc.unodc.org/**.

[132] UNODC, SHERLOC case law database, Germany, Case No. DEUx029, BGH, Beschluss vom 31.05.2012, 2 StR 74/12. Available at **https://sherloc.unodc.org/**.

[133] The German Criminal Code (Strafgesetzbuch), which covers counterfeiting of guaranteed payment cards and blank Eurocheques, defines "guaranteed payment cards" as credit cards, Eurocheque cards and other cards which oblige the issuer to make a guaranteed payment by money transfer and which are specially protected against imitation by dint of their design or coding (sect. 152b (4)).

[134] Sect. 263a of the German Criminal Code (Computer fraud).

[135] UNODC, SHERLOC case law database, Germany, Case No. DEUx026, BGH, Beschluss vom 06.07.2010, 4 StR 555/09. Available at **https://sherloc.unodc.org/**.

Card-not-present fraud involves the illicit possession, procurement, use and/or distribution of debit and credit card data. Examples of card-not-present fraud include e-skimming, whereby malware is injected on a site that captures payment data, and carding, which involves the use of stolen credit card or debit card data to obtain goods and/or services. In *R v. Nicholas Webber*,[136] a young male (between 17 and 18 years old) pleaded guilty to conspiracy to defraud for creating a website (**www.ghostmarket.net**) dedicated to carding, where debit and credit data were made available for purchase. In another case, known as *Unlimited Operations*, a transnational organized criminal group conducted an international fraud operation by hacking into global financial institutions networks to illegally obtain data on debit cards.[137] The group then cloned the cards, removed the withdrawal limits, and then distributed the cards to cashers to go to ATMs at a coordinated date and time to withdraw money. The withdrawals occurred in over 20 countries. The banks targeted in this scheme were in Oman and the United Arab Emirates.[138]

(b) Phishing

Criminals impersonate legitimate organizations in email messages in order to trick targets of the crime into trusting the content of the communications and following instructions that are designed to induce a target: to unknowingly reveal personal and/or financial information; and/or to access malicious links and/or download malware onto the target's systems to enable the criminals to gain unauthorized access to the target's system, network and/or data. When this tactic targets a variety of users (and not a specific target), this crime is commonly known as phishing.[139]

While the term "phishing" may not be directly used in many international, regional and national laws, it is considered a crime. In *National Association of Software and Services Companies (NASSCOM) v. Ajay Sood*,[140] the High Court of Delhi held that, even though phishing was not specifically criminalized in law, it was an illegal act under law (i.e., an Internet fraud) because it involved a misrepresentation made in the course of trade leading to confusion as to the source and origin of the email causing immense harm not only to the consumer but even to the person whose name, identity or password was misused.

Phishing is a cyber-enabled crime and has been used to facilitate several forms of cyber-enabled crimes, and even cyber-dependent crimes (see the box below). Phishing schemes can be perpetrated by actors with or without technical skills and abilities because the tools and know-how are readily available online (as part of "crime as a service").[141] If the goal or one of goals of the phishing operation is to either take control of the target's system and/or steal information from the system, malware is used to infect the target's device.[142] For example, members of FIN7, an international cybercrime group, were charged with offences relating to illicit acts against the confidentiality, integrity and availability of computer data and systems. The members of the group used "spear phishing" (sending emails or other electronic forms of communication to a specific individual, organization or business in order to steal data for malicious purposes or to install malware on the target's computer system) and social engineering tactics to trick targets into opening a malicious email with

[136] England and Wales Court of Appeal, *R. v. Nicholas Webber* [2011] EWCA Crim 3135; *R. v. Nicholas Webber* [2012] 2 Cr. App. R. (S.) 41 (2011).

[137] *United States of America v. Jael Mejia Collado et al.*; *United States of America v. Ercan Findikoglu*; United States Attorney's Office, Eastern District of New York, "Leader of global cybercrime campaigns pleads guilty to computer intrusion and access device fraud conspiracies", 1 March 2016.

[138] United States Attorney's Office, Eastern District of New York, "Eight members of New York cell of cybercrime organization indicted in $45 million cybercrime campaign", 9 May 2013.

[139] See also UNODC, Education for Justice Module Series, Cybercrime, Module 2: general types of cybercrime, "Computer-related offences".

[140] *National Association of Software and Services Companies (NASSCOM) v. Ajay Sood & Others*, 119 (2005) DLT 596, 2005 (30) PTC 437 Del, Judgment, 23 March 2005.

[141] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 15 and 17.

[142] See, for example, UNODC, SHERLOC case law database, Germany, Case No. DEUx032, LG Bonn, Urteil vom 07.07.2009, 7 KLs 01/09 (phishing Trojans used). Available at **https://sherloc.unodc.org/**; United States, District Court, Western District of Washington at Seattle, *United States of America v. Fedir Oleksiyovych Hladyr*, Case No. CRl7-276RSL, Superseding Indictment, 25 January 2018; *United States of America v. Fedir Oleksiyovych Hladyr*, Case No. CR17-276RSM, Plea Agreement, 11 September 2019). (Carbanak malware); *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus* (Bayrob Trojan).

an attachment that contained malware (Carbanak malware) designed to steal customers' financial data.[143] Three FIN7 members (F.O.H., A.K. and D.I.) were extradited from Germany, Spain and Thailand, respectively, to the United States. Two members of the group (A.K. and F.O.H.) pleaded guilty to conspiracy to commit wire fraud and conspiracy to commit computer hacking.[144] The trial of the other defendant (D.I.) has been set for 2022.[145] Another member of the group (D.F.) was arrested in Poland; his extradition to the United States is still pending.

Fiscalía Metropolitana Sur, Chile, Rol Único de Causa No. 1700623543-3 (Zares de la Web) (Chile)

Between February 2014 and October 2018, clients of two banks and other financial institutions, as well as the banks themselves, were victims of successive cases of fraud (81 victims of fraud, including individuals and small businesses, were identified). Funds from various bank accounts were being transferred to accounts of recipients who were part of a criminal organization.

The criminal group's modus operandi consisted of the use of computer tools to deceive bank account holders and steal their passwords and security codes. The criminal group obtained the customer's banking information from databases on the deep web and later sent them cloned emails and fake links to web pages of their banks to obtain their passwords. By accessing the malicious links, the customers were involuntarily delivering their passwords to the false banking platform (i.e., on a fraudulent website). Members of the organized criminal group also impersonated bank executives while making telephone calls to obtain security codes from customers or posed as customer representatives to request a "coordinate card" to the bank (a security mechanism facilitated by the banks to approve transactions). "Chip spoofing" (or "SIM card hijacking") was also among the techniques used to obtain additional security keys. Once the coordinate card or the security device were materially obtained, the criminals had access to the security keys of the clients. With all of this information, they were able to access the accounts without authorization and transfer funds to previously recruited third parties. Participation in an organized criminal group was established given the systematic way in which they repeatedly committed fraud.

This criminal group operated in an organized manner within a hierarchical structure and with specific roles for each member. The hierarchical structure of the group was as follows: the group had two leaders (M.A.M. and D.Z.C.), who were in charge of organizing the illicit activity aimed at obtaining money from bank accounts and obtaining security codes and access to online (or virtual) accounts. This role implied general planning and distribution of tasks, which were followed by the other members, who made their personal contributions to the common goal. The leaders were in charge of granting and implementing the means of obtaining passwords (computer viruses, use of databases on the deep web, etc.) to seize bank information and make successive fraudulent electronic transfers. The leaders issued direct instructions, received reports, managed the money obtained and distributed the proceeds of the crime among the different members of the organization. The defendant, M.A.M., served as administrator, an essential role in the survival of the organization and the

[143] *United States of America, Fedir Oleksiyovych Hladyr*, Case No. CRl7-276RSL, Superseding Indictment; *United States of America v. Fedir Oleksiyovych Hladyr*, Case No. CR17-276RSM, Plea Agreement; see also court documents, United States Attorney's Office, Western District of Washington, *United States of America v. Fedir Oleksiyovych Hladyr, United States of America v. Dmytro Valerievich Fedorov, United States of America v. Andrii Kolpakov, United States of America v. Denys Iarmak*.

[144] United States District Court, Western District of Washington at Seattle, *United States of America v. Andrii Kolpakov*, Case No. 18-CR-159RSM, Plea Agreement, 16 November 2020; *United States of America v. Fedir Oleksiyovich Hladyr*, Case No. CR17-276RSM, 11 September 2019.

[145] United States Attorney's Office, Western District of Washington, *United States of America v. Fedir Oleksiyovych Hladyr, United States of America v. Dmytro Valerievich Fedorov, United States of America v. Andrii Kolpakov, United States of America v. Denys Iarmak*.

continuity of criminal operations. Other members of the groups were responsible for security and recruitment. These individuals were part of the permanent operational arms of the organization, receiving direct instructions from the leaders. They were responsible for providing security to the members of the organization, ensuring that the "recipients" actually delivered the money to the organization. They directly supervised the transfer of money and the "recruiters of recipients". The role of the recruiters of recipients was to find account holders who, in exchange for a commission, were willing to receive the money illegally obtained in their bank accounts. The recipients provided the organization their bank accounts, obtained the transferred money and delivered the illicit funds to the recruiters and the leaders.

The defendant was sentenced to one year in prison for the crime of criminal association,[a] two years' imprisonment for the crime of reiterated fraud[b] and two years' imprisonment for money-laundering.[c]

For more information about this case, see UNODC, SHERLOC case law database, Case No. CHLx007.[d]

[a] Article 293 in relation to article 467 of the Penal Code of Chile.
[b] Article 467, final paragraph, of the Criminal Code in relation to article 351 of the Criminal Procedure Code.
[c] Chile, Law No. 19,913 on the Establishment of the Financial Analysis Unit and Amendment of Several Provisions on Money-Laundering (2003), art. 27.
[d] Available at https://sherloc.unodc.org/.

When phishing is used against specific targets, it is known as spear phishing.[146] The Bayrob group perpetrated this type of fraud by pretending to be legitimate organizations, such as a well-known company offering protection against computer viruses and a well-known money transfer service, and sending to targets emails with infected attachments. When individuals who received the emails clicked on the attachment, malware was installed on their computers. This malware would harvest data and make the infected computers part of a botnet.[147] Data harvested from the infected systems (account access data, financial data and passwords) were also sold on the darknet.[148]

When such emails are used to target companies that have suppliers abroad and conduct wire transfers abroad, the tactic is known as business email compromise because the perpetrators pretend to be a known company that the target conducts business with. The emails sent making the requests are often spoofed emails (which are considered slight variations of the legitimate emails of known companies and personnel within those companies) and/or hacked email accounts of actual company personnel. "Operation Wire Wire", led by authorities in the United States, revealed that a criminal group had been masquerading as a legitimate entity that its targets (other companies) had worked with in some capacity in order to trick the targets into wiring money to the criminal group and/or its associates.[149] The proceeds of this fraud were laundered with the help of "money mules", who had opened various shell company bank accounts to launder the proceeds of this crime.

[146] See also UNODC, Education for Justice University Module Series, Cybercrime, Module 2: general types of cybercrime, "Computer-related offences".

[147] *United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus*, pp. 7–9.

[148] Ibid.

[149] United States District Court, District of Connecticut, *United States of America v. Adeyemi Odufuye and Stanley Hugochukwu Nwoke*, Case No. 3:16R232 (JCH), Indictment, 20 December 2016 (Operation Wire Wire case).

United States of America v. Obinwanne Okeke, Case No. 4:19-mj-00116 (E.D. Virginia, 2 August 2019)

Example of a business email compromise scam

A chief financial officer of a company received an email message that purportedly contained a weblink to the login page of a well-known software company.[a] The victim, having an email account with this host, trusted the link and viewed it as legitimate. He clicked on the link and the page that appeared resembled the login page of the software company. For this reason, the chief financial officer inserted his login credentials, which unbeknown to him, were captured by criminals, who then used this information to access his account.[b] His email account was then used to send fraudulent emails requesting wire transfers from other members of the company's financial team. Moreover, having observed company policy and the internal practice of forwarding emails from vendors, the perpetrator forwarded a fictitious email message he had created to make it look as if a vendor were sending an invoice.[c] Ultimately, this fraudulent scheme resulted in approximately US$ 11 million of wire transfers being sent to the perpetrator of this crime[d] and other conspirators.

[a] United States District Court, Eastern District of Virginia, *United States of America v. Obinwanne Okeke*, Case No. 4:19-mj-116-1, 2 August 2019.
[b] Affidavit in support of criminal complaint and arrest warrant (Obinwanne Okeke), 2 August 2019.
[c] Ibid.
[d] The defendant pleaded guilty to conspiracy to commit wire fraud (United States Attorney's Office, Eastern District of Virginia, "Nigerian businessman pleads guilty to $11 million fraud scheme", press release, 18 June 2020.

When higher-level executives in an organization are the targets of spear phishing, the tactic is referred to as "whaling" because the perpetrators targeting those individuals are seeking the highest payout possible. In the Europol report *Internet Organised Crime Threat Assessment 2020*, the term "CEO fraud" was used instead of "whaling".[150]

Phishing is more likely to be mentioned in court documents than terms such as spear phishing, business email compromise scam, "CEO fraud" and "whaling". The term "whaling" is not commonly found in court documents because it could be considered as a form of business email compromise if the targets are higher-level executives, such as the chief executive officer or the chief financial officer.

(c) Advance fee fraud scam

An advance fee fraud scam involves a request for a target to pay money in advance of receiving something of greater value.[151] When the money is obtained by the criminal, nothing is provided to the target in return. The criminals perpetrating this scam alternate the stories they use and the people (e.g., a friend, an acquaintance, a colleague or a stranger), agencies or organizations (e.g., banks, governments agencies or non-governmental agencies) that they pretend to be. The stories commonly used include the one about a government official seeking to transfer money out of a country and needing the assistance of the target and inheritance from a long-lost relative that requires a fee in order for the target to receive it. In the *Federal Republic of Nigeria v. Harrison Odiawa*,[152] the perpetrators pretended to be a representative from an agency of the Government of Nigeria and offered to transfer money to the target's company accounts and procure government contracts for the target's company. The advance fee fraud scam is locally known in Nigeria as "yahoo-yahoo", and perpetrators of this crime from that country and other countries in West Africa are known as "Yahoo boys" (although women also engage in this crime).[153] The ultimate goal of the advanced fee fraud scam is to get the target to transfer and/or otherwise provide money to the perpetrators.

[150] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 47.
[151] Maras, *Cybercriminology*.
[152] UNODC, SHERLOC Case law database, Case No. NGAx001. Available at **https://sherloc.unodc.org/**.
[153] UNODC, Nigeria, "West Africa takes lead in fighting 419 scams". Available at **www.unodc.org/**; Lily Hay Newman, "Nigerian email scammers are more effective than ever", *Wired*, 3 May 2018.

(d) Romance scam

The perpetrators of romance scams (or "catfishing") prey on peoples' emotions and need for companionship.[154] These scams often involve perpetrators opening up fake profiles on dating sites and social media platforms and/or using chat rooms and other forums and websites to identify targets. The perpetrators of this cybercrime use manipulation tactics to build rapport with the targets and gain their trust.[155] During these scams, the perpetrator quickly professes to have fallen in love with the target and continuously showers the target with affection, either through declarations of love or other overt acts (such as writing love letters, poems and songs) or by sending small gifts. After the perpetrator establishes rapport and builds up trust with the target, the perpetrator tries to get the target to provide money or goods or some form of service.

One story commonly used in a romance scam is that the perpetrator has experienced an emergency situation that requires the victim to send money (e.g., unexpected hospitalization or some other health-related emergency). The perpetrator may also request funds to be used to travel, to help in the payment of unpaid bills, to purchase items or to buy or rent a house or an apartment, etc. Or the perpetrator may request funds for marriage or for a wedding engagement. If the victim gives the perpetrator money, the victim may not hear from the perpetrator again or may receive future requests for money. In one case in France, an organized criminal group identified their potential victims on dating sites, taking advantage of the victims' loneliness and credulity. The offenders developed fake relationships with their victims.[156] Once they gained a victim's trust, they asked the victim for help, including money, to resolve a situation. In one case, the request was for assistance in getting a suitcase of money out of another country.[157] After receiving the money, offenders usually disappeared and did not contact their victims again. In another case, the modus operandi of the scam was somewhat different: the cybercriminals met with their victims in person in an attempt to get more money from them (thereby committing a romance scam both online and in person).

The purpose of the romance scam is to lure a target into a relationship (albeit a fake one, unbeknown to the target). A perpetrator can feign having a background and experiences similar to those of the target. This information is often available online in the target's dating profiles, social media accounts and on other sites that include information about the target. The perpetrator uses a fake image, often an attractive image from a website, platform or app obtained without authorization, that is resonant with his or her target. The type of profile encountered depends on who the target is. For example, some perpetrators who target retirees create profiles of individuals who are of a similar age, are in retirement and/or have recently been widowed. The fake profiles created by perpetrators often include employment that would justify significant absences in communication with the target and or the ability to travel. For instance, fake profiles on dating websites have been set up by people pretending to be military personnel. In one romance scam, which targeted women over 50 years old on online dating sites, the perpetrators pretended to be male members of the United States military.[158] Perpetrators create bank accounts in different names in order to receive money sent from their targets and/or to obtain money orders from targets that are then dispersed to other conspirators in the perpetrators' country.[159]

These scammers can manipulate targets into wittingly or unwittingly aiding and abetting crimes.Thus, their targets may wittingly or unwittingly engage in money-laundering, deliver controlled drugs and/or other illegal goods and scam other individuals out of money or goods.[160] These individuals are known as "mules". Mules may be motivated by fear, love or the prospects of financial compensation to wittingly commit an illicit activity.[161] Mules play a primary role in many crimes and cybercrimes, such as money-laundering and

[154] Monica T. Whitty and Tom Buchanan, "The online dating romance scam: the psychological impact on victims – both financial and non-financial", *Criminology and Criminal Justice*, vol. 16, No. 2 (April 2016), pp. 176–194; Tom Buchanan and Monica T. Whitty, "The online dating romance scam: causes and consequences of victimhood", *Psychology, Crime & Law*, vol. 20, No. 3 (March 2013), pp. 261–283.

[155] Maras, *Cybercriminology*, p. 244.

[156] France, Tribunal de grande instance de La Roche-sur-Yon, 24 septembre 2007.

[157] Ibid.

[158] United States Attorney's Office, Eastern District of Kentucky, "Nigerian national pleads guilty in romance fraud and grant fraud scheme", press release, 24 August 2020.

[159] Ibid.

[160] Maras, *Cybercriminology*.

[161] Better Business Bureau, "Fall in love: go to jail – BBB report on how some romance fraud victims become money mules" (February 2019).

various online frauds. Money mules may be wittingly recruited and/or solicited online in order to engage in money-laundering for criminals by opening up a bank account and receiving money from others, which is then forwarded to the criminals in various ways (through wire transfers, by purchasing prepaid cards and mailing those cards, through online payment platforms, etc.). Other money mules may be duped into opening up bank accounts to receive or transfer funds from a criminal masquerading as a romantic interest for what they believe to be a legitimate purpose; or the money mules may be duped into utilizing their own bank account to receive and transfer the funds from a criminal pretending to be a romantic interest (or legitimate employer).

United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase, and Rasaq Aderoju Raheem, Case No. 17-60397 (5th Circuit, 4 March 2019) (United States of America)

An organized criminal group stole the personal and financial information of targets and impersonated the victims whose information they had stolen to obtain money and transfer funds from the victims' bank accounts. The defendants and other conspirators then conducted romance scams with the aim of convincing the targets of the scams to launder the proceeds of their crimes (e.g., by serving as money mules) and engage in financial fraud, such as the purchasing of goods with stolen credit cards and the cashing of counterfeit cheques and money orders.[a] The defendants (O.S.A., R.A.R. and F.A.M.) were convicted of multiple criminal charges, including conspiracy to commit bank fraud, wire fraud, mail fraud, identity theft and money-laundering (with the exception of F.A.M.).[b] O.S.A. received a sentence of 95 years' imprisonment and R.A.R. received a sentence of 115 years' imprisonment.[c]

For more information about this case, see UNODC, SHERLOC case law database, Case No. USA005R.[d]

[a] *United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase and Rasaq Aderoju Raheem*, Case No. 17-60397.
[b] Ibid.
[c] United States Department of Justice, Office of Public Affairs, "Three Nigerians sentenced in international cyber financial fraud scheme", press release, 25 May 2017.
[d] Available at https://sherloc.unodc.org/.

(e) Other fraud-related scams

Various online scams have been perpetrated worldwide to steal the targets' personal information, financial data, health (or medical) data and money. Criminals who commit this type of fraud seek to manipulate, dupe or trick individuals into providing information or money or engaging in desired acts. Online scams can be perpetrated via unsolicited email messages, telephone calls, text messages, social media platforms, applications and websites. Examples of online scams are work-related scams, lottery scams, auction fraud, online sales scams and subscription traps.

Work-related scams include the advertisement of and recruitment for job opportunities that can be a front for illegal activities and operations. Illegal activities that masquerade as jobs can include working for an employer that requires the employee: to receive and ship merchandise from home; to receive and transfer funds from personal bank accounts to other bank accounts; to receive and cash fraudulent cheques; to receive funds from various sources, buy goods or prepaid credit cards with this money and then mail those items to others; and/or to receive funds from various sources and then transfer this money to others using online payment services, money orders, cryptocurrencies and/or other digital currencies.[162] Job-related scams may also include advertisement for work opportunities that do not exist. For example, in India, in the *State of Maharashtra v. Opara Chilezien Joseph*, the defendants were charged with and convicted for their respective roles in sending fraudulent email and SMS messages to targets about getting a job in England.[163]

[162] Maras, *Computer Forensics*, p. 149.
[163] India, *State of Maharashtra v. Opara Chilezien Joseph*, Regular Criminal Case No. 724/2012, 28 October 2013.

The purpose of this scam was to convince the targets to send money for a purported (albeit fictitious) fee associated with the job. In this case, the defendants also perpetrated lottery scams, whereby the defendants solicited funds from the targets by claiming that they had won a lottery or prize for which fees must be paid to collect the winnings.

Another online scam is auction fraud. Auction fraud occurs when the seller of an item that is being auctioned deceives buyers in order to defraud them.[164] In France, a member of an organized criminal group was sentenced to six years of imprisonment for his role in engaging in online auction fraud.[165] The group recruited people to retrieve the money from the fraudulent online sales at various post offices using forged identity documents (i.e., passports). The individuals who were recruited to retrieve the money were paid for their services, as well as travel and subsistence expenses. Auction fraud may also include the non-delivery of items after payment has been rendered and the delivery of items not as advertised and/or of lower quality than what was advertised. This type of fraud may involve sellers purposely driving up bids by bidding on their own items multiple times using different accounts (a form of shill bidding).

United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus, Case No. 1:16-CR-00224 (N.D. Ohio, 8 July 2016) (Bayrob Group) (United States of America)

An organized criminal group perpetrated several cybercrimes, one of which was online auction fraud. The fraud was perpetrated by members of the group by posting hundreds or thousands of listings for automobiles, motorcycles and other high-priced goods on online auction sites.[a] The images of the items being sold that were included in the postings were infected with their malware (the Bayrob Trojan).[b] When individuals clicked on the images of the items, their devices were infected with the malware, which had been designed to redirect the individuals to web pages that looked identical to the legitimate web pages of the auction sites. For example, their fake web pages included the trademark of a well-known online auction site and had a similar layout, design and style of the legitimate web pages of that auction site. The fake web pages, however, prompted users to pay for the auctioned items using something called an "eBay escrow agent", which did not exist on the legitimate platform of the auction site.[c] This purported service claimed to hold the money of the buyer in escrow until the item was received and the buyer was satisfied with the condition of the item delivered before the buyer's funds were released to the seller. The web pages also included a live chat function that enabled the unknowing users to speak with members of the group posing as customer service agents of the online auction site.[d] The victims of this online auction fraud never received the items they had paid for and never received a refund for the money they had paid for the non-delivered items.[e]

One of the defendants (T.D.) pleaded guilty to aggravated identity theft, wire fraud and conspiracy offences relating to wire fraud and money-laundering and received a sentence of 10 years of imprisonment for his crimes.[f] B.N. and R.M. were charged with, convicted and sentenced to 20 and 18 years of imprisonment, respectively, for aggravated identity theft, wire fraud and conspiracy offences relating to wire fraud and money-laundering, as well as conspiracy to traffic in counterfeit service marks.[g]

For more information on this case, see see UNODC, SHERLOC case law database, Case No. USAx170.[h]

[a] *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclaus*, p. 8.
[b] Ibid.
[c] Ibid.
[d] Ibid.
[e] Ibid.
[f] United States Attorney's Office, Northern District of Ohio, "Multiple victim case update: United States v. Nicolescu et al.", 16 January 2020; United States, Federal Bureau of Investigation, "Romanian hackers sentenced".
[g] Ibid.; United States Department of Justice, Office of Public Affairs, "Two Romanian cybercriminals convicted of all 21 counts relating to infecting over 400,000 victim computers with malware and stealing millions of dollars", 11 April 2019.
[h] Available at https://sherloc.unodc.org/.

[164] For more information on online auction frauds, see Maras, *Computer Forensics*, pp. 113–115 and 143.
[165] France, Cour de cassation, Chambre criminelle, No.11-84.437, 21 March 2012.

Another example of an online scam is online sales fraud. This type of fraud involves the online purchasing – from websites that may be designed to look similar to known and/or popular commercial websites – of goods: that do not exist, that are never delivered, that are counterfeit but advertised as authentic or that are damaged, of lower quality or otherwise not as advertised.[166] In Germany, a defendant operated over 20 online shops, mostly offering coffee machines or other kitchen items.[167] The websites were modelled after popular e-commerce websites, including the website of a well-known multinational online sales enterprise. Customers had to pay in advance and received an automated order confirmation. Payment agents then transferred the money received to the defendant. The products were never sent to the customers. The fraudulent operation took place mostly in Spain and, to a lesser extent, in the Netherlands. The defendant pleaded guilty and received a sentence of five years and five months of imprisonment.

A further example of an online scam is a "subscription trap", where websites offer for a fee services that are offered free of charge on other websites; such services may include access to databases of publicly available information, love and sex tests and the use of software that is available elsewhere at no cost (freeware). A case in Germany revealed that a group included "subscription traps" on various websites.[168] On the group's website, the registration pages were designed so that individuals signing up for the services on the site would not notice that there was a fee associated with the use of the services. The information about the cost associated with the use of the services was located at the bottom of the login page and was not visible to users with average-sized monitors unless they scrolled down to the end of the page. Individuals could complete their registration without needing to scroll down to the end of the page, where the cost was indicated. Once the individuals registered on the page, they received an email confirming the contract and ordering them to pay €60 or €84 (depending on the type of service they had signed up for). If they did not pay, the lawyer of the group (one of the defendants) sent payment and collection notices to the individuals who had registered for the service. The defendants were charged with and convicted of numerous crimes, including fraud (see the discussion of copyright infringement in chapter V, section B.4, below).[169]

2. Computer-related identity offences

Identity-related crime refers to acts whereby the identity of a target is unlawfully assumed and/or misappropriated and/or this identity and/or any information associated with it is used for unlawful purposes.[170] Identity-related information is considered a commodity online. Identity-related information, such as personal, medical and financial data, is bought, sold and traded online for a fee on the clearnet and the darknet. The type of identity-related information that is sought by criminals includes identification numbers (e.g., social security numbers), passport information, national identification information, driving licence information, medical insurance data, financial account information, credit card data, debit card data, online credentials (i.e., account information and passwords), email addresses, telephone numbers, IP addresses and media access control addresses.[171]

[166] For more information, see Maras, *Computer Forensics*, p. 115.

[167] UNODC, SHERLOC case law database, Case No. DEUx030, LG München, Urteil vom 07.06.2017, 19 KLs 30 Js 18/15. Available at **https://sherloc.unodc.org/**.

[168] UNODC, SHERLOC case law database, Case No. DEUx031, LG Hamburg, Urteil vom 21.03.2012, 608 KLs 8/11. Available at **https://sherloc.unodc.org/**.

[169] Section 263 (Fraud) of the German Criminal Code (Strafgesetzbuch). For further information about these crimes, see UNODC, SHERLOC case law database, Case No. DEUx031.

[170] See also UNODC, Education for Justice University Module Series, Cybercrime, Module 2: general types of cybercrime, "Computer-related offences".

[171] UNODC, *Handbook on Identity-related Crime* (Vienna, 2011), pp. 12–15.

Poder Judicial de Córdoba – "Emiliozzi, Arturo Osvaldo y otros PSSAA Estafa, etc." – Expediente SAC No. 2654377 (Argentina)

Between July 2015 and February 2017, five defendants (V.I.S., A.O.E., S.G.M., D.M.M.R. and M.J.F.), together with other unidentified persons, were accused of forming and maintaining an organized criminal group for the purpose of committing fraud. The group allegedly started an illegal business oriented to the commercialization of agricultural products, mainly agrochemicals and rural machinery, fraudulently acquired and sold to third parties in different areas in Argentina.

The group allegedly had a clear division of roles and tasks for members. Of the five defendants, V.I.S., A.O.E. and S.G.M. had leadership roles and were responsible for organizing the activities of the group, whereas D.M.M.R. and M.J.F. executed assigned tasks. V.I.S. was in charge of (through third parties) obtaining the information related to different credit card holders for the purchase of agricultural products and contacting different businesses by telephone or by email. He committed fraud by using the identity of the credit card holders and/or their agents and deceiving merchants and convincing them to sell him agricultural products. He was also responsible for hiring drivers to transport the acquired products. A.O.E. and S.G.M. were in charge of organizing the trafficking in fraudulently obtained products, including the receipt, storage, distribution and redistribution of the products. They also administered and divided the profits that corresponded to each member of the gang and recruited new members. Two of the new members recruited were D.M.M.R. and M.J.F., who were responsible for arranging spaces for the sale of the products. D.M.M.R. received and stored the agrochemicals in rural areas in the Province of Buenos Aires, while M.J.F. provided the legal facade for this fraud through his commercial farm, Agrocampo, which sold agricultural products in the Province of Córdoba.

The defendants were charged with and convicted for their crimes. Specifically, V.I.S. was found guilty of fraud[a] and sentenced to four years and six months of imprisonment and ordered to cover procedural costs.[b] S.G.M. was initially sentenced to five years and six months of imprisonment and ordered to pay a fine of 400 Argentine pesos and procedural costs; his sentence was subsequently reduced to three years' imprisonment, and he was ultimately ordered to pay a fine of $Arg 200 and procedural costs. A.O.E. was found guilty of fraud through the use of a false private documents, was sentenced to two years of imprisonment and was ordered to pay procedural costs. S.G.M. and A.O.E. were also found criminally responsible for the crime of illicit association, as co-organizers[c] of the fraud committed by means of illegitimate use of stolen credit card data.[d]

For more information about this case, see UNODC, SHERLOC case law database, Case No. ARGx013.[e]

[a] Art. 172 of the Penal Code of Argentina.
[b] Arts. 12, 40, 41, 50 and 58 of the Penal Code and arts. 550–551 of the Penal Procedure Code of Argentina.
[c] Arts. 45 and 210 of the Penal Code.
[d] Arts. 45, 55 and 173 (15) of the Penal Code.
[e] Available at https://sherloc.unodc.org/.

The methods used by criminals to obtain non-digital and digital identity-related information include: dumpster diving; mail theft or the redirection of mail; theft of identity documents; the use of publicly available information (e.g., public records); skimming; phishing; "pharming" (a combination of the words "phishing" and "farming"), or installing a malicious code on a computer or server that automatically directs the user to a fraudulent website that mimics the appearance of a legitimate website; malware; and hacking.[172] Criminals may also obtain identity-related information by conducting simple searches for such information using search engines, social media platforms, websites and online public and private databases.[173] All of the aforementioned online sites and repositories serve as a rich source of information that includes a mix of data

[172] UNODC, *Handbook on Identity-related Crime* (Vienna, 2011), pp. 15–19.
[173] Ibid., pp. 19 and 21–22.

that individuals willingly share with the platforms, as well as data that are collected, made available and distributed about individuals and consolidated about them without the individuals' knowledge and/or consent (or, at the very least, without their informed consent). This information can then be widely distributed online via chat rooms, forums, websites, social media platforms, peer-to-peer file-sharing networks, instant messaging, text messages and encrypted and unencrypted communications applications, as well as via darknet sites.

United States of America v. Sergey Medvedev, Case No. 2:17-CR-306-JCM-VCF (D. Nevada, 26 June 2020) and *United States of America v. Valerian Chiochiu*, Case No. 2:17-CR-306-JCM-PAL (D. Nevada, 31 July 2020) (the Infraud Organization) (United States of America)

The Infraud Organization, founded in 2010, was active between 2010 and 2018. The slogan of the organization was "In fraud we trust". The organization operated as a criminal enterprise with the objective of financially enriching its members through the commission of cybercrime, particularly online fraud and identity theft. The illicit acts that the organization engaged in included money-laundering; trafficking in stolen means of identification; trafficking in and production and use of counterfeit identification; identity theft; trafficking in and production and use of unauthorized and counterfeit access devices; bank fraud; and wire fraud.[a] The organization had over 10,000 members throughout the world before it was shut down by United States criminal justice agencies in 2018.[b] The Infraud Organization was well known for selling and advertising illicit goods and services on an online forum bearing the name of the organization.

The roles of individuals that were part of this criminal enterprise included the following:[c]

(a) *Administrators*. Administrators were responsible for long-term strategic planning of the enterprise and daily management tasks such as determining responsibilities and levels of access of all members, vetting prospective members, deciding which individuals could join the organization, and rewarding and punishing existing members;

(b) *Supermoderators.* "Supermoderators" were responsible for moderating content by reviewing contraband for sale, editing and deleting posts based on reviews, and mediating disputes between buyers and vendors. The content they moderated was assigned on the basis of either geographical area or criminal expertise;

(c) *Moderators*. Moderators had some of the same responsibilities for moderating content as "supermoderators", but had less authority and fewer privileges;

(d) *Vendors*. Vendors were individuals who sold and/or advertised illicit goods and services on the site;

(e) *VIP members*. VIP members were longstanding, distinguished members of the platform;

(f) *Member*s. General members of the forum.

The founders of the organization were S.B. and S.M. In addition to being one of the founders, S.M. served as the administrator of the forum and ran the escrow service of the organization,[d] which was in place to minimize instances of vendor fraud. Fraudulent vendors were known on the site as "rippers".[e] These escrow services held funds for a purchase in escrow until the buyer received the items purchased (in good order). For quality control of contraband recovered from acts of fraud and identity theft, members also provided feedback and ratings of vendors and their products. To protect participants in this criminal enterprise, measures were taken to secure the forum and restrict access to it. S.B. established rules governing members' conduct, which were enforced by administrators, moderators and "supermoderators" of the site.[f] Members who violated these rules were punished by bans from the forum and other sanctions. All new members had to be vetted before being granted access to the forum.

One of the founders of the Infraud Organization, S.M., pleaded guilty to conspiracy to engage in a racketeer-influenced corrupt organization.[g] On 19 March 2021, he was sentenced to 10 years' imprisonment.[h] The other founder, S.B., is currently still at large. V.C., a member of the Infraud Organization and malware author, also pleaded guilty to conspiracy to engage in a racketeer-influenced corrupt organization.[i]

For more information on these cases, see see UNODC, SHERLOC case law database, Case No. USAx171.[j]

[a] *United States of America v. Svyatoslav Bondarenko et al.*, p. 6.
[b] United States Department of Justice, Office of Public Affairs, "Russian national pleads guilty for role in transnational cybercrime organization responsible for more than $568 million in losses", press release, 26 June 2020.
[c] *United States of America v. Svyatoslav Bondarenko et al.*, pp. 12–14.
[d] *United States of America v. Svyatoslav Bondarenko et al.*, p. 15.
[e] "Rippers" are individuals who do not deliver purchased items and/or deliver items of poor quality (*United States of America v. Svyatoslav Bondarenko et al.*, p. 9).
[f] *United States of America v. Svyatoslav Bondarenko et al.*, p. 25.
[g] United States District Court, District of Nevada, *United States of America v. Sergey Medvedev*, Case No. 2:17-CR-306-JCM-VCF, Plea Agreement, 26 June 2020.
[h] United States Department of Justice, Office of Public Affairs, "Foreign nationals sentenced for roles in transnational cybercrime enterprise", press release, 19 March 2020.
[i] United States District Court, District of Nevada, *United States of America v. Valerian Chiochiu*, Case No. 2:17-CR-306-JCM-PAL, Plea Agreement, 31 July 2020.
[j] Available at https://sherloc.unodc.org/.

3. Falsified medical product-related crime

Falsified medical product-related crime refers to illicit acts whereby the "identity",[174] "composition"[175] or "source"[176] of a medical product is "deliberately/fraudulently misrepresented".[177] Intellectual property right considerations are excluded from this definition. Falsified medical products are considered distinct from substandard and unregistered/unlicensed medical products (see figure I).[178]

[174] The World Health Organization (WHO) defines "identity" as "the name, labelling or packaging or to documents that support the authenticity of an authorized medical product" (document A70/23, annex, appendix 3, para. 7 (c)).

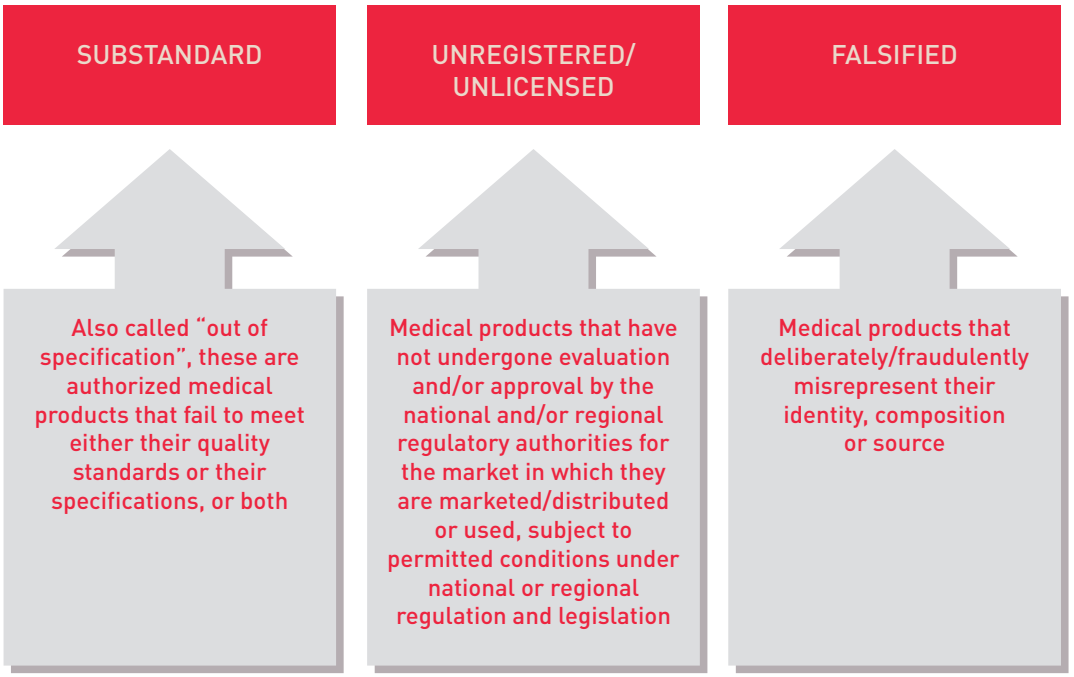
[175] WHO defines "composition" as "any ingredient or component of the medical product in accordance with applicable specifications authorized/recognized by" national and/or regional regulatory authorities (document A70/23, annex, appendix 3, para. 7 (c)).

[176] WHO defines "source" as "the identification, including name and address, of the marketing authorization holder, manufacturer, importer, exporter, distributor or retailer, as applicable" (document A70/23, annex, appendix 3, para. 7 (c)).

[177] The WHO defines "deliberate/fraudulent misrepresentation" as "any substitution, adulteration, reproduction of an authorized medical product or the manufacture of a medical product that is not an authorized product" (document A70/23, annex, appendix 3, para. 7 (c)).

[178] UNODC, Combating Falsified Medical Product-Related Crime: A Guide to Good Legislative Practices (Vienna, 2019), p. 8.

Figure I. Substandard, unregistered/unlicensed and falsified medical products



Source: World Health Organization (WHO), Report by the Director-General on the Member State mechanism on substandard/spurious/falsely-labelled/falsified/counterfeit medical products, document A70/23, annex, appendix 3, para. 5.

Falsified medical products have negative public health, economic and socioeconomic consequences.[179] They may be of poor quality, unsafe or ineffective. They may endanger health, prolong illness, promote antimicrobial resistance and the spread of drug-resistant infection, and kill patients.[180] They may also undermine confidence in health professionals, health-care systems and legitimate medical products, resulting in further negative public health consequences if patients forego treatment or seek alternative treatment from unregulated care providers.[181]

The coronavirus disease (COVID-19) pandemic has shed light on the threats posed by falsified medical products.[182] COVID-19 has been the catalyst for the emergence of a global market for trafficking in personal protective equipment.[183] There is also evidence of trafficking in other forms of falsified medical products purporting to test, treat or prevent COVID-19.[184]

[179] See WHO, *A Study on the Public Health and Socioeconomic Impact of Substandard and Falsified Medical Products* (Geneva, 2017), pp. 15–19; WHO, *WHO Global Surveillance and Monitoring System for Substandard and Falsified Medical Products* (Geneva, 2017), pp. 5–7; see also Tim K. Mackey and Gaurvika Nayyar, "A review of existing and emerging digital technologies to combat the global trade in fake medicines", *Expert Opinion on Drug Safety*, vol. 16, No. 5 (April 2017), p. 587.

[180] WHO, *A Study on the Public Health and Socioeconomic Impact*, pp. 15–16.

[181] Ibid., p. 17.

[182] See also UNODC, Research and Trend Analysis Branch and Global Research Network, "Report on COVID-19-related trafficking of medical products as a threat to public health", Research brief (Vienna, 2020).

[183] Ibid., p. 10.

[184] Ibid., p. 9.

Trafficking in falsified medical products takes place both offline and online.[185] Such trafficking takes place via online marketplaces, online pharmacies, e-commerce platforms and social media and other platforms.[186] In recent years, the number of online pharmacies, as well as the number of people purchasing medical products online, has greatly increased.[187] Nevertheless, the majority of online pharmacies conduct business illegally and without appropriate safeguards, including by not requiring a valid prescription, operating without a valid licence/certification and failing to meet national or international pharmacy regulations.[188] Online pharmacies pose particular challenges to investigating and prosecuting authorities, including practical difficulties in identifying physical locations and jurisdictional challenges.[189]

United States of America v. Kristjan Thorkelson, 14-CR-27-BU-DLC (D. Mont., 10 December 2018)

In 2001, K.T. founded Canada Drugs as an online pharmacy based in Winnipeg, Canada. The business model of Canada Drugs was based on illegally importing unapproved and misbranded prescription pharmaceutical drugs into the United States from abroad and selling the drugs illegally to consumers throughout the United States. K.T., the defendant and chief executive officer of Canada Drugs, and other conspirators oversaw the distribution of substantial quantities of prescription drugs within the United States, including clinical cancer medications, that were not approved by the Food and Drug Administration of the United States.[a] In addition to unapproved and misbranded prescription pharmaceutical drugs, two counterfeit clinical cancer medications (both purportedly containing bevacizumab) were distributed to physicians in the United States.

The defendant, companies associated with him (Canada Drugs, Rockley Ventures, Global Drug Supply and River East Supplies) and those conspiring with him were charged with: conspiracy to smuggle goods into the United States in contravention of Title 18, sections 371 and 545, of the United States Code; conspiracy to commit money-laundering in violation of Title 18, sections 1956 (h) and 1957; and international money-laundering in contravention of Title 18, section 1956 (a), paragraph (2)(A). Ultimately, the defendant pleaded guilty to the crime of misprision of felony for having knowledge of the actual commission of a felony cognizable by a court of the United States, concealing the felony and not informing a judge or other person in civil or military authority under the United States of the felony.[b] For this crime, the defendant was sentenced to five years of probation and six months of house arrest and was required to pay a fine of US$ 250,000.

CanadaDrugs.com ceased its operations in 2018, and Canada Drugs was required to surrender its domain names. Canada Drugs and its associated companies were sentenced to five years' probation and were required to forfeit US$ 29 million in proceeds and to pay a fine of US$ 5 million.[c]

For more information about this case, see UNODC, SHERLOC case law database, Case No. USAx108.[d]

[a] UNODC, SHERLOC case law database, Case No. USAx108, United States of America, Plaintiff, vs. Kristjan Thorkelson, Defendant.
[b] United States Code, Title 18, sect. 4, Misprision of felony.
[c] United States Attorney's Office, District of Montana, "Canadian drug firm admits selling counterfeit and misbranded prescription drugs throughout the United States", press release, 13 April 2018.
[d] Available at https://sherloc.unodc.org/.

[185] See Tim K. Mackey and others, "Counterfeit drug penetration into global legitimate medicine supply chains: a global assessment", *American Journal of Tropical Medicine and Hygiene*, vol. 92, Suppl. No. 6 (2015).

[186] WHO, "Substandard and falsified medical products", 31 January 2018; WHO, *WHO Global Surveillance and Monitoring System*, p. 15.

[187] WHO, *WHO Global Surveillance and Monitoring System*, p. 15.

[188] Mackey and Nayyar, "A review of existing and emerging digital technologies", p. 589.

[189] WHO, *A Study on the Public Health and Socioeconomic Impact*, p. 22; WHO, *WHO Global Surveillance and Monitoring System*, p. 16.

4. Counterfeiting

Counterfeiting involves the unlawful manufacture, sale and distribution of fake currency, documents or products.[190] Counterfeits are created for a variety of identity-related documents (e.g., identification documents, passports, driving licences), money and goods such as food, drinks, electronics, software, toys, automobile parts, chemicals, alcohol, cigarettes, clothing, shoes, accessories, toiletries and household products. Counterfeit products pose significant threats to the economy, the environment, and health and safety.[191]

Traditional organized criminal groups are involved in trafficking in counterfeit products. The groups mainly do not focus exclusively on trafficking in counterfeit products but commit this form of trafficking along with other forms of serious crime, such as a drug trafficking, trafficking in human beings and money-laundering.[192] The funds obtained from trafficking in counterfeit products are often subjected to money-laundering and/or used to develop and sell more counterfeit goods and/or engage in other forms of serious crime.[193]

The availability, manufacture and distribution of counterfeit products have expanded as a result of the ease of movement of individuals across borders and advances in ICT.[194] Organized criminal groups have produced, sold and distributed counterfeit money, documents and goods throughout the world, advertising the sale of these items on both the clearnet and the darknet. Trafficked counterfeit products enter the market either by being introduced into the legitimate market through online commercial websites, social media platforms and/or other places online or by being introduced into the illegitimate market, for example, through the sale of counterfeit products on darknet sites predominantly dedicated to the sale of illicit goods and services. The illegal markets online were termed by a German court as the "underground illegal economy".[195]

Counterfeit products can be created, represented and/or marketed to look like copyrighted, trademarked and/or patented goods in violation of intellectual property laws. One example is pirated copyright goods, which are defined in the Agreement on Trade-Related Aspects of Intellectual Property Rights (art. 51) as any goods which are copies made without the consent of the right holder or person duly authorized by the right holder in the country of production and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the law of the country of importation.[196] For example, in *Queen v. Paul Mahoney*,[197] the appellant, with other known and unknown conspirators, created and operated websites that enabled individuals to access and view newly released films and television programmes for free.

[190] For more information on counterfeiting, see UNODC, *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (United Nations publication, 2010), chap. 8.

[191] UNODC, "Counterfeit goods: a bargain or a costly mistake?", Factsheet (2012); Italy, Ministry for Economic Development, Department for Enterprise and Internationalization, General Anti-Counterfeiting Directorate, "No to fake: the counterfeiting in the food sector–consumer guide" (Rome, n.d.).

[192] UNODC, "Counterfeit goods".

[193] UNODC, "'Counterfeit: don't buy into organized crime' – UNODC launches new outreach campaign on $250 billion a year counterfeit business", 14 January 2014.

[194] UNODC, "Counterfeit goods".

[195] This case involved the sale of counterfeit money and forged identification documents, as well as the sale of drugs, on online illicit markets (UNODC, SHERLOC case law database, Case No. DEUx025, LG Duisburg, Urteil vom 05.04.2017, 33 KLs-111 Js 32/16 - 8/16).

[196] WHO, document A70/23, annex, appendix 3, footnote 1.

[197] United Kingdom of Great Britain and Northern Ireland, *Queen v. Paul Mahoney* [2016] NICA 27.

TGI Lille, 7e ch.corr., jugement du 29 janvier 2004 (France)

Between 2000 and 2002, the defendants, members of the online forum Boom-e-rang, participated in a scheme to share on the forum pirated content such as films, music and video games. Under this scheme, any member who wanted to access the files had to, in return, give access to other content. As the forum did not have the capacity to store all the files, members of the forum hacked into open-source ftp servers, such as university servers, and provided access to the servers to forum members to enable them to upload pirated content for download by other members. Some forum members operated as "scanners", using scanning software to find open-source ftp servers. Others were "uploaders", overseeing the uploading of files onto the hacked servers. Two members of the forum also committed a scam using stolen credit card data and software generating credit card numbers to buy DVDs and compact discs.

In France, the national police were made aware of the Boom-e-rang forum when a third party who was being investigated for electronic fraud divulged the name of two members of the forum and informed the police of the offences that they had committed. The national police conducted electronic surveillance of the forum and collected several IP addresses that were used to identify forum members.

In this case, the defendants were charged with illegal access to a computer system with the aggravating factor of system interference, as well as with illegal introduction of data into a computer system. As the system interference resulted from the illegal introduction of data into the computer systems (reducing their storage capacity) and not illegal access to the computer system itself, the court held that the aggravating factor of system interference could not be applied to the case. The court also held that the offence of illegal access to a computer system could be applied even if the computer systems that had been accessed had not been protected from breach.

The 13 defendants were convicted of charges relating to hacking into servers, uploading pirated material to the servers and downloading pirated material from the servers. One defendant, J.D., was found guilty of committing a scam and was sentenced to 10 months' imprisonment. All the other defendants were sentenced to terms of imprisonment ranging from two to four months. All custodial sentences were suspended.

The two defendants convicted for offences related to the stolen credit card scam were ordered to pay a symbolic sum of €1 to the victim, as well as €200 for legal fees. All defendants were sentenced to pay jointly €1 as provisional damages to the 23 other victims, with the matter being referred to a civil court for further determination.

For more information about this case, see UNODC, SHERLOC case law database, Case No. FRAx028.[a]

[a] Available at https://sherloc.unodc.org/.

Perpetrators of online copyright infringement may be part of communities that illegally distribute copyrighted works for free to obtain accolades from members of their community. For instance, in *Regina v. Reece Baker and Sahil Rafiq*,[198] the appellants (S.R. and R.D.B.) had leadership roles in release groups (i.e., they formed and/or ran the groups), which often competed with each other to make the best copy of an original copyrighted work freely and widely available or to be the first to illegally release a copyrighted work.

[198] United Kingdom, Royal Courts of Justice, *Regina v. Reece Baker and Sahil Rafiq* [2016] EWCA Crim 1637, Approved Judgment, 18 October 2016.

LG Leipzig, Urteil vom 14.06.2012, 11 KLs 390 Js 191/11 (Germany)

The LG Leipzig case involved the criminal prosecution of the founder of the German-language streaming portal (Kino.to), the defendant, for having made available online pirated versions of more than 100,000 copyrighted works, including films, documentaries and television series. Starting in March 2008, the defendant, along with seven others who were prosecuted separately, gradually started forming an organized criminal group in order to operate this website. Until June 2011, the website was the biggest German website for pirated films and was listed as one of the 50 most visited websites in Germany, at times receiving over four million hits per day. The domain of the website was registered in countries such as Tonga. The access portal to the website was at first placed on servers in the Netherlands; subsequently, starting in mid-2008, it was placed on servers in the Russian Federation. The location of the administrators, as well as the focus of the group's operations, was, however, Germany.

On the website, the defendant and his accomplices provided over one million links to copyrighted works of film and television free of charge, without having the rights to do so. In total, 1,360,450 links were made public on this website. The links were used to stream or download the pirated content. The pirated content was hosted on file hosting services selected by uploaders (those who uploaded pirated content to the website). The uploaders and file host service providers were not part of the core employees of Kino.to. However, some of the file host services used by the site were operated by the defendant or the members of the group who were subsequently prosecuted separately. File hosting services that were operated by the defendant or other members of the group were preferred and were given competitive advantage in that their links were placed on the top of the website.

Communication between the core employees usually took place using a well-known software application that provides videophone and videoconferencing capabilities. Written communication took place using the message tool of the access control protocol. When important decisions were to be made, videoconferences were held, and all core employees would usually participate. The employees tasked with publishing the links were responsible for communicating – using their aliases – with the uploaders and file hosting service providers via the same access control protocol.

The defendant was prosecuted for the commercial exploitation of copyrighted works contrary to intellectual property laws.[a] The court held that the inclusion of pages on a site that was linked to stored copyright content on a different site (e.g., content-sharing hosting sites) without the consent of the copyright holder was a violation of copyright law.[b] For the over one million counts of commercial unlawful exploitation of copyrighted works to which the defendant pleaded guilty, he received a sentence of four years and six months of imprisonment and was required to pay more than €3.7 million in compensation.

For more information on this case, see UNODC, SHERLOC case law database, Case No. DEUx033.[c]

[a] Specifically, section 106 of the German Act on Copyright and Related Rights (Urheberrechtsgesetz) (see UNODC SHERLOC case law database, Case No. DEUx033).
[b] LG Leipzig, Urteil vom 14.06.2012, 11 KLs 390 Js 191/11 (kino.to was the largest German-language platform providing links to pirated copies of films and television shows).
[c] Available at https://sherloc.unodc.org/.

5. Extortion, blackmail and ransom

Extortion is an illicit act whereby an individual seeks to obtain money or other material or financial benefits or force a target to engage in some act through intimidation, fear, violence or threat of violence or some other form of harm.[199] The nature of this harm or threatened harm varies in national law. While national

[199] Marie-Helen Maras, *Real Criminology* (forthcoming).

extortion laws predominantly require that a threat be made, they do not require something to be actually obtained from the target as a result of the threat for the act to be considered extortion.

Individuals, groups, private organizations, non-governmental organizations and government agencies are common targets of extortion. When extortion is facilitated through ICT, it is referred to as cyberextortion. Cyberextortion, however, is not a term identified in law. Extortion and fraud-related laws are commonly used to prosecute individuals who commit this cybercrime. Cyberextortionists commit Internet fraud, distributed denial-of-service attacks, interpersonal cybercrime[200] and other forms of cybercrime in order to force targets to engage in desired acts or to provide offenders with money, goods and/or services. Blackmail is a form of extortion. Blackmail occurs when an individual threatens to reveal compromising information designed to embarrass or cause some other form of harm to the target unless a demand is met.

Ransom can be described as the holding of something or someone of value to the target and threatening to cause harm unless a payment is rendered to the offender. Criminals that perpetrate cyber-dependent and cyber-enabled crime have demanded ransom from targets. For example, members of the TDO hacking group were known for hacking several organizations in the health, entertainment, finance, commercial, real estate and transportation sectors, stealing personal information from the systems they hacked and then seeking ransom from the targets.[201] The members of this group threatened targets by indicating that failure to pay would result in the personal information being posted online in hacking forums or public forums or leaked to journalists, which would harm the reputation of the company or organization to which the data belonged. One of the members of the TDO group, known as Dark Overlord, was arrested for and pleaded guilty to conspiracy to commit aggravated identity theft and computer fraud and was sentenced to five years' imprisonment.[202] Other members of the group remain at large.

(a) Sexual extortion

Sexual extortion (or sextortion) occurs when an individual threatens to share or otherwise distribute personal information or intimate images or videos if the target does not provide the offender with other images or videos of a sexual nature, engage in sexual acts in view of the perpetrator online or provide the perpetrator with money or other goods. Both adults and children can be the targets of sextortion. Where sextortion is not explicitly proscribed by law, depending on the specifics of the crime, elements of sextortion are considered criminal according to existing statutes that relate to extortion, image-based sexual abuse,[203] harassment and child sexual abuse, among other crimes.

[200] See UNODC, Education for Justice, University Module Series, Cybercrime, Module 12: Interpersonal cybercrime. Available at **www.unodc.org/**.

[201] United States District Court, Eastern District of Missouri, *United States of America v. Nathan Wyatt*, Case No. 4:17CR00522 RLW/SPM, Indictment, 8 November 2017.

[202] United States Department of Justice, Office of Public Affairs, "UK national sentenced to prison for role in 'The Dark Overlord' hacking group", press release, 21 September 2020.

[203] Image-based sexual abuse is defined in academic literature as the "non-consensual creation, distribution and threat to distribute nude or sexual images" (Nicola Henry, Asher Flynn and Anastasia Powell, "Policing image-based sexual abuse: stakeholder perspectives", *Police Practice and Research: An International Journal*, vol. 19, No. 6 (September 2018), pp. 565–581).

Rajesh and others v. State of Rajasthan, Division Bench Appeal No. 178, 122 and 123 / 2016 (India)

The case *Rajesh and others v. State of Rajasthan* involved the rape and sextortion of a 17-year-old female. When the victim was walking home from school, the three defendants asked her to board their vehicle. When the victim refused, they forcibly kidnapped her and covered the rear window of the vehicle with a curtain. The defendants stuffed the victim's mouth, and she was forcibly removed from the vehicle and dragged into a jungle where she was stripped and raped by the defendants. She was subsequently driven back to her village. The defendants made a video recording of the rape on a mobile phone and threatened to circulate the recording and share it with her relatives if she disclosed the rape to anyone. The victim did not talk about the incident out of fear that doing so would damage her reputation and that it might lead to her engagement being broken off. She felt so intimidated by the threats of the defendants that she stopped going to school and was under immense mental stress.

The defendants also attempted to blackmail her into performing further sexual acts by threatening to make available online the video recording of her rape if she did not agree to their demands. This sextortion continued for more than one year after the rape occurred. When the victim refused to agree to her sexual exploitation, the defendants uploaded the video recording on the Internet. The recording was seen by one of the victim's relatives, who brought it to her father's attention. Thereafter, the victim lodged a written complaint to the court. The court convicted the three defendants of rape,[a] violation of privacy,[b] publishing or transmitting obscene material in electronic form,[c] publishing or transmitting material containing a sexually explicit act in electronic form,[d] publishing or transmitting material depicting children in a sexually explicit act in electronic form,[e] kidnapping, abducting or inducing a woman to compel her marriage,[f] procuration of a minor girl,[g] kidnapping or abducting in order to subject a person to grievous harm, slavery,[h] distribution of obscene material[i] and criminal conspiracy.[j] The three defendants were sentenced to life imprisonment. On appeal, their sentences were reduced to 10 years of imprisonment. The defendants were also required to pay a fine of 392,000 rupees.

For more information about this case, see UNODC, SHERLOC case law database, Case No. INDx032.[k]

[a] R. was convicted pursuant to section 376, clause (g), of the Indian Penal Code of 1860; S.S. and D. were convicted pursuant to section 376, subsection (2), clause (g), of the Indian Penal Code.
[b] Section 66E of the Information Technology Act, 2000, of India.
[c] Section 67 of the Information Technology Act.
[d] Section 67A of the Information Technology Act.
[e] Section 67B of the Information Technology Act.
[f] Section 366 of the Indian Penal Code.
[g] Section 366A of the Indian Penal Code.
[h] Section 367 of the Indian Penal Code.
[i] Section 292 of the Indian Penal Code.
[j] Section 120B of the Indian Penal Code.
[k] Available at https://sherloc.unodc.org/.

A common tactic of perpetrators of sextortion is the utilization of fake profiles online to target the victims, using various websites, forums, chat rooms, social media platforms and messaging applications. The perpetrators ultimately seek to coerce their targets into performing sexual acts via webcam and/or to create and/or distribute sexual images or video recordings. The images or recordings are then used to threaten the victim. The perpetrator threatens to reveal the images or recordings to the victim's family, friends, significant others, employers, colleagues, classmates and/or others if the victim does not provide more sexualized media content, pay the perpetrator and/or engage in some other act desired by the perpetrator.

United States of America v. Antwine Lamar Matthews, Malcolm Cooper, Andreika Mouzon and Flossie Brockington, United States of America v. Jimmy Dunbar, Jr. and Mitchlene Padgett, United States of America v. Rakeem Spivey and Roselyn Pratt, United States of America v. David Paul Dempsey and Edgar Jermaine Hosey, United States of America v. Wendell Wilkins, Jalisa Thompson, Tiffany Reed, Brandon Thompson and Laben McCoy (D. South Carolina, 14 November 2018) (United States of America)

Sexual extortion scheme run from prison

In the United States, inmates in the South Carolina Department of Corrections, using smartphones they had smuggled into the prison, perpetrated a sextortion scheme targeting United States military personnel.[a] The inmates would sign up for dating applications and target members of the military utilizing the applications. The inmates would create fake profiles of women for whom they had found both nude and non-nude images online. The fake profiles would be created using the non-nude images. After contacting the targets and obtaining personal information from them, the inmates would send the nude images and request that the targets share nude images of themselves.[b] The inmates would then call the targets and, impersonating the father of the woman with whom the targets were in contact, claim that the targets had been communicating with a minor and therefore the nude images the targets had received were nude images of a minor. The inmates would then threaten to contact the authorities and report the targets if money was not paid to the "victim" (for example, to enable medical bills or fees to be paid).[c] In some cases, inmates would contact the targets and, impersonating a police officer, threaten to arrest them if money was not paid to the "victim". The targets were directed to pay the fees via wire transfers, using, for example, a well-known money transfer service.[d] The inmates recruited "money mules", who would receive the wire transfers from the members of the military and then send the funds to the inmates as directed.

The defendants were charged with conspiracy to commit wire fraud, extortion and money-laundering. Several of the defendants pleaded guilty to one or more of these crimes. T.R. pleaded guilty and was sentenced to three years' probation for conspiracy to commit wire fraud.[e] Another defendant, W.W., also pleaded guilty to conspiracy to commit wire fraud, but has not been sentenced yet.[f] Another defendant, A.M., pleaded guilty to conspiracy to commit wire fraud and money-laundering,[g] while other defendants, J.T., B.T., and F.B., pleaded guilty to money-laundering.[h] J.T. and B.T. each received time served and 15 months' imprisonment for their crimes. D.P.D pleaded guilty to all three charges and was sentenced to 3 years and 10 months of imprisonment. The prosecution also submitted a motion to dismiss the indictment against one of the defendants, L.M.[i]

For more information on this, see UNODC, SHERLOC case law database, Case No. USAx172.[j]

[a] United States Attorney's Office, District of South Carolina, "5 inmates among 15 defendants indicted for wire fraud, extortion, and money laundering scheme at SCDC", press release, 29 November 2018.

[b] United States District Court, District of South Carolina, *United States of America v. Antwine Lamar Matthews, Malcolm Cooper, Andreika Mouzon and Flossie Brockington*, Case No: 2:18-CR-1024, Indictment, 14 November 2018, pp. 2–3.

[c] Ibid.; United States District Court, District of South Carolina, *United States of America v. Jimmy Dunbar, Jr. and Mitchlene Padgett*, p. 3; *United States of America v. Rakeem Spivey and Roselyn Pratt*, p. 3; United States District Court, District of South Carolina, *United States of America v. David Paul Dempsey and Edgar Jermaine Hosey*, Case No. 2:18-CR-1022, Indictment, 14 November 2018, pp. 2–3; United States District Court, District of South Carolina, *United States of America v. Wendell Wilkins, Jalisa Thompson, Tiffany Reed, Brandon Thompson and Laben McCoy*, Case No. 2-18-CR-101, Indictment, 14 November 2018, p. 2.

[d] *United States of America v. Jimmy Dunbar, Jr. and Mitchlene Padgett*, p. 3; *United States of America v. Rakeem Spivey and Roselyn Pratt*, p. 3.

[e] For further information, see United States District Court, District of South Carolina, *United States of America v. Tiffany Reed*, Case No. 2:18-CR-1017-DCN, 4 May 2020; *United States of America v. Brandon Thompson*, Judgement, 20 December 2019.

[f] For further information, see *United States of America v. Wendell Bernard Wilkins*, Case No. 2:18-cr-01017-DCN-1, Plea, 2 December 2019.

[g] For further information, see United States Attorney's Office, District of South Carolina, "Two money mules plead guilty in Federal Court for role in sextortion scheme", press release, 31 July 2019.

[h] For further information, see United States District Court, District of South Carolina, *United States of America v. Jalisa Thompson*, Sentencing Memorandum in Support of Downward Departure and or Defendant, Case No. 2:18-CR-01017-002, 2 December 2019; United States Attorney's Office, District of South Carolina, "Two money mules plead guilty in Federal Court".

[i] For further information, see United States District Court, District of South Carolina, *United States of America v. Laben Weykshaw Renee McCoy*, Case No. 2:18-CR-1017-5, Motion to Dismiss Indictment, 15 September 2020.

[j] Available at **https://sherloc.unodc.org/**.

(b) Ransom scams

There are many variations of scams that seek ransom from targets. Perpetrators of ransom scams seek to frighten their targets into paying a ransom by claiming that they have access to some of the targets' personal data (e.g., login credentials) or have access to the targets' devices and have recorded compromising information about the targets, which they threaten to release if a ransom is not paid. The money for ransom scams can be paid in person (to accomplices of the perpetrators), using online payment services, prepaid debit and credit cards and digital currencies (e.g., cryptocurrencies).

Ransom scams may also involve offenders pretending to represent banks, creditors, lawyers, law enforcement agencies or other government agencies demanding that outstanding debts or other matters be dealt with expeditiously through payment of a fine or other fee. A Peruvian call centre was used to carry out fraud and extortion schemes via Internet-based telephone calls.[204] The defendants, who managed and operated Peruvian call centres, utilized Internet-based telephone calls to threaten targets with arrest, deportation, negative impact on their credit rating and/or seizure of property if the targets did not pay a fee.[205] The defendants targeted Spanish-speaking individuals residing in the United States. The defendants, who posed as attorneys and government representatives, would claim that the targets owed thousands of dollars in fines because they had failed to accept the delivery of specific products.[206] The defendants would also claim that failure to pay a so-called settlement fee to resolve the matter would result in some form of harm to the target (e.g., bad credit rating, lawsuit, arrest and deportation).[207]

Ransom scams may also involve calling targets and pretending to have arrested or otherwise detained one of their relatives and demanding money for their release. An example of this type of scam is a virtual kidnapping scheme, whereby perpetrators contact a target claiming that they have the target's child (or relative or significant other) and threaten to kill or seriously harm the "kidnapped" person[208] unless a ransom is paid (see the box below).

Tribunal de Enjuiciamiento del Distrito Judicial Morelos – número de juicio 38/2020 (Mexico)

On 6 February 2018, Victim 1 received a call on his mobile phone from a man who initially identified himself as the commander of the prosecutor's office and later as a member of an organized criminal group. By means of threats and intimidation, the perpetrator forced Victim 1 to change the subscriber identification module (SIM) card of his mobile phone, go to a local motel and stay there for four days. During this period, Victim 1 was instructed to take photographs of himself naked, simulate a victim of kidnapping and send the images to the extortionist.

Between 6 and 9 February 2018, Victim 2 received various telephone calls from different numbers, including calls from Victim 1's number via a well-known messaging application that uses the Internet. The callers sent images of Victim 1 (simulated images designed to make Victim 1 appear to be a victim of kidnapping) to Victim 2 via the messaging app and threatened to kill Victim 1. Using threats and intimidation, the extortionists persuaded Victim 2 to deposit 2,148,160 Mexican pesos in various bank accounts, including one under the accused person's name. Victim 2 reported the extortion to the local police, who managed to locate Victim 1 on 9 February 2018.

[204] United States District Court, Southern District of Florida, *United States of America v. Hidalgo Marchan*, Case No. 1:15-CR-20471, 23 June 2015.

[205] United States Department of Justice, Office of Public Affairs, "Three men extradited for overseeing call centers that threatened and defrauded Spanish-speaking U.S. consumers", press release, 19 December 2019.

[206] United States Department of Justice, Office of Public Affairs, "Peruvian man pleads guilty to overseeing call centers that threatened and defrauded Spanish-speaking U.S. consumer", 1 May 2020.

[207] Ibid.; United States Department of Justice, Office of Public Affairs, "Three men extradited for overseeing call centers".

[208] The person may or may not be kidnapped (or otherwise held) by the perpetrators of this crime.

A person incarcerated in a federal prison in the city of Tamaulipas was identified as the leader of the organized criminal group. He led and coordinated the virtual kidnapping operation from prison. The prosecutor's office had information about the modus operandi of the criminal group because the mobile phone number of one of the extortionists in this case had been linked to complaints filed by victims in 15 similar cases.

Deposits of money stemming from the proceeds of this cyber-enabled crime had been made in the United States through certain companies where other members of the criminal group went to collect the money. Video recordings of these transactions were gathered, enabling other members of the group to be identified. A chronological series of images were also obtained from video recordings from the different offices where the money deposits were withdrawn.

In this case, investigative and prosecutorial challenges were highlighted. The defence argued that some of the evidence presented in court had been obtained illegally. For example, authorization from a federal judge had not been obtained before extracting data from seized devices, in contravention of article 16 of the Constitution. There were also inconsistencies and missing information in the chain of custody for some of the evidence introduced in court.

Ten members of the criminal group were captured and nine members were sentenced to 22 years and 6 months of imprisonment. The defendants who were sentenced for their crimes were also required to pay restitution[a] to Victim 2 (Mex$ 37,800 for psychological therapy and Mex$ 2,148,160, the exact amount the sent by Victim 2 to the criminal group) and to Victim 1 (Mex$ 40,500 for psychological therapy).

For more information about this case, see UNODC, SHERLOC case law database, Case No. MEXx004.[b]

[a] This restitution was made in in accordance with article 20, section B, of the Political Constitution of the United Mexican States, as well as articles 43–51 of the Penal Code for the State of Chihuahua.
[b] Available at https://sherloc.unodc.org/.

(c) Ransomware

Ransomware is a form of malware that infects a user's device and posts a warning on the device that, if the victim does not make a payment, there will be some negative consequence to the owner of the device. This type of malware may also be designed to block access to data, files and/or systems; the access is to be restored when a sum of money (i.e., ransom) is paid. One form of ransomware is crypto-ransomware, a Trojan Horse designed to encrypt data on a victim's system and extort money from the victim to release information.[209]

In its report *Internet Organised Crime Threat Assessment 2020*, Europol noted that ransomware remains a significant threat both within and outside of Europe.[210] Individuals, businesses, non-governmental organizations and government agencies are targeted by ransomware. Ransomware is largely an underreported crime, particularly when it involves the private sector, which may fear the negative effects of reporting this cybercrime (e.g., reputational harm, exposure to further cybervictimization by other perpetrators).[211] Ransomware has evolved from targeting individual users of ICT to becoming more targeted and focusing on public and private organizations.[212] Initially, crypto-ransomware threatened to permanently prevent targets from accessing files, data and/or their systems unless payment was rendered. However, cybercriminals have deployed crypto-ransomware, which threatens to wipe data from devices and/or auction data online if

[209] Maras, *Cybercriminology*, p. 334.
[210] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 25.
[211] Ibid., p. 28.
[212] Ibid., p. 25.

money is not paid.[213] When criminals threaten to release personal data online unless payment is made, this is a form of "doxxing".

6. Child sexual abuse and child sexual exploitation

Online child sexual abuse and online child sexual exploitation involve the use of ICT to facilitate the sexual abuse and the sexual exploitation of children.[214] There is considerable overlap between child sexual abuse and child sexual exploitation.[215] Child sexual abuse refers to contact or interaction between a child and an older or more knowledgeable child or adult (a stranger, sibling or person in a position of authority such as a parent or caretaker) when the child is being used as an object for the older child's or adult's sexual needs.[216] Child sexual exploitation encompasses child sexual abuse, as well as other sexualized acts aimed at and/or performed by a child.[217] Online child sexual abuse and child sexual exploitation are prohibited by national, regional and international laws.[218] The manner in which online child sexual abuse and child sexual exploitation are criminalized by law, however, varies.

Three types of offences involving child sexual abuse and child sexual exploitation are covered in the sub-sections that follow: child sexual abuse material and child sexual exploitation material, the enticement or solicitation of children to engage in sex acts (i.e., child grooming) and live-streaming child sexual abuse.

(a) Child sexual abuse material and child sexual exploitation material

The term "child pornography" has been rejected by civil society, law enforcement agencies, academics and others because it minimizes what is actually occurring - child sexual abuse and not sex with a child.[219] The preferred term is "child sexual abuse material". While child sexual abuse material depicts child sexual abuse, all other sexualized material depicting children is considered "child sexual exploitation material".[220] Nevertheless, the term "child pornography" still exists in national, regional and international laws.

Laws criminalizing the possession, production and distribution of child sexual abuse material and child sexual exploitation material vary by jurisdiction. Some jurisdictions do not proscribe computer-generated child sexual abuse material, which refers to the production, through digital media, of child sexual abuse material and other wholly or partly artificially or digitally created sexualized images of children; they proscribe only images depicting real children.[221] In some countries, possession of child sexual abuse material is criminalized if there is an intent to distribute the material.[222] In those countries, the possession of the material alone would not be considered criminal.

Child sexual abuse material and child sexual exploitation material are created, shared and distributed via websites, Internet newsgroups, web-conferencing software, social media platforms, unencrypted and

---

[213] Ibid., p. 26.

[214] Susanna Greijer and Jaap Doek, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, adopted by the Interagency Working Group in Luxembourg, 28 January 2016 (Luxembourg, ECPAT International and ECPAT Luxembourg, 2016), pp. 23 and 28.

[215] Ibid., p. 25.

[216] UNICEF, "Building knowledge and awareness: sexual violence", Communities Care: Transforming Lives and Preventing Violence Programme (New York, 2014).

[217] UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (Vienna, 2015).

[218] See, for example, the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (also known as the Lanzarote Convention), the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, of Nigeria (sect. 23); **directive 2011/93/EU** of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, replacing Council framework decision **2004/68/JHA** of 22 December 2003 on combating the sexual exploitation of children and child pornography; article 27 of the African Charter on the Rights and Welfare of the Child; and Republic Act No. 9775 of the Philippines (known as the Anti-Child Pornography Act of 2009).

[219] For more information, see UNODC, Education for Justice University Module Series, Cybercrime, Module 2: General types of cybercrime, "Computer-related offences" Module 12: Interpersonal cybercrime, "Online child sexual exploitation and abuse". Available at **www.unodc.org/**.

[220] Greijer and Doek, *Terminology Guidelines for the Protection of Children*, pp. 39–40.

[221] Ibid., p. 40; and UNODC, Education for Justice, University Module Series, Cybercrime, Module 12: Interpersonal cybercrime, "Online child sexual exploitation and abuse".

[222] International Centre for Missing and Exploited Children, *Child Pornography*, pp. 18–42.

encrypted communication applications and other online platforms.[223] This material is also shared using text messages, instant messaging, email messages, chat rooms, bulletin boards and peer-to-peer file-sharing networks.[224]

Perpetrators of online child sexual abuse and child sexual exploitation can be part of large online communities[225] or smaller communities where child sexual abuse material is sent directly between perpetrators using various applications, such as encrypted messaging platforms.[226] The online communities of child sex offenders are tightly controlled with platform affiliation rules and codes of conduct.[227] Rules are enforced by moderators and administrators of the site, and members of the site must follow the official affiliation rules and codes of conduct in order to remain active members on the site.[228] Within these forums, individuals are often promoted based on their contributions on the site and/or rewarded for their contributions. Active participation in the forums builds a person's reputation and can increase a person's position, standing and/or rank within the community. Active participation in these forums is associated with the advertisement, posting, distribution or otherwise making available of child sexual abuse material and child sexual exploitation material. To maintain access to the sites and/or to gain access to more child sexual abuse and child sexual exploitation material on the site, members have to continuously post such material. Failure to contribute to the site would lead to a revocation of privileges and removal from the site. Some child sexual abuse and child sexual exploitation sites (e.g., Dreamboard and the Giftbox Exchange) also require new members to post child sexual abuse material during registration for verification purposes,[229] whereas other sites (e.g., Elysium) did not have these requirements.[230]

Ogranized criminal groups predominantly follow profit-driven models that are characteristic of legitimate and illegitimate organizations. Europol, in its report *Internet Organised Crime Threat Assessment 2020*, identified a trend in the commercialization of child sexual abuse material and child sexual exploitation material:[231] the monetization of such material on the clearnet and the darknet.[232] Individuals receive credit based on the number of downloads of the content they upload to the site and get paid via cryptocurrencies or other forms of payment.[233] An example of this is the case in the Republic of Korea involving the website Welcome to Video (see chap. IV), whereby bitcoin was used to monetize child sexual exploitation material.[234]

---

[223] Maras, *Cybercriminology*; Australia, *R v. Mara* [2009] QCA 208 (Internet newsgroups); Canada, Provincial Court of Saskatchewan, *R v. Philip Michael Chicoine*, 2017 SKPC 87 (Communication applications); and United States Court of Appeals, Third District, *United States of America v. Dylan Heatherly*, Case No. 19-2424 (2020) and *United States of America v. William Staples*, No. 19-2932 (2020) (Web-conferencing software).

[224] See, for example, *R v. Philip Michael Chicoine*, 2017 SKPC 87 (Peer-to-peer sharing platforms); Germany, Federal Court of Justice, Decision 2 StR 321/19 of 15 January 2020 (BGH, Beschluss vom 15.01.2020, 2 StR 321/19); *United States of America v. Caleb Young* (Chat rooms); and United States District Court, Western District of North Carolina, *United States of America v. Steven W. Chase*, Case No. 5:15-CR00015-001, 8 May 2017 (Bulletin board).

[225] See, for example, *United States of America v. John Doe #1, Edward Odewaldt et al*. (Dreamboard); Germany, Federal Court of Justice, Decision 2 StR 321/19 of 15 January 2020 (BGH, Beschluss vom 15.01.2020, 2 StR 321/19); Europol, *Internet Organised Crime Threat Assessment 2020*, p. 38.

[226] See, for example, *United States of America v. Caleb Young*, p. 3 (the Bored group); see also Europol, *Internet Organised Crime Threat Assessment 2020*, p. 37.

[227] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 38.

[228] Ibid.

[229] *United States of America v. John Doe #1, Edward Odewaldt et al*. (Dreamboard); Germany, Federal Court of Justice, Decision 2 StR 321/19 of 15 January 2020 (BGH, Beschluss vom 15.01.2020, 2 StR 321/19) (the Giftbox Exchange); see also Maras, *Cybercriminology*, chap. 10.

[230] Germany, Federal Court of Justice, Decision 2 StR 321/19 of 15 January 2020 (Elysium) (BGH, Beschluss vom 15.01.2020, 2 StR 321/19); see also Maras, *Cybercriminology*, chap. 10.

[231] Ibid.

[232] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 40; see also, Costa Rica, Tribunal Penal del Tercer Circuito Judicial de San José, Causa penal No.15-001824-0057-PE & Causa Penal No. 19-000031-0532-PE (Operación R-INO); Argentina, Tribunal Oral Federal de Jujuy, Causa FSA 8398/2014/TO1; and Republic of Korea, Seoul Central District Court (Criminal Department I-I), 2018NO2855, 2 May 2019.

[233] Ibid.

[234] Republic of Korea, Seoul Central District Court (Criminal Department I-I), 2018NO2855, 2 May 2019.

R v. Philip Michael Chicoine [2017] S.J. No. 557, 2017 SKPC 87 (Canada)

The defendant, P.M.C., lured children to commit sexual assault and produce child sexual abuse material, had in his possession child sexual abuse material (over 4,132 unique images and 582 videos of child sexual abuse) and created, accessed, shared and/or otherwise distributed child sexual abuse material online, using a well-known communication application, a well-known messaging application, instant messaging service applications and peer-to-peer file-sharing platforms.[a] The defendant used a communication application to communicate with child sex offenders located in the Philippines and Romania and paid those individuals to sexually abuse female children 4–9 years old, directing the offenders as to what specific type of sexual abuse he wanted to see. The child sexual abuse material was either pre-recorded or live-streamed.[b] The defendant also directly communicated with children through an instant messaging service and sexually exploited them, sending them sexualized and graphic images, including images of his penis, offering them money in exchange for images of their vaginas and directing the child victims to give the defendant's messaging service account to other young girls. The exact number of the defendant's victims is not known. The defendant pleaded guilty to over 40 offences involving child sexual abuse and child sexual exploitation, including conspiracy charges relating to creating child sexual abuse material. He was sentenced to 12 years' imprisonment for his offences and was required to register as a sex offender for life (pursuant to the Sex Offender Information Registration Act of Canada). The defendant was also prohibited from using the Internet or any other digital network to access content that violates the law, to communicate with a minor, to directly or indirectly access any social media sites, social networks, Internet discussion forums or chat rooms or to maintain a personal profile on any such service.[c] Furthermore, he was required to pay a "victim fine surcharge" of 200 Canadian dollars for each of the 40 counts to which he had pleaded guilty, for a total of $Can 8,000.[d]

For more information on this case, see UNODC, SHERLOC case law database, Case No. CANx138.[e]

[a] *R v. Philip Michael Chicoine* [2017] S.J. No. 557, 2017 SKPC 87, para. 11.
[b] For further information about live-streaming child sexual abuse, see chap. V, sect. B.6, below.
[c] *R v. Philip Michael Chicoine* [2017] 2017 SKPC 87, para. 67 (d) (iii).
[d] Ibid., para. 68.
[e] Available at https://sherloc.unodc.org/.

(b) Child grooming

Child grooming can be described as the means by which an adult "befriends" a child with the intention of sexually abusing the child.[235] Child grooming can occur both online and offline. Research shows that girls are predominantly the victims of this crime, whereas males are predominantly the perpetrators of this crime.[236]

[235] Greijer and Doek, *Terminology Guidelines for the Protection of Children*, p. 49.

[236] Alessia Altamura, "Online child sexual abuse and exploitation: spotlight on female sex offenders", *ECPAT International Journal: Online Child Sexual Exploitation–An Analysis of Emerging and Selected Issues*, No. 12 (2017), pp. 26–46.

The term "grooming" is not commonly found in law;[237] what is found are terms such as "luring", "enticement", "solicitation" and "seduction".[238] Some laws criminalize online grooming if it can be shown that the offender intended to meet the child in person,[239] while other laws do not have this requirement.[240]

The grooming process varies. Essential elements, however, are: victim selection, which is based on the appeal, ease of access and vulnerability of the victim; victim contact; rapport-building and forming a friendship between the offender and the victim; and the sexual abuse or sexual exploitation of the victim (e.g., the coercion or manipulation of the victim into producing child sexual abuse or child sexual exploitation material).[241]

United States of America v. Caleb Young, Case No. 18-20128 (E.D. Michigan, 11 May 2018) (the Bored Group) (United States of America)

An international child sexual exploitation ring, the Bored group,[a] met, organized their activities and operated exclusively online. Initially, the group met on a social media platform that was popular for live-streaming video chats.[b] Frustrated with the moderating that existed on that site, they migrated to other sites and ultimately ended up using one unidentified site that was not moderated.[c] The chat rooms created on this site could not be found unless a person knew the uniform resource locator (URL) of the chat room.

The perpetrators devised and executed a plan to lure targets from moderated platforms to an unmoderated chat room and convince them to engage in sex acts. Specifically, the members of the group worked together to recruit, entice and coerce minors to engage in sex acts during video chat sessions. To accomplish this, members of the group created fake profiles of teenage boys on social media and dating sites to target underage girls.[d] The members would then identify minors to target, contact and communicate with in order to get the victims to join the offenders in the unmonitored chat room. All of the members of the group spent a considerable amount of time communicating with their targets in order to gain their trust, build rapport and, ultimately, entice the victims into commiting sex acts.[e]

Members of the Bored group used several techniques to manipulate victims, including:[f]

(a) *Dares*. A group member would dare the victim to engage in sexualized behaviour and sex acts;

(b) *Polls*. Running polls would be conducted with participants in the chat room about the attractiveness of minors and/or the participants would vote on what type of items of clothing the minor should remove and/or what type of sex act the minor should engage in;

[237] There are exceptions, such as section 131B of the Crimes Act 1961 of New Zealand, which is entitled "Meeting young person following sexual grooming, etc."; section 15 of the Sexual Offences Act 2003 of the United Kingdom; the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse; and directive 2011/93/EU replacing Council framework decision 2004/68/JHA.

[238] See Costa Rica, Penal Code, art. 167 bis (Seduction or encounters with minors through electronic means); Antigua and Barbuda, Electronic Crimes Act, art. 10 (Entice); Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, art. 23 (Solicitation of children for sexual purposes); and directive 2011/93/EU. Germany uses the word "influences" (see the German Criminal Code (Strafgesetzbuch), sect. 176 (Sexual abuse of children)).

[239] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse; directive 2011/93/EU; section 15 of the Sexual Offences Act 2003 of the United Kingdom.

[240] For more information about the countries that have these laws, see International Centre for Missing and Exploited Children, *Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review* (2017), p. 7.

[241] Kenneth V. Lanning, *Child Molesters: A Behavioral Analysis for Professional Investigating the Sexual Exploitation of Children*, (Alexandria, Virginia, National Center for Missing and Exploited Children, 2010; Georgia M. Winters and Elizabeth L. Jeglic, "Stages of sexual grooming: recognizing potentially predatory behaviors of child molesters", *Deviant Behavior*, vol. 38, No. 6 (2017), pp. 724–733; Rachel O'Connell, "A typology of cybersexploitation and online grooming practices (Preston, United Kingdom, University of Central Lancashire, Cyberspace Research Unit, 2003); Susan Aitken, Danielle Gaskell and Alan Hodkinson, "Online sexual grooming: exploratory comparison of themes arising from male offenders' communications with male victims compared to female victims", *Deviant Behavior*, vol. 39, No. 9 (February 2018), pp. 1170–1190.

United States of America v. Caleb Young, Case No. 18-20128 (E.D. Michigan, 11 May 2018) (the Bored Group) (United States of America) (*continued*)

(c) *Competitions*. Minors would be pitted against each other in an effort to be rewarded (i.e., they would receive points for engaging in certain sexualized behaviour and sex acts and would advance to higher levels based on points);

(d) *Purporting to block webcams*. To reduce the inhibitions of minors, a group member whom the victim trusted (called a "handler") would claim that he could block the victim's webcam and prevent other participants in the chat room from viewing the victim. When the handler told the other participants that this tactic was being used, they would pretend that they were unable to see anything via the victim's webcam;

(e) *Loops*. Pre-recorded videos of other minors talking and/or engaging in sexualized behaviour or sex acts were played as if they were occurring in real time in order to manipulate the minor into engaging in similar conduct and/or acts.

Members of the Bored group had distinct roles: "hunters", "talkers" and "loopers".[g] "Hunters" would lure victims to the chat room.[h] Once the victims had joined the chat room, "talkers" would attempt to convince them to undress and masturbate on camera by engaging them in conversation and building trust and rapport.[i] "Loopers" would pose as female minors and play a pre-recorded video of another minor talking or engaging in sex acts, which the "loopers" would seek to pass off as an event happening in real time.[j] The "loopers" would play the pre-recorded videos in an effort to convince the girls to perform a sex act.

One method used to monitor, evaluate and coordinate their activities, track progress and share their knowledge and expertise was to discuss their plans, activities and experiences on a separate site (the now defunct TitanPad) and record their activities and experiences on a password-protected spreadsheet on that site that included information about which chat rooms on the website were associated with which victims and the social media accounts associated with members that were used to lure each of the victims.[k] The spreadsheet also enabled the members of the group to keep track of the manipulation techniques that had been successful with each victim and what sex acts each victim had engaged in (the sex acts included extremely depraved acts; for example, one member of the group had enticed a minor to engage in a sex act with a dog).[l] After TitanPad ceased its operation in 2017, the Bored group moved its activities to Discord, a group chat platform with voice and video capabilities.[m]

The defendant (C.Y.) pleaded guilty to engaging in a child exploitation enterprise[n] and received a sentence of 30 years' imprisonment for that offence.[o] C.M., the leader of the child exploitation enterprise, received a sentence of 40 years' imprisonment.[p] He was killed in prison during an altercation with other inmates in January 2019.[q] Other members of the group received sentences of 38 years (A.S.), 37 years and 6 months (O.O.), 35 years (J.N.R.), 31 years and 3 months (M.F.) and 30 years and 6 months of imprisonment (B.J.S. and D.W.).[r] All of the members of the group were ordered to pay each identified victim restitution (US$ 5,000).[s]

For more information on this case, see UNODC, SHERLOC case law database, Case No. USAx173.[t]

[a] The Bored group earned this nickname because the chat rooms they created all included the word "bored" in them.
[b] *United States of America v. Caleb Young*, p. 3.
[c] Ibid.
[d] Ibid., p. 5.
[e] Ibid., pp. 7 and 13–16.
[f] Ibid., pp. 7–9.
[g] *United States of America v. Caleb Young*, Affidavit in support of application for complaint and arrest warrant, p. 6.
[h] Ibid.
[i] *United States of America v. Caleb Young*, Sentencing Memorandum, p. 7.
[j] *United States of America v. Caleb Young*, Plea Agreement, p. 6.
[k] *United States of America v. Caleb Young*, Affidavit in support of application for complaint and arrest warrant, pp. 6–7.

[l] *United States of America v. Caleb Young*, Sentencing Memorandum, pp. 10–11.
[m] Ibid., p. 12.
[n] United States Code, Title 18, sect. 2252A (g).
[o] *United States of America v. Caleb Young*, Plea Agreement; United States Attorney's Office, Eastern District of Michigan, "Eight men sentenced for their roles in an international child pornography production ring", press release, 6 December 2018.
[p] Ibid.
[q] Associated Press, "Child porn leader dies after fight at detention center", 4 January 2019.
[r] United States Attorney's Office, Eastern District of Michigan, "Eight men sentenced".
[s] Ibid.
[t] Available at https://sherloc.unodc.org/.

(c) Live-streaming child sexual abuse

Live-streaming child sexual abuse involves the broadcasting of child sexual abuse in real time.[242] Participants in the live-stream can be passive or active viewers. Passive viewers pay to watch, while active viewers pay to play a role in the child sexual abuse by communicating what sexual acts they want to see performed by the abusers, the child and/or the child's handlers (active viewers enage in what is known as "child sexual abuse to order").[243] In Canada, in *R v. Pitts*,[244] the defendant (J.T.P.), with other unidentified individuals, engaged in live-streaming child sexual abuse, whereby children in the Philippines were sexually exploited and abused. Specifically, during the live sessions, the defendant made the children perform specific sex acts on adult females and/or other children.[245] The defendant pleaded guilty to offences relating to possessing, accessing and making child sexual abuse material and to conspiring to commit the indictable offence of sexual assault on a child and was subsequently sentenced to five years' imprisonment.[246] He unsuccessfully appealed his sentence, claiming that it was excessive.

Live-streaming child sexual abuse is prohibited by law.[247] However, the criminalization of this act varies by country. Active participants in live-streaming child sexual abuse could be charged with laws criminalizing the production of child sexual abuse material.[248] Passive participants in live-streaming child sexual abuse could also be charged, although this depends on national laws. Passive and active participants in live-streaming child sexual abuse can be charged with the possession of child sexual abuse material if they have in their possession a recording of the session and/or pictures that were taken during the live-stream.[249] Nevertheless, the child sexual abuse that is live-streamed may not be recorded by participants, abusers and/or child handers in an effort to evade detection by law enforcement authorities and make it more difficult for them to be prosecuted for this cybercrime. However, even in these cases, the financial transactions between participants and abusers in live-streaming child sexual abuse (e.g., online payment services, money transfers and payments using digital currencies) can be used to detect this cybercrime and can be used in court as evidence of this

[242] For more information, see UNODC, Education for Justice University Module Series, Cybercrime, Module 2: General types of cybercrime, "Computer-related offences" and Module 12: Interpersonal cybercrime, "Online child sexual exploitation and abuse".

[243] UNODC, *Study on the Effects of New Information*; Greijer and Doek, *Terminology Guidelines for the Protection of Children*, p. 47.

[244] Canada, Nova Scotia Court of Appeal, *R v. Pitts*, 2016 NSCA 78.

[245] Ibid., para. 10.

[246] Ibid., paras. 1 and 18.

[247] In article 2, paragraph (e), of directive 2011/93/EU, "pornographic performance" is defined as a live exhibition aimed at an audience, including by means of ICT, of: a child engaged in real or simulated sexually explicit conduct; or the sexual organs of a child for primarily sexual purposes. In article 21, paragraph 1, of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, parties to the Convention are required to criminalize: (a) recruiting a child into participating in pornographic performances or causing a child to participate in such performances; (b) coercing a child into participating in pornographic performances or profiting from or otherwise exploiting a child for such purposes; and (c) knowingly attending pornographic performances involving the participation of children. Section 4 of the Anti-Child Pornography Act of 2009 of the Philippines states that it shall be unlawful for any person: (a) to hire, employ, use, persuade, induce or coerce a child to perform in the creation or production of any form of child pornography; (b) to produce, direct, manufacture or create any form of child pornography; and (c) to publish offer, transmit, sell, distribute, broadcast, advertise, promote, export or import any form of child pornography.

[248] Greijer and Doek, *Terminology Guidelines for the Protection of Children*, p. 46.

[249] Ibid.

cybercrime.[250] A case in point involved Xoom.com, an online money transfer service. It reported to a well-known messaging service provider that certain users of their services were engaging in child sexual abuse by selling child sexual abuse material and live-streaming child sexual abuse. An investigation by the service provider identified multiple instances in which their account holders were believed to be buying and selling child sexual abuse material and participating in live-streaming child sexual abuse from the Philippines.[251] This case highlights an important facet of live-streaming child sexual abuse and child sexual abuse material. While such crimes are perpetrated primarily for the personal sexual gratification of the offenders, the offenders also have a financial motivation for the creation and distribution of child sexual abuse material.

United States of America v. Dylan Heatherly, No. 19-2424 (3d Circuit 2020) and *United States of America v. William Staples*, No. 19-2932 (3d Circuit 2020) (United States of America)

In Canada, an undercover investigation by a female law enforcement officer revealed that a well-known videoconferencing platform was being used as a chat room and live-streaming space for child sexual abuse material. The Canadian law enforcement officer reached out to her contacts in the Government of the United States to inform them of the illicit activity that had been observed. United States federal agents subsequently contacted the chief executive officer of the platform, who assisted them in their investigation of the illicit activity that had been observed on the platform. One outcome of the cooperation is the case described below, where two individuals were charged with and convicted for their roles in the use of the videoconferencing platform to facilitate child sexual abuse and exploitation.

The two defendants (W.S.) and (D.H.) used a videoconferencing platform as a chat room space where they virtually met with others to view, request, receive, distribute and otherwise facilitate the receipt and distribution of child sexual abuse material. Using the platform, pre-recorded child sexual abuse material was shared, as well as live-streaming child sexual abuse. One male user of the platform (A.) repeatedly live-streamed himself raping and sexually abusing his six-year-old nephew.[a] Other users of the platform, including the two defendants, encouraged A. to rape and sexually abuse his nephew. Other members of the session even directed A. to perpetrate specific types of child sexual abuse and sexual assault on the victim (a form of "child sexual abuse to order"). The defendants also requested child sexual abuse material from other users of the platform.

One of the defendants (W.S.) was found guilty of conspiracy to advertise, receive and/or distribute, and aid and abet the receipt and/or distribution of, child sexual abuse material.[b] The other defendant (D.H.) was found guilty of conspiracy to receive and/or distribute, and aid and abet the receipt and/or distribution of, child sexual abuse material.[c] For their crimes, D.H. and W.S. were sentenced to 25 and 30 years' imprisonment, respectively.[d]

The two defendants appealed their convictions and sentences for conspiracy charges relating to child sexual abuse material, claiming, among other things, that the evidence introduced in court against them was highly prejudicial. The defendants claimed that they were not interested in child sexual abuse material but wanted to watch other men masturbate on the platform. Child sexual abuse video recordings and chat logs of the platform sessions and the child sexual abuse material found on the defendants' devices had been introduced as evidence at trial to rebuke the defendants' claims that they were not aware and/or did not enter the chat room space for the purposes of child sexual abuse and exploitation.

[250] Andrea Varrella, "Live streaming of child sexual abuse: background, legislative frameworks and the experience of the Philippines", in *Online Child Sexual Exploitation: An Analysis of Emerging and Selected Issues*, *ECPAT International Journal*, No. 12 (2017), p. 49.

[251] United States District Court, Southern District of California, *United States of America v. Carsten Igor Rosenow*, Case No. 17-CR-3430, Motion to Suppress Evidence and Motion to Dismiss Indictment (2018), p. 3; United States Attorney's Office, Southern District of California, "San Diego man sentenced to 25 years in federal prison for child pornography offenses", press release, 2 March 2020.

The introduction of the child sexual abuse video recordings as evidence was a particular point of contention for the defendants. The introduction of the video recordings as evidence was viewed as necessary to prove conspiracy to engage in child sexual abuse and child sexual exploitation by showing that the chat room space had served as a "haven" where individuals gathered to discuss and share child sexual abuse material.[e] The United States Court of Appeals for the Third Circuit held that:

> The video clips helped to establish the culture that permeated the ... chats. That was an important part of proving that the participants were involved in such a unity of purpose and common undertaking that they had necessarily entered into an agreement that this type of material be received or distributed... The government's attempt to verbalize what the defendants were watching may well have been inadequate to communicate the nature of the ... chats or whether the unity of purpose between these defendants was such that it suggested an implicit agreement to participate in these live-streams, as opposed to "merely" separately observing them.[f]

The Court of Appeals ultimately ruled that risk of the prejudicial influence of this evidence on jurors was outweighed by the evidence being highly probative of the conspiracy and the defendants' awareness of what they were involved in.[g] The Court of Appeals found no error in the defendants' convictions and sentences and affirmed the lower court's decisions.

For more information on these cases, see UNODC, SHERLOC case law database, Case No. USAx174.[h]

[a] *United States of America v. Dylan Heatherly*, Case No. 19-2424, p. 3; and *United States of America v. William Staples*, Case No. 19-2932, p. 3.
[b] United States Department of Justice, Office of Public Affairs, "Two men convicted of engaging in child exploitation conspiracy", press release, 25 January 2018.
[c] Ibid.
[d] *United States of America v. Dylan Heatherly*, Case No. 19-2424; and *United States of America v. William Staples*, Case No. 19-2932, p. 10.
[e] Ibid., p. 21.
[f] Ibid., pp. 7–8.
[g] Ibid., p. 3.
[h] Available at https://sherloc.unodc.org/.

Tribunal Oral Federal de Jujuy, Causa FSA 8398/2014/TO1 (Argentina)

In Argentina, an investigation was initiated on 6 January 2014, following the receipt of information from the Australian Federal Police and the FBI via the United States Embassy in Buenos Aires about an Internet user located in Argentina (the defendant) who had downloaded child sexual abuse images and video recordings. The downloads involved pages from the following:

(a) IMGSRC.RU, a website based in the Russian Federation and dedicated to the publication of child sexual abuse that included links to child sexual abuse material: on this site, the defendant uploaded a photograph called "a beuty boy 3yo before to ..." from his personal email account;

(b) The Love Zone (TLZ), a platform dedicated to the exchange of child sexual abuse material requesting its aspiring members to make an initial contribution of 50 megabytes of unpublished child sexual abuse material: the defendant joined TLZ in 2013, and, after becoming a VIP member, uploaded several images and video recordings under the computer moniker "miguelboysnew". To maintain his membership, he made monthly contributions of 40 megabytes of child sexual abuse material.

Tribunal Oral Federal de Jujuy, Causa FSA 8398/2014/TO1 (Argentina) (*continued*)

The investigation of the case was led by the division of technological crimes of the federal police of Argentina, which preserved, analysed and produced reports based on the electronic evidence shared by the law enforcement authorities of Australia and the United States and the electronic evidence obtained from material seized in Argentina. The seized material, resulting from raids on two residences in Argentina, included four electronic devices, as well as various documents, used and unused condoms, and clothing of adults and children. A significant number of images and video recordings indicating the production, distribution, facilitation and acquisition of child sexual abuse material were obtained from the devices seized in the defendant's bedroom. Images and video recordings of activities that could be related to the recruitment of minors were also found. After further investigation, it was established that the defendant had filmed and photographed himself sexually abusing minors. The produced child sexual abuse material was later exchanged on the aforementioned website and platform. Forensic data extracted from the defendant's mobile phone and from his tablet computer revealed a significant number of photographs of children with Anglo-Saxon features, including a child holding a sign that read: "for my friend...", with the defendant's name following the word "friend". An analysis of metadata of the images linked some of the images with the defendant's mobile phone.

The defendant used the images of minors to obtain an exclusive benefit for himself, which was to have access to more child sexual abuse material on the website and platform. The defendant exploited minors by subjecting them to register their images in order to obtain a benefit for themselves, revealing the purpose of exploitation required by the type of trafficking. What the defendant did in relation to the TLZ site is payment in kind.

The federal oral court of Jujuy sentenced the defendant to 32 years' imprisonment for the crimes of "trafficking in persons for the purpose of exploitation, to promote, facilitate and commercialize child pornography" and "sexual abuse with repeated carnal access".

For more information about this case, see UNODC, SHERLOC case law database, Case No. ARGx012.[a]

[a] Available at https://sherloc.unodc.org/.

7. Trafficking in persons

Trafficking in persons refers to:

> The recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.[252]

ICT is used to recruit, coerce and control victims, to advertise trafficked persons, solicit clients and launder profits, among other illicit activities.[253] For example, in Belgium, an organized criminal group used ICT to recruit victims of trafficking in persons and "employees" to work for the organization (e.g., drivers), to

[252] Article 3, paragraph (a), of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime.

[253] See Maras, *Cybercriminology*.

advertise trafficked victims and to solicit clients.[254] To recruit victims, perpetrators may use "sockpuppet" profiles (multiple fictitious online profiles controlled by the same user to bolster some point of view) to manipulate and deceive targets and may browse social media profiles to identify vulnerable targets. Fake job advertisements have also been used to recruit victims and/or reach out to victims for fictitious work.[255]

Women and girls have been coerced to perform sex acts in front of cameras live-streaming to clients in different parts of the world (see the box below). Traffickers have also recruited and coerced persons to commit crimes, including cybercrimes and fraud. In one case in Denmark, trafficked persons were coerced into committing fraud involving the use of fake digital signatories to file tax returns.[256] In another case in Denmark, trafficked persons were coerced into perpetrating credit card and other forms of fraud (see, for example, the discussion on the Wasp Nest case in chap. VI, sect. E.3).[257]

Regional Trial Court of Misamis Oriental, 10th Judicial Region, Branch 41, CRIM Case No. 2009-337 (Philippines)

The victims in this case were recruited from different areas of the Philippines and transported to and harboured in the City of Cagayan de Oro, Philippines. Some of the victims were lured under the pretence of working as an administrative assistant for a good salary, either in the Philippines or overseas, while others were informed that the work involved cybersex. Irrespective of what was discussed with victims, all of the victims worked in a cybersex den. The den, located on the third floor of a building, included several rooms, each with a bed and a computer with a webcam and Internet connection. The victims were required to interact with paying customers and comply with the requests of the customers, such as undressing, dancing and/or engaging in sex acts streamed via webcam.

The defendants took advantage of the vulnerable position of the victims and sexually exploited them. The defendants argued that cybersex was not against the law. The court emphasized that that did not exculpate the defendants. The defendants were charged not with facilitating cybersex, but with the crime of trafficking in persons. The court held that evidence presented in the case demonstrated a conspiracy between the defendants and others not charged in the case.

The defendants were charged with conspiracy and trafficking in persons in violation of sections 4 (a), 4 (e) and 6 (e) of Republic Act No. 9208. The defendants, B.S.S., E.A.S., A.G.R., A.P.B and A.L.R., were found guilty of these crimes. Two of the defendants (B.S.S. and E.A.S., both males with Swedish citizenship) received a sentence of life imprisonment, and each of them was required to pay a fine of 2 million Philippine pesos. The other three defendants (A.G.R., A.P.B and A.L.R.) were sentenced to 20 years' imprisonment, and each of them was required to pay a fine of Pts 1 million.

For more information, see UNODC, SHERLOC case law database, Case No. PHL007.[a]

[a] Available at https://sherloc.unodc.org/.

[254] Belgium, Tribunal correctionnel d'Anvers, Antwerpen, 2 mai 2016.

[255] Maras, *Cybercriminology*.

[256] Danmark B (R), ref. 9-3441/2015, domfældelse 14 December 2015.

[257] Ibid.

The advertisement of services are an essential element of trafficking in persons, as it enables the traffickers to obtain clients for the services they are offering. Such advertisements may appear on online classified advertisement sites, may be posted on social media platforms advertising trafficked persons (even the sale of children) and may be in the form of individual websites dedicated to advertising trafficked victims, prostitution or escort services.[258] In the United States, six defendants (four male and two female offenders) were charged with and convicted for their role in trafficking two female victims, an adult and a minor, for the purpose of sexual exploitation in two states (Maryland and Virginia) between 2018 and 2019.[259] Recruitments and advertisements of the minor victim were placed on Backpage.com shortly before it was shut down (see the box in chap. IV), as well as YesBackpage, Bedpage and CityXGuide, which were viewed and promoted as sites that had taken the place of Backpage once it had been taken down. The advertisements were also available on a site that consolidates in one location escort advertisements from various sites, and an online community forum where information and reviews of escorts are shared. A well-know messenging application was used by the defendants to distribute images of the victims, to communicate with each other, the clients and victims and to advertise the victims, both the minors and the adults, by sending photographs of them to a "listserv"[260] of clients. Clients visited hotels and a brothel apartment leased by one of the female perpetrators to meet the victims. The defendants received sentences ranging from 6 years and 6 months to 16 years of imprisonment, whereby the average sentence was 15 years of imprisonment (one defendant received a sentence of 6 years and 6 months of imprisonment).[261]

8. Smuggling of migrants

The smuggling of migrants refers to the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State party (to the Protocol to Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime) of which the person is not a national or a permanent resident".[262]

Like trafficking in persons, ICT plays an integral role in the facilitation of the smuggling of migrants. ICT has been used to advertise and finance the smuggling of migrants and has served as a tool for communication between members of the smuggling operation and the migrants.[263] Advertisements of smuggling services, fees, methods of payment, modes of transport (e.g., by land, air or sea) and routes are posted on websites, social media platforms and other online platforms.[264] These platforms are also used to recruit migrants and other participants in the smuggling operations (e.g., drivers). ICT also facilitates the payment of fees associated with the smuggling of migrants. Payment can be rendered to smugglers and others involved in the smuggling operations using traditional commercial financial transactions (e.g., cash payments and wire transfers), cryptocurrencies or online payment and money transfer services via websites or applications.[265] Moreover, communication between smugglers and their associates, as well as between members of the smuggling operation and the migrants, is facilitated by encrypted and unencrypted telecommunications and electronic communication channels.[266]

[258] See, for example, *United States of America v. Daniel Palacios Rodríguez et al*. and Belgium, Tribunal correctionnel d'Anvers, Antwerpen, 2 mai 2016.

[259] *United States of America v. Daniel Palacios Rodriguez et al*.

[260] A listserv distributes messages to the subscribers of a mailing list.

[261] United States Attorney's Office, Eastern District of Virginia, "Sex traffickers sentenced to combined 81 years in prison", press release, 28 July 2020.

[262] Article 3, paragraph (a), of the Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the Organized Crime Convention.

[263] **CTOC/COP/WG.7/2020/3**, paras. 7-15; **A/CONF.234/11**, paras. 41–48.

[264] Ibid.

[265] **CTOC/COP/WG.7/2020/3**, paras. 14–15; see also A/CONF.234/11.

[266] CTOC/COP/WG.7/2020/3, paras. 7–15.

United States of America v. Cristian Hirales-Morales, Marcos Julian Romero and Sergio Anthony Santivanez, Case No. 19CR4089DMS (S.D. California, 10 October 2019) (United States of America)

Smuggling migrants across the border between Mexico and the United States

The leader (C.H.-M.) and two other high-ranking members (M.J.R. and S.A.S.) of a transnational criminal organization engaged in migrant smuggling operations and based in Tecate, Mexico, were charged with various violations of Title 8, section 1324, of the United States Code, including alien smuggling, conspiracy to bring illegal aliens into the United States for financial gain, and conspiracy to transport undocumented aliens within the United States for financial gain.[a] The organization had illegally smuggled migrants from Mexico through the southern border of California for a fee of US$ 8,000 per person.[b] M.J.R. and S.A.S had arranged meetings at hotels and motels to obtain the fees. Arrangements had subsequently been made to send the fees to C.H.-M. in Mexico.

ICT played an integral role in the logistics of the migrant smuggling operations. In particular, the leader, higher-ranking members and associates of the criminal organization used a well-known messaging application to communicate and coordinate with each other before and during smuggling operations.[c] M.J.R. and other criminal associates were responsible for recruiting drivers for the smuggling operations. Drivers were recruited through employment advertisements on an online classified advertisement site and other websites.[d] Among those recruited were secondary school students from San Diego, California.[e] C.H.-M. also used ICT to monitor and track movements of operatives and migrants, as well as to inform drivers of the pick-up locations for migrants by using a well-known mapping and navigation application for mobile devices.[f]

The two higher-ranking members (M.J.R. and S.A.S.) pleaded guilty to "conspiracy to bring illegal aliens into the United States for financial gain" and "conspiracy to transport undocumented aliens within the United States for financial gain", respectively. They have not been sentenced for their crimes and the leader of the organization, C.H.-M., has not yet been tried for his crimes.

[a] *United States of America v. Cristian Hirales-Morales, Marcos Julian Romero and Sergio Anthony Santivanez*, Case No. 19-CR-4089-DMS.
[b] Ibid., p. 3.
[c] Ibid., pp. 3–4.
[d] NBC San Diego, "Migrant smuggling ring accused of recruiting local high school students", 17 October 2019.
[e] Ibid.; Kristina Davis, "Trio charged with using high-schoolers to smuggle migrants", *The San Diego Union-Tribune*, 15 October 2019.
[f] *United States of America v. Cristian Hirales-Morales, Marcos Julian Romero and Sergio Anthony Santivanez*, p. 4.

9. Drug trafficking

Drug trafficking involves the illicit sale and distribution of drugs in violation of national laws or international laws, such as the Single Convention on Narcotic Drugs of 1961 as amended by the 1972 Protocol, the Convention on Psychotropic Substances of 1971 and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988. Every country is affected in some way by drug trafficking, regardless of whether it is used by drug traffickers as a source country, a transit country or a country of destination.

In *World Drug Report 2020*, it was noted that the global illicit drug market had expanded, and so had the illicit use of drugs worldwide.[267] New drug trafficking patterns have also been identified.[268] These patterns

[267] *World Drug Report 2020*, booklet 4, *Cross-Cutting Issues: Evolving Trends and New Challenges* (United Nations publication, 2020), p. 9.
[268] *World Drug Report 2020*, booklet 4.

include not only the types of drugs that are produced, demanded and distributed, but also the tools used (and the manner in which they are used) in the illicit drug trade. One example of such a tool is ICT. ICT has long been used by criminals to facilitate drug trafficking. Websites, online marketplaces, classified advertisements, social media platforms and applications have been used in the advertisement, sale and purchase of controlled drugs online.[269] For example, well-known messaging, chatting and social media platform applications have been used for daily operations, price negotiation, communication, arranging deliveries and other activities related to drug trafficking.[270] ICT has also been used to evade law enforcement detection through the use of prepaid mobile phones, encryption and the darknet.

Darknet drug markets have removed or at least reduced barriers to entry into drug markets. In *United States v. Ulbricht*, the testimony of a vendor from Silk Road (a now defunct darknet market) revealed that darknet drug markets such as Silk Road provided individuals with a platform to create a drug business irrespective of their geographical location, by providing them with the resources they needed to sell drugs via the platform: "an anonymous online sales portal, a huge pre-existing customer base, how-to advice from the 'Seller's Guide' and Silk Road discussion forum, and an escrow system…to collect payment from … customers remotely".[271] Silk Road and similar darknet sites that facilitate the illicit drug trade also made it easier for buyers to access drugs that they might not have been able to access offline. Even drug vendors can use other darknet vendors as drug suppliers to obtain the drugs that they sell online or offline, especially for drugs that are not easy to obtain physically in their geographical location. The drugs that are purchased online via the clearnet, as well as the darknet, are predominantly delivered by mail and express consignment shipping carriers worldwide (depending on the geographical location of the buyers and sellers and the quantity of the drugs).

United States of America v. Aaron Michael Shamo, Drew Wilson Crandall, Alexandrya Marie Tonge, Katherine Lauren Anne Bustin, Mario Anthony Noble, and Sean Michael Gygi, Case No. 2:16-CR-00631-DAK (D. Utah, 31 May 2017) (PHARMA-MASTER, AlphaBay vendor) (United States of America)

A.M.S. ran a drug trafficking organization that imported controlled substances, such as fentanyl and alprazolam, from China and used the drugs to manufacture fake oxycodone tablets made with fentanyl and counterfeit Xanax (alprazolam) tablets,[a] which were subsequently sold on the darknet market AlphaBay using the vendor name PHARMA-MASTER. A.M.S., through his organization, sold 1 million fake oxycodone tablets containing fentanyl to unsuspecting buyers in the United States.[b] Ultimately, A.M.S. was charged with and convicted for running, organizing, supervising and directing a continuing criminal enterprise that imported and distributed controlled substances.[c] Along with five other individuals (D.W.C., a male; M.A.N., a male; S.M.G., a male; A.M.T., a female; and K.L.A.B, a female), A.M.S. engaged in drug-related offences to obtain money. All members of the continuing criminal enterprise, with the exception of A.M.S., pleaded guilty to various drug-related offences (e.g., conspiracy to distribute fentanyl and conspiracy to distribute alprazolam) and/or to conspiracy to commit money-laundering charges.[d] A.M.S. was charged with and ultimately convicted by a jury for: engaging in a continuing criminal enterprise; three counts of aiding and abetting the importation of a controlled substance; possession of a controlled substance with intent to distribute; manufacture of a controlled substance; two counts of knowing and intentional adulteration of drugs while held for

[269] European Monitoring Centre for Drugs and Drug Addiction, "The Internet and drug markets: summary of results from an EMCDDA Trendspotter study" (2016).

[270] *United States of America v. Ramiro Ramirez-Barreti et al.*, Criminal No. 4:19-CR-47; United States District Court, Western District of North Carolina, *United States of America v. Anthony Blane Byrnes*, Case No. 3:20-MJ-51, Criminal Complaint, 13 February 2020.

[271] *United States of America v. Ross William Ulbricht*, 14-CR-68 (KBF), Government Sentencing Submission, 26 May 2015, pp. 2–3.

sale; aiding and abetting the use of the United States mail in furtherance of a drug trafficking offence; conspiracy to commit money-laundering; money-laundering promotion and concealment; and engaging in monetary transactions in property derived from specified unlawful activity.[e]

For his crimes, A.M.S. was sentenced to life imprisonment.[f]

[a] United States Attorney's Office, District of Utah, "Jury convicts Shamo of leading drug trafficking network", press release, press release, 30 August 2019.
[b] United States Attorney's Office, District of Utah, "Shamo sentenced to life in prison after conviction for organizing, directing drug trafficking organization", press release, 15 October 2020.
[c] *United States of America v. Aaron Michael Shamo, Drew Wilson Crandall, Alexandrya Marie Tonge, Katherine Lauren Anne Bustin, Mario Anthony Noble, and Sean Michael Gygi*, Case No. 2:16-CR-00631-DAK, Superseding Indictment, 31 May 2017, pp. 2 and 8.
[d] United States, Immigration and Customs Enforcement, "Utah grand jury returns superseding indictment in Shamo case; adds distribution of fentanyl count resulting in death", 18 October 2018.
[e] United States Attorney's Office, District of Utah, "Jury convicts Shamo of leading drug trafficking network".
[f] United States Attorney's Office, District of Utah, "Shamo sentenced to life in prison".

10. Trafficking in firearms

Trafficking in firearms is defined in article 3, paragraph (e), of the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime, as the import, export, acquisition, sale, delivery, movement or transfer of firearms, their parts and components and ammunition from or across the territory of one State party (to the Protocol) to that of another State party if any one of the States parties concerned does not authorize it in accordance with the terms of the Protocol or if the firearms are not marked in accordance with article 8 of the Protocol. ICT facilitates firearms trafficking by enabling perpetrators to advertise and sell firearms to customers worldwide in contravention of national and international laws.[272]

Firearms are advertised and sold on the clearnet and on the darknet.[273] On the clearnet, websites, chat rooms, discussion forums, social media platforms, online marketplaces and online classified advertisement sites are used in the solicitation, advertisement and sale of firearms.[274] Firearms can be advertised and sold on clearnet sites legally or in contravention of existing laws and/or terms of service of websites. Firearms are also advertised and sold on the darknet, predominantly through cryptomarkets (sites that resemble those of well-known online sales enterprises, where many vendors can sell their goods and services) and vendor sites (where vendors sell their own goods or services). For example, Ross Ulbricht, the former administrator of Silk Road, the now defunct darknet marketplace, allowed firearms sales on Silk Road until March 2012 and then moved those sales to a site called the Armory that had been created specifically for the advertisement and sale of firearms (see, for example, figure II).[275] Technical information and other data related to the development, assembly, procurement and use of firearms are also shared on the clearnet and the darknet.

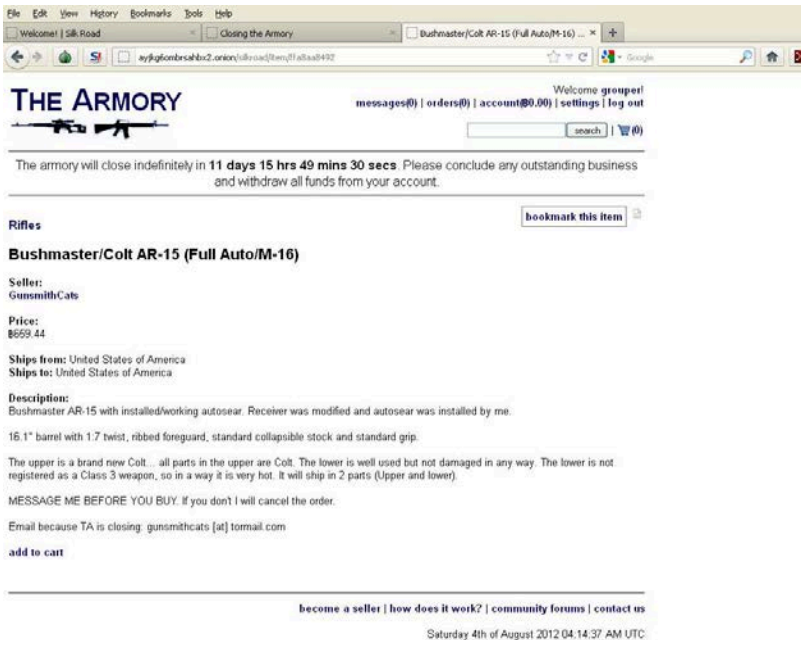
[272] See UNODC, Education for Justice University Module Series, Cybercrime, Module 13. For information on global firearms trafficking, see *Global Study on Firearms Trafficking 2020* (United Nations publication, 2020).

[273] For more information, see Maras, *Cybercriminology*, pp. 354–356; UNODC, Education for Justice University Module Series, Firearms, Module 4: the illicit market in firearms, "Supply, demand and criminal motivations". Available at **www.unodc.org/**; Giacomo Persi Paoli and others, *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Santa Monica, California; Cambridge, United Kingdom, RAND Corporation 2017).

[274] United States, Government Accountability Office, Report to Congressional Requesters, "Internet firearm sales: ATF enforcement efforts and outcomes of GAO covert testing" (November 2017).

[275] *United States of America v. Ross William Ulbricht*, Government Sentencing Submission, p. 2.

Figure II. Screenshot showing the page of a now defunct website created solely for the advertisement and sale of firearms



Source: United States District Court, Southern District of New York, *United States of America v. Ulbricht*, Government Sentencing Submission, 14 Cr. 68 (KBF) (2015).

LG Karlsruhe, Urteil vom 19.12.2018, 4 KLs 608 Js 19580/17 (Germany)

A dark web forum by the name of "Deutschland im Deep Web – Keine Kontrolle, alles erlaubt!" (Germany on the deep web – no control, everything allowed!) was created by the defendant, A.U., who operated under the username "luckyspax". From 18 March 2013 to his provisional arrest on 8 June 2017, the defendant operated and acted as the sole administrator of this dark web forum from his residence in Germany. The forum set up in the Tor network via the domain "germanyhusicaysx.onion", which was used by its users primarily for discussions and the (predominantly public) exchange of messages, but also for conducting illicit sales. To actively use the platform of the forum, it was necessary to register under a username and to provide an encrypted message address. Until it was shut down on 8 June 2017, the platform was one of the largest underground forums in German, with over 23,000 registered users.

The defendant subdivided the platform into different thematic categories, which were intended for exchanging information on certain topics or sales transactions. The categories and subcategories included:

(a) Religions (Islamists, Christian fundamentalists, doomsday);

(b) Freedom (free speech, will and suppression);

(c) Sports (martial arts, bodybuilding, steroids and doping);

(d) Politics and economy;

(e) Deep web:

(i) General (general topics about the deep web);
(ii) Websites (overview and discussion about hidden services);
(ii) Tutorials (tutorials in German about Tor, hidden services, encryption, etc.);
(iii) Bitcoins (speculation, anonymizing and trading);

(f) Security in information technology;

(g) Playground (rip-offs, etc.);

(h) Fraud and deception (fraud, carding and crime);

(i) Weapons (production, distribution and proper use);

(j) Eroticism (sex, preferences, relationships and prostitution);

(k) Suicide (effects, sharing of experiences and execution);

(l) Drugs (general topics on medicines and drugs):

(i) Experience reports and tips (safer use, trip reports, opinions);
(ii) Cultivation and production (exchange of experiences, problems and help);
(iii) Research chemicals (experiences, problems, ingredients and legality);

(m) Marketplace:

(i) Offer verified (cannabis verified, stimulants verified, psychedelics verified, pharmacy verified);
(ii) Offer (cannabis, stimulants, psychedelics, pharmacy, new services and software);
(iii) Search (services, goods, information, etc.);
(iv) Free trade zone (bargain bin);
(v) Contact exchange (interested in new contacts?);
(vi) Experience reports and reviews (regarding offers here or on other marketplaces).

Communication on the platform mainly took place through the forums, which were accessible to every user and only partially encrypted. In addition, users could communicate by means of the internal messaging function for private messages, which was mandatorily encrypted using a standard encryption system. Messages older than one month were automatically deleted. The users could also communicate via a well-known encrypted communications protocol or, in real time, via a messaging service that required users to have a separate instant messaging application. In addition, an escrow service was offered for transactions made on the platform.

The defendant did not receive a share of the profit from the sales on the platform. The use of the escrow service was, likewise, not based on a fee. The platform and the defendant were solely financed by donations in bitcoin. Following an appeal for donations on 24 December 2015, the defendant received €9,850.

The authorities were able to identify the defendant following his appeal for donations. The platform used bitcoin as virtual currency and donations were transferred to a bitcoin address. Via a bitcoin exchange, these donations could be transferred back to fiat currency. The bitcoins were transferred back to fiat currency via "Bitcoin.de", where the defendant used his real name and could therefore be identified.

Between 27 September 2015 and 18 August 2016, the defendant put online at least 15 advertising texts from users for the sale of narcotic drugs. The defendant also moved existing advertisements and those previously released by him from the subcategory "Offer" to the subcategory "Offer verified" and marked each respective seller as a "Verified Seller". By creating the category "Weapons" on the forum, the defendant also supported trading transactions for weapons from 11 February 2015 until his provisional arrest in June 2017. Neither the defendant nor users of the forum had any applicable permit to trade in narcotic drugs or weapons.

The transactions conducted via the platform included the sale of a handgun and the corresponding ammunition by the user "rico" (later identified as P.K.) to the user "Maurächer" (later identified as D.S.). Using the acquired weapon, D.S. carried out a mass shooting at a shopping centre on 22 July 2016, killing nine persons and severely injuring five others. In connection with the sale of the weapon to D.S., P.K. was convicted of nine counts of negligent homicide and five counts of negligent bodily harm and was sentenced to seven years' imprisonment.

LG Karlsruhe, Urteil vom 19.12.2018, 4 KLs 608 Js 19580/17 (Germany) (*continued*)

A.U. was charged with aiding the unlawful advertising of narcotic drugs (28 counts), aiding intentional unlawful trading in a firearm (7 counts), aiding the intentional unlawful acquisition of a semi-automatic pistol (2 counts) and intentional unlawful acquisition of narcotic drugs (4 counts). He was also charged with aiding intentional unlawful trading in a firearm in conjunction with negligent killing (9 counts) and with negligent bodily harm (5 counts) in relation to the sale of the weapon used by D.S. to carry out the mass shooting. A.U. was sentenced to six years of imprisonment.

For more information about this case, see UNODC, SHERLOC case law database, Case No. DEUx035.[a]

[a] Available at **https://sherloc.unodc.org/**.

The manufacture and distribution of firearms are regulated by law. Because firearms are manufactured and distributed legally and illegally, the identification, tracing and investigation of illegal firearms are complex.[276] Like drug traffickers, firearms traffickers take advantage of ICT and social media platforms (to advertise, sell and procure firearms) and also take advantage of mail and express consignment shipping carriers (to deliver the firearms to buyers located anywhere in the world).[277]

11. Trafficking in wildlife

Wildlife crime contributes to the destruction of wildlife resources and ecosystems, desertification, environmental degradation and the reduction and extinction of species. It has an impact on a wide range of wild animal species, including rhinoceros, elephants, pangolins, tigers, parrots, reptiles and eels, as well as a number of plant species, such as the variety of tropical hardwoods commonly referred to as "rosewood". It also threatens livelihoods, affects national security and undermines social and economic development.

Although the serious threats posed by wildlife crime are increasingly being recognized, there is no universally accepted definition of wildlife crime, nor are there international instruments that attempt to propound such a definition.[278] For the purposes of this publication, however, wildlife crime refers to harvesting of and trade in wild flora and fauna contrary to national law, including but not limited to national laws implementing obligations under the Convention on International Trade in Endangered Species of Wild Fauna and Flora.[279]

Wildlife crime has become a significant and specialized area of transnational organized crime.[280] Like other traffickers, wildlife traffickers use ICT to enhance their operations and facilitate the advertisement, sale and distribution of wildlife to customers throughout the world. Online trade in wildlife and wildlife products is growing,[281] a fact that has been recognized with concern by the General Assembly.[282]

While online marketplaces continue to be the most popular platforms for online wildlife trade, wildlife trade is increasingly occurring on social media platforms.[283] The growing trend in trafficking taking place through social media and messaging applications has been observed in relation to a number of species, including

[276] See also UNODC, Education for Justice University Module Series, Organized crime, Module 3: organized crime markets, "Firearms trafficking". Available at **www.unodc.org/**.

[277] Maras, *Cybercriminology*, pp. 354–356.

[278] See also *World Wildlife Crime Report 2020: Trafficking in Protected Species* (United Nations publication, 2020), p. 29.

[279] See also UNODC, *Guide on Drafting Legislation to Combat Wildlife Crime* (2018), p. 2.

[280] *World Wildlife Crime Report 2020*, p. 109.

[281] Ibid., p. 13.

[282] See, for example, General Assembly resolution 71/326.

[283] International Fund for Animal Welfare, "Disrupt: wildlife cybercrime" (London, 2018), p. 30.

species of reptiles and big cats.[284] One study of illicit marketplaces operating in the the United Kingdom found 1,194 advertisements selling 2,456 specimens of wildlife at prices totalling almost US$ 1 million.[285] In some countries, wildlife traffickers have been reported to prefer online sales to physical markets as they entail lower overhead costs and less scrutiny from authorities.[286] Traffickers change usernames and use technologies such as virtual private networks to avoid apprehension.[287] When online sales points are detected by law enforcement authorities, the traffickers simply move to different online platforms.[288]

United States of America v. Eoin Ling Churn Yeng and Gal Vin Yeo Siang Ann, Case No. 3:16 CR 00090 (D. Oregon, 23 February 2016) (United States of America)

The defendants, E.L.C.Y. and G.Y.S.A., operated Borneo Artifact, a company based in Malaysia. Borneo Artifact illegally sold wildlife and wildlife products (orangutan skulls, rhinoceros hornbill heads, helmeted hornbill skulls, etc.) via its website (borneoartifact.com) and an online auction site. The defendants conspired with others to illegally ship and import wildlife and wildlife products into the United States, concealing the true nature of the merchandise by purposely mislabelling the shipments (as "crafts for decoration", for example).

During the investigation of the enterprise, one of the defendants, E.L.C.Y., communicated via email with an individual who, unbeknown to E.L.C.Y., was an undercover special agent from the United States Fish and Wildlife Service of the Department of the Interior. The special agent was posing as an associate of E.L.C.Y. who, following an investigation into his activities, had agreed to act as a confidential informant and allowed the agent to use his email.[a] In his email messages sent to the special agent, E.L.C.Y. revealed the types of illicit wildlife and/or wildlife products that were for sale, the manner in which the merchandise would be transported to the United States, connections the defendants had in the countries from which the products would be shipped and the ways in which detection by border and custom agencies would be evaded.

The defendants ultimately pleaded guilty to conspiracy to smuggle goods into the United States, receiving six months' imprisonment, a fine of US$ 25,000, and 240 hours of community service to be completed during their one year of supervised release from prison.[b]

For more information on this case, see UNODC, SHERLOC case law database, Case No. USAx200.[c]

[a] United States District Court, District of Oregon, *United States of America v. Eoin Ling Churn Yeng and Gal Vin Yeo Siang Ann*, Case No. 15-MJ-173, Criminal Complaint 1 December 2015); *United States of America v. Eoin Ling Churn Yeng and Gal Vin Yeo Siang Ann*, Case No. 3:16 CR 00090, Criminal Indictment, 23 February 2016.

[b] United States Attorney's Office, District of Oregon, "Two Malaysian men sentenced to federal prison for smuggling endangered wildlife into U.S.", press release, 27 April 2016.

[c] Available at https://sherloc.unodc.org/.

[284] *World Wildlife Crime Report 2020*, pp. 13, 15 and 87.

[285] International Fund for Animal Welfare, "Disrupt".

[286] *World Wildlife Crime Report 2020*, p. 76.

[287] Coalition to End Wildlife Trafficking Online, "Offline and in the wild: a progress report of the Coalition to End Wildlife Trafficking Online" (2020), p. 3.

[288] *World Wildlife Crime Report 2020*, p. 76.

12. Trafficking in cultural property

Trafficking in cultural property is a crime that strikes at cultural heritage – the unique testimony to the identity of peoples.[289] Trafficking in cultural property deprives people of fundamental elements of their identity and of valuable resources for their sustainable development, dispossessing them of their past and thus prejudicing their future.

The General Assembly has expressed its alarm at the growing involvement of organized criminal groups in all forms and aspects of trafficking in cultural property and related offences.[290] On numerous occasions, the Assembly has reaffirmed the need to strengthen international cooperation in preventing, prosecuting and punishing all aspects of trafficking in cultural property.[291]

Notwithstanding the international consensus concerning the need to prevent and combat trafficking in cultural property, there is no single, universally agreed definition of "cultural property".[292] In article 1 of the Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property, adopted by the General Conference of the United Nations Educational, Scientific and Cultural Organization in 1970, the term "cultural property" is defined as property that, on religious or secular grounds, is specifically designated by each State as being of importance for archaeology, prehistory, history, literature, art or science and that belongs to the categories listed in that article. In article 2 of the UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects, adopted in 1995, "cultural objects" are defined as those objects which, on religious or secular grounds, are of importance for archaeology, prehistory, history, literature, art or science and which belong to one of the categories listed in the annex to the Convention. This definition is similar to that in article 1 of the 1970 Convention but does not require that such objects be specifically designated by a State as being of importance.

There is also no internationally agreed definition of "trafficking in cultural property". Trafficking in cultural property is generally understood to be a phenomenon rather than a single type of conduct in relation to cultural property.[293] "Trafficking in cultural property" hence refers to a broad range of conduct relating to the illicit trade in cultural property.

Trafficking in cultural property using the Internet has also been recognized as a matter of concern to the international community.[294] The General Assembly, expressing its alarm at the growing involvement of organized criminal groups in all forms and aspects of trafficking in cultural property and related offences, has noted that illicitly trafficked cultural property is increasingly being sold through all kinds of markets, in particular over the Internet.[295]

[289] See also International Guidelines for Crime Prevention and Criminal Justice Responses with Respect to Trafficking in Cultural Property and Other Related Offences (General Assembly resolution 69/196, annex).

[290] Ibid.

[291] See, for example, General Assembly resolutions 66/180, 69/196, annex, and 73/130.

[292] United Nations Educational, Scientific and Cultural Organization (UNESCO), International Standards Section, Division of Cultural Heritage, "Legal and practical measures against illicit trafficking in cultural property: UNESCO handbook" (Paris, 2006), p. 4.

[293] UNODC, *Practical Assistance Tool to Assist in the Implementation of the International Guidelines for Crime Prevention and Criminal Justice Responses with Respect to Trafficking in Cultural Property and Other Related Offences* (Vienna, 2016).

[294] See also UNESCO, International Criminal Police Organization (INTERPOL) and International Council of Museums, "Basic actions concerning cultural objects being offered for sale over the Internet" (2006).

[295] See General Assembly resolutions **66/180** and **69/196**.

Organized criminal groups have engaged in the trafficking in cultural property through legitimate markets online and credible auction sites, as well as through underground illicit markets. Since the late 2000s, social media and communication applications have also been used for trafficking in cultural property.[296] The shift to online trade has expanded the potential customer base for traffickers, has created new markets for small, inexpensive objects such as coins that previously would not have been profitable to trade and has provided traffickers with opportunities to sell cultural property and receive payment without being detected.[297] These trends have led to a rise in the number of dealers in trafficked cultural property.[298]

United States of America v. Ijaz Khan, Case No. 17-4301 (4th Circuit 2018) (United States of America)

The defendant (I.K.) was convicted by a jury for crimes that included the smuggling of goods into the United States[a] (the smuggling of stolen cultural artefacts (e.g., coins, pottery, arrowheads and bronze weapons) from Pakistan into the United States) and conspiracy.[b] The defendant had submitted fraudulent documents, purportedly from the Government of Pakistan, authorizing his export of the cultural artefacts and certifying the value of the objects. The defendant used his company, Indus Valley, to sell the stolen cultural artefacts to his existing customer base, in person (at shows) and online (on websites and auction sites).[c]

The defendant was identified as the leader and organizer of an organized criminal group made up of his family members (his wife and sons) and others who were not related to the defendant (e.g., J.B.M.). He played a central role in the planning and operations and in the recruitment of accomplices, and he controlled and exercised authority over others in the group. Because of his central leadership role, he received a sentencing enhancement, which he unsuccessfully appealed. The defendant pleaded guilty and was sentenced to three years' imprisonment and was required to pay a fine of approximately US$ 115,000 and to forfeit more than 1,300 cultural artefacts.[d] The defendant unsuccessfully appealed his conviction and sentence to the United States Court of Appeals for the Fourth Circuit.

Others in the organized criminal group pleaded guilty and were also sentenced for their roles in the conspiracy to commit smuggling. For example, V.L. (the defendant's wife) and J.B.M. received sentences of four months of imprisonment (and two years of supervised release from prison) and two years of probation, respectively.[e]

[a] The offence of "smuggling goods into the United States" is included in Title18, section 545, of the United States Code.
[b] United States Court of Appeals, Fourth Circuit, *United States of America v. Ijaz Khan*, Case No. 17-4301 (4th Circuit 2018).
[c] United States Attorney's Office, Eastern District of Virginia, "Three indicted for smuggling artifacts into U.S. and citizenship fraud", press release, 27 May 2016; United States District Court, Eastern District of Virginia, *United States of America v. Assorted Artifacts*, Civil Action No. 1:16cv1393, 21 February 2017.
[d] United States Attorney's Office, Eastern District of Virginia, "Man sentenced for smuggling artifacts from Pakistan into United States", press release, 5 May 2017.
[e] Pahedra Haywood, "Santa Fe duo sentenced in immigration fraud, artifacts-smuggling case", *The New Mexican*, 5 May 2017; Matt Zapotosky, "Probation for dealer who smuggled artifacts from grave sites in Pakistan", *The Washington Post*, 26 January 2016.

[296] Neil Brodie and Donna Yates, *Illicit Trade in Cultural Goods in Europe: Characteristics, Criminal Justice Responses and an Analysis of the Applicability of Technologies in the Combat against the Trade–Final Report* (Luxembourg, Publications Office of the European Union, 2019), p. 106; United Nations Educational, Scientific and Cultural Organization, Fourth Session of the Subsidiary Committee of the Meeting of States Parties to the Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property, document C70/16/4.SC/10, paras. 20–22.

[297] Brodie and Yates, *Illicit Trade in Cultural Goods in Europe*, p. 106.

[298] Ibid.

Authorities investigating trafficking in cultural property online face a number of challenges, including the variety of platforms on which cultural property is trafficked online, missing information hindering proper identification of items, and difficulties identifying vendors. To avoid detection, traffickers of cultural property operating online have used hacker techniques such as IP address spoofing (i.e., replacing the source IP address with a fake one).[299]

13. Money-laundering

Money-laundering can be described as the process whereby criminals conceal and legitimate illicit funds.[300] To accomplish this, criminals take the proceeds of a crime and transform them into what appears to be legally obtained funds. Money-laundering enables criminals to keep and use the proceeds of their crimes and to conceal the predicate offences that enabled them to obtain those proceeds. In article 6 of the Organized Crime Convention, States parties to the Convention are required to criminalize four types of offences related to money-laundering:

(a) The conversion or transfer of property, knowing that such property is the proceeds of crime;[301]

(b) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;

(c) The acquisition, possession or use of property, knowing that such property is the proceeds of crime;

(d) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with article 6 of the Convention.

State v. Naidu et al [2018] FJHC 873 (Fiji)

The case *State v. Naidu et al* involved an online scam with international consequences undertaken by the defendants (R.R.N., A.R.D. and R.R.). The defendants hacked into the electronic banking facility of several accounts of a large bank based in Australia. They made unauthorized online money transfers to two other accounts from the same bank: the accounts of the defendant A.R.D. and another person (A.C.). The stolen money deposited into those accounts was later withdrawn on the instructions of R.R.N. A.R.D. gave the withdrawn sums to R.R.N., who then transferred the money abroad through a well-known money transfer service. He was helped by R.R., who was a teller at that company.

The defendants were all charged with money-laundering. In order to prove the offence of money-laundering, the prosecution had to prove that the accused person engaged, directly or indirectly, in a transaction that involved proceeds of crime (in this case, stolen money) and that the accused knew, or ought to have known, that the money was derived or realized, directly or indirectly, from some form of unlawful activity. In Fiji, the offence of money-laundering is not predicated on proof of the commission of the offence from which the proceeds derived, thereby facilitating convictions of organized criminal groups.

Ultimately, the court found all of the defendants guilty of money-laundering.[a] On 18 September 2018, the court sentenced the defendants R.R.N., A.R.D. and R.R. to six years and nine months of imprisonment, three years of imprisonment and five years of imprisonment, respectively. In addition, R.R.N. was ordered to pay a restitution of 12,000 Fiji dollars to the bank.

[299] European Commission, Commission staff working document: impact assessment accompanying the document proposal for a regulation of the European Parliament and of the Council on the import of cultural goods, document SWD(2017) 262 final, p. 15.

[300] Maras, *Cybercriminology*, p. 336.

[301] In article 2, paragraph (e), of the Organized Crime Convention, "proceeds of crime" is defined as "any property derived from or obtained, directly or indirectly, through the commission of an offence".

The defendant, R.R., filed a notice of appeal against her conviction and sentence and applied for bail pending appeal. Both the leave to appeal and the application for bail pending appeal were refused by the court. The defendant, R.R.N., filed a notice for appeal against his conviction and sentence, arguing that his sentence was manifestly harsh and excessive and wrong in principle, and applied for bail pending appeal. While the Court of Appeal of Fiji noted that the defendant had not substantiated why his sentence was harsh and excessive, it reiterated what the trial court had said — that the tariff for the offence of money-laundering was not well settled in Fiji. The Court of Appeal further noted that, at that stage, it was not able to tell if the sentencing tariff of 5–12 years set by the trial judge was widely accepted and implemented among all trial courts in Fiji. The court held that the issue of sentencing tariffs should thus be taken on by the Court of Appeal or the Supreme Court to guarantee uniformity. The Court of Appeal found that, since it was a question of law, no leave for appeal was required, but it allowed for leave to appeal against the sentence as a matter of formality. However, the Court of Appeal also noted that none of the grounds of appeal had any reasonable prospect of success at that stage. The Court of Appeal refused the application filed by R.R.N. for bail pending appeal and leave for appeal against the conviction but allowed leave for appeal against the sentence. Appeal proceedings have not yet taken place.

This case is of great significance, since it is one of only a few judgments in the region involving cybercrime. At the time of the investigation, the authorities of Fiji had only limited experience with cybercrime and no direct evidence proving that the proceeds of crime were derived from cybercrime was provided to the court. The defendants could, nonetheless, be convicted of money-laundering since, in Fiji, the offence of money-laundering is not predicated on proof of the commission of the offence from which the proceeds derived. The trial court was therefore able to rely on circumstantial evidence when convicting the members of the organized criminal group.

For more information, see UNODC, SHERLOC case law database, Case No. FJIx008.[b]

[a] Fiji, Proceeds of Crime Act 1997, as amended by the Proceeds of Crime (Amendment) Act 2004, sect. 69, paras. (2) (a) and (3) (a).

[b] Available at https://sherloc.unodc.org/.

The money-laundering process consists of three stages: placement, layering and integration. During the placement stage, the illicitly obtained money is distributed into the financial system (e.g., through the purchasing of assets or currency exchanges). The next stage, layering, includes multiple activities that seek to further distance the proceeds of the crime from their original source, making it more difficult to uncover money-laundering. More specifically, once the proceeds of the crime have been placed into the financial system, they are moved to other financial institutions or converted from one type of asset to another in order to further distance the proceeds of the crime from their illicit origin. Finally, the proceeds of the crime are introduced back into the economy. At this stage of money-laundering, integration, the proceeds of the crime appear to be legitimate and are used by criminals to buy property and/or acquire other assets.

The mechanisms (e.g., people, financial and non-financial institutions, such as banks, wire transfer companies, currency exchanges and casinos) and instruments (e.g., securities or wire transfers) used in money-laundering vary. For instance, in the GozNym malware case, the offenders stole money from victims' bank accounts and laundered those funds using United States and foreign beneficiary bank accounts controlled by the defendants;[302] in contrast, the Bayrob criminal enterprise, and criminals in other cases included in this digest, used money mules to do the money-laundering.[303] Money-laundering can also be done through unlicensed money transmitters, which do not comply with laws and internationally recognized standards for countering money-laundering. Unlicensed money transmitters have enabled individuals

[302] *United States of America v. Alexander Konovolov et al.* (GozNym malware).

[303] See, for example, *United States of America v. Bogdan Nicolescu, Tiberiu Danet and Radu Miclau* (Bayrob); and *United States of America v. Aleksei Yurievich Burkov* (Card Planet).

to transfer funds without providing and proving their identities. A case in point is e-Gold, an unlicensed and unregistered money transfer business that operated in contravention of money-laundering laws and regulations, thereby enabling criminals to use it to anonymously expand and profit from their illicit activities.[304] In particular, e-Gold provided their services (i.e., transferable gold-denominated accounts) via two websites, where users could register and use the platforms to buy, transfer and exchange digital currency backed by precious metals, known as units of e-gold, without validating their identity. Ultimately, e-Gold and its corporate affiliate pleaded guilty to conspiracy to engage in money-laundering and conspiracy to operate an unlicensed money transmitting business.[305]

United States of America v. Andre-Catalin Stoica et al., Case No. 5-18-CR-81-JMH (E.D. Kentucky, 5 July 2018) (Alexandria Online Auction Fraud Network) (United States of America)

A transnational criminal organization (called the "Alexandria Online Auction Fraud Network" by United States authorities in the criminal indictment) perpetrated online auction fraud (i.e., advertising and selling non-existent items) against victims in the United States on licit online marketplaces, an online classified advertisement site and an online sales website.[a] The organization operated primarily in Alexandria, Romania, with some operations taking place in other areas of Eastern Europe, as well as in the United States.[b] The victims of the online auction fraud paid for the fake items with reloadable prepaid cards, prepaid debit cards and gift cards of various types; United States postal money orders; cashier's cheques; wire transfers from a well-known money transfer service; and bank wires and deposits.[c]

The Alexandria Online Auction Fraud Network worked with others to launder criminal proceeds, by taking the money paid by victims for the fake items sold online, converting the money to bitcoin, transferring the bitcoin to members and associates in Eastern Europe and using bitcoin exchanges to convert the bitcoin to fiat currency.[d] Associates of the organizations in the United States, such as J.A.V., obtained victims' payments, converted them to bitcoins and sent the bitcoins to members of the organization who had perpetrated the online auction fraud.[e] Third parties in the United States who participated in money-laundering (A.E.N., D.A.B. and R.W.D.L.T) were also used to collect, redeem and convert victims' payments into cash or bitcoins.[f] In addition, two bitcoin exchangers were used by the Alexandria Online Auction Fraud Network. R.I., a national of Bulgaria and owner of the Bulgarian bitcoin exchange RG Coins, was charged with and convicted of conspiracy to commit racketeering and conspiracy to commit money-laundering in contravention of United States laws.[g] V.-C.N., a national of Romania and owner of a bitcoin exchange (Coinflux Services SRL) registered in Romania, pleaded guilty to conspiracy to commit racketeering.[h]

Of the 20 individuals charged in the United States, 16 were foreign nationals. Twelve of the foreign nationals have been extradited to the United States.[i] To date, 17 individuals have been convicted for crimes relating to the online auction fraud perpetrated by members and associates of the criminal organization, including conspiracy to commit racketeering, money-laundering, wire fraud and identity-related fraud.[j]

[304] United States District Court, District of Columbia, *United States of America v. E-Gold Limited*, Criminal Action No. 07-109 (RMC), 20 July 2007.

[305] United States Department of Justice, "Digital currency business E-Gold pleads guilty to money laundering and illegal money transmitting charges", press release, 21 July 2008.

For more information see, see UNODC, SHERLOC case law database, Case No. USAx175.[k]

[a] *United States of America v. Andre-Catalin Stoica et al.*, p. 3; *United States of America v. Beniamin-Filip Ologeanu*; United States Attorney's Office, Eastern District of Kentucky, "United States v. Andrei Catalin Stoica, et al. (5:18-CR-81-JMH) and United States v. Beniamin-Filip Ologeanu, et al. (0:19-CR-10-JMH)", updated 20 July 2020.

[b] *United States of America v. Andre-Catalin Stoica et al.*, p. 3.

[c] Ibid., p. 4.

[d] Ibid., pp. 3–4.

[e] United States District Court, Eastern District of Kentucky, *United States of America v. Joshua Aaron Vallance*, Case No. 20 CR. 08, 28 May 2020), p. 3.

[f] *United States of America v. Beniamin-Filip Ologeanu et al.*, Superseding Indictment, p. 6.

[g] *United States of America v. Andre-Catalin Stoica et al.*, pp. 9–10; United States Department of Justice, Office of Public Affairs, "Owner of bitcoin exchange convicted of racketeering conspiracy for laundering millions of dollars in international cyber fraud scheme", press release, 28 September 2020.

[h] *United States of America v. Andre-Catalin Stoica et al.,* p. 9.; United States Department of Justice, Office of Public Affairs, "Fifteen defendants plead guilty to racketeering conspiracy in international cyber fraud scheme", press release, 11 June 2020.

[i] United States Department of Justice, Office of Public Affairs, "United States and international law enforcement dismantle online organized crime ring operating out of Romania that victimized thousands of U.S. residents", press release, 7 February 2019.

[j] United States Department of Justice, Office of Public Affairs, "Owner of bitcoin exchange convicted of racketeering conspiracy"; "United States and international law enforcement dismantle online organized crime ring"; United States District Court, Eastern District of Kentucky, *United States v. Alexandru Ion*, Case No. 5:18-CR-81-REW-MAS-6, 10 October 2019; United States Attorney's Office, Eastern District of Kentucky, "Fifteen defendants plead guilty to racketeering"; *United States of America v. Beniamin-Filip Ologeanu et al.*; *United States of America v. Andre-Catalin Stoica et al.*; United States Department of Justice, Office of Public Affairs, "United States and international law enforcement dismantle online organized crime ring".

[k] Available at https://sherloc.unodc.org/.

14. Internet gambling

Internet gambling involves the offering of casino-style games (e.g., poker) and/or betting (e.g., at horse-racing and sporting events) online. Internet gambling varies from offline gambling, particularly with respect to currency and language. Internet gambling websites and content are available in multiple languages and offer a wide variety of currencies and payment options. For traditional (offline) gambling establishments, such as casinos and betting establishments, there are limited language, currency and payment options, which depend on the geographical location of the establishment. Nevertheless, the main difference between such conventional gambling and Internet gambling is that a person can engage in Internet gambling at any time and at any place irrespective of his or her geographical location.

Internet gambling services can be provided by "bricks-and-mortar" casinos (i.e., casinos with physical locations) or betting establishments and organizations that do not have "bricks-and-mortar" casinos or by betting establishments that only have remote gambling services. In some jurisdictions, those providing Internet gambling services are required to have physical establishments that offer similar services in person;[306] in those cases, online services are viewed merely as an extension of services already provided in person. Internet gambling raises concern over problematic and compulsive gambling behaviour; gambling by minors; fraud and other crimes committed online for and against the gambling organizations; the fairness and integrity of gaming and associated processes; the oversight and accountability of online gambling sites; and the cybersecurity of those sites.[307]

[306] See, for example, the government websites in countries that include information about Internet gambling licences. In the United States, casinos in New Jersey have been given licences. The licences enable them to offer Internet gambling services in the State of New Jersey (United States, State of New Jersey, Division of Gaming Enforcement, "Internet gaming sites". Available at www.nj.gov/oag/ge/gamingsites.html).

[307] "Because of the lack of direct contact between consumer and operator, games of chance accessible via the internet involve different and more substantial risks of fraud by operators compared with the traditional market for such games" (Court of Justice of the European Union, *Sporting Exchange Ltd v. Minister van Justitie*, Case No. C-203/08, Judgment, 3 June 2010, para. 34). See also Masood Zangeneh, Mark Griffiths and Jonathan Parke, "The marketing of gambling", in *In the Pursuit of Winning: Problem Gambling Theory, Research and Treatment,* Masood Zangeneh, Alex Blaszczynski and Nigel Turner, eds. (New York, Springer, 2008), pp. 135–15); John L. McMullan and David Perrier, "The security of gambling and gambling with security: hacking, law enforcement and public policy", *International Gambling Studies*, vol. 7, No. 1 (2007), pp. 43–58; Sangeeta Ranade, Stuart Bailey and Alexandra Harvey, "A literature review and survey of statistical sources on remote gambling" (October 2006); UNODC, *Comprehensive Study on Cybercrime*, draft, p. 21.

Internet gambling is not universally criminalized at the national level. The type of gambling that is considered illegal also varies from country to country.[308] Because of the variation in laws, companies and criminal organizations can house their servers and conduct their operations in multiple jurisdictions where Internet gambling is legal. Organizations and criminal groups offering Internet gambling can have their operations located in various countries – they can have the headquarters of their company in one country, servers in one or more countries and support centres in different countries, depending on the regulations of each country on Internet gambling and taxation, which vary between countries. Some countries support Internet gambling as long as it occurs in accordance with existing laws and meets licensing, regulatory and taxation requirements.[309] Other countries allow Internet gambling under certain circumstances in accordance with national law and restrict and control and limit Internet gambling operations.[310] In other countries, Internet gambling is strictly prohibited.[311]

Cassazione penale, sezione VI, sentenza No. 11356, 8 Novembre 2017 (Italy)

This case concerns the involvement of a mafia-type group, the Clan of Casalesi, in illegal online gambling. The Clan of Casalesi emerged decades prior to the instant case in the province of Caserta in the region of Campania, in the south of Italy. After emerging in Caserta, the Clan of Casalesi progressively established its control in the region of Campania. The group subsequently expanded its activities into other regions of Italy, including the region of Emilia-Romagna, in the north of Italy.

The modus operandi used by the Clan of Casalesi for their illicit activities relating to online gambling in the region of Emilia-Romagna differed from the modus operandi used in the region of Campania. In Campania, the main group of the Clan offered protection to entrepreneurs working in the gambling industry. In exchange for a monthly fee, the main group, through intimidation and violence, imposed on local businesses the services and products of the protected entrepreneurs, fending off the competition. In Emilia-Romagna, where the main group had recently expanded its influence, a relatively autonomous branch of the Clan used a different method. Rather than offering protection to the entrepreneurs in the region, the Emilia-Romagna branch used a formally legitimate enterprise as a front for their activities, opening betting points at which unauthorized slot machines were installed and online links to illegal gambling websites were made available to clients. The illegal gambling business allowed the branch to make profits while avoiding the payment of taxes and made possible the money-laundering of the criminal group's proceeds derived from other activities.

The judgment of the Supreme Court of Cassation in this case dealt with the defendants who opted for shortened judicial proceedings. The issue in this case concerned the application of criminal association offences – both the "simple" criminal association offence and the mafia-type association offence – to a mafia-type group consisting of: *(a)* the main group operating in the region of Campania, which adopted intimidation, submission and silence as its modus operandi (the mafia method); and *(b)* the Emilia-Romagna branch, which did not adopt the mafia method. The Court was required to determine the correct application of the criminal association offence and the mafia-type offence in relation to the participants of the two units of the mafia-type group.

[308] For example, in the United States, betting on horse racing is considered legal (with few exceptions), whereas sports betting was considered illegal in many states until 2018, when the Supreme Court struck down a federal law prohibiting sports gambling at the state level (see *Murphy, Governor of New Jersey, et al. v. National Collegiate Athletic Association*, No. 16-476, 584 U.S. ___ (2018), 138 S. Ct. 1461). The Wire Act of 1961, a United States federal law, is currently being interpreted as applying to interstate sports gambling and interstate Internet sports gambling.

[309] See, for example, United Kingdom, Gambling Act of 2005.

[310] See, for example, Ordinance 30 of 1960 of Singapore and its subsequent revisions (i.e., the Betting Act) and the Remote Gambling Act of 2015.

[311] See, for example, the Common Gaming Houses Act of Brunei Darussalam, which prohibits all forms of gambling, and article 17 of the Federal Decree-Law No. 5 of 2012 of the United Arab Emirates, which prohibits Internet gambling.

The prosecutor charged the members who had participated in the main group and the Emilia-Romagna branch with the mafia-type association offence and with the criminal association offence, whereas those who had participated only in the Emilia-Romagna branch were charged with only the criminal association offence. In the opinion of both the court of first instance and the Court of Appeal of Naples, the presence of the relatively autonomous Emilia-Romagna branch, which had adopted a modus operandi that differed from that of the main group, required the application of two different criminal association offences, the mafia-type association offence being applicable to the main group and the criminal association offence being applicable to the Emilia-Romagna branch. The courts rejected the choice made by the prosecutor in the indictment (i.e., charging those members who had participated in both the main group and the Emilia-Romagna branch with two different criminal association offences) on the grounds that that constituted double jeopardy. This finding was supported by the court's conclusion that the main group and the Emilia-Romagna branch were not distinct criminal groups but rather a single criminal group sharing the same aims, notwithstanding the fact that the Emilia-Romagna branch exercised relative autonomy. Accordingly, to convict the defendants for membership of both the main group and the subgroup would be to convict them twice for the same offence. The proper approach was for the defendants that had participated in both the main group and the Emilia-Romagna branch to face punishment only for their participation in the main group (i.e., punishment for the mafia-type association offence).

Following the decision of the Court of Appeal of Naples, those members who had participated only in the Emilia-Romagna branch appealed to the Supreme Court of Cassation seeking an acquittal for their convictions for the criminal association offence. For almost every defendant, the Supreme Court of Cassation upheld the decision of the Court of Appeal of Naples, which largely confirmed the findings of guilt. In particular, the Court rejected the appeals of those defendants who had participated only in the Emilia-Romagna branch and stated, in line with the ruling of the Court of Appeal of Naples, that it was necessary to bring charges of both the criminal association offence and the mafia-type association offence against different defendants, even if all defendants were part of the same larger criminal group. This was because, first, the Emilia-Romagna branch showed some degree of autonomy and, secondly, the Emilia-Romagna branch did not share the same modus operandi - that is, the pattern of violence and intimidation - of the main group. Moreover, the Supreme Court of Cassation agreed with the decision of the Court of Appeal of Naples and the trial court that to convict the members who had operated in both regions, Campania and Emilia-Romagna, of both the mafia-type association offence and the criminal association offence, as they had been charged by the prosecutor, would constitute double jeopardy. Both the Court of Appeal and the trial court had, therefore, correctly avoided the application of multiple criminal association offences to those defendants.

CHAPTER VI.

RELEVANT PROCEDURAL ISSUES

VI. RELEVANT PROCEDURAL ISSUES

Relevant procedural issues in cases of cyber organized crime include jurisdictional issues; identification, tracing, freezing and seizure of assets and confiscation of proceeds of crime; special investigative techniques (i.e., electronic surveillance, undercover operations, controlled deliveries and other techniques); the collection and use of electronic evidence (i.e., expedited preservation of data, production orders, real-time collection of communication traffic data and interception of content data); and various forms of international cooperation (i.e., extradition, mutual legal assistance, law enforcement cooperation and joint investigations). Each of these procedural issues are explored below.

A. Jurisdiction

Jurisdiction provides countries with the power and authority to define and preserve the duties and rights of people within its territory, enforce laws and punish law violations.[312] Countries claim jurisdiction over crimes committed within their territory (principle of territoriality), when crimes are committed by their own nationals (principle of nationality; active personality principle), when the victims of the crimes are their own nationals (principle of nationality; passive personality principle) and when the crime impacts the interests and security of the country (protective principle).[313]

Laws are implemented to establish rules, mechanisms and ways to resolve jurisdictional issues when multiple jurisdictional claims are made over transnational organized crime, such as cyber organized crime. Article 15 of Organized Crime Convention establishes conditions under which jurisdiction can be asserted and provides guidance on exercising jurisdiction. The conditions under which jurisdiction can be asserted are when transnational organized crime offences are committed in a country's territory, when such offences are committed on board an aircraft or a vessel registered in a country, when such offences are committed in one country by nationals of another and the country in which the offences were committed does not extradite the offenders on the ground that they are nationals of the other country and when such offences are committed in one country against nationals of another country.[314] Similar conditions are included in other international laws, such as the United Nations Convention against Corruption (see art. 42) and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 (see art. 4).[315] Countries establish jurisdiction over cybercrimes in national law. For example, Botswana can assert jurisdiction over a cybercrime committed in its territory or in part of its territory; when the cybercrime involves one of its nationals outside of its territory if the national's conduct would constitute an offence under the law of the country where the offence was committed and if the person has not been prosecuted for the offence in that country; when the offence was committed on a ship or aircraft registered in Botswana; and if the offence was committed outside of its territory but had an impact on Botswana.[316]

[312] See also UNODC, Education for Justice University Module Series, Cybercrime, Module 7: international cooperation against cybercrime, "Sovereignty and jurisdiction"; and Module 3: legal frameworks and human rights, "The role of cybercrime law". Available at www.unodc.org/.

[313] Ibid.

[314] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime* (Vienna, 2016), pp. 75–80.

[315] Ibid., para. 248.

[316] Botswana, Cybercrime and Computer Related Crimes Act, 2018, sect. 3.

United States v. Aleksey Vladimirovich Ivanov, 175 F. Supp. 2d 367 (2001) (United States of America)

The defendant illegally accessed a corporation in the United States that hosted websites and processed financial transactions of retail establishments. The corporation collected and stored financial data of customers, merchants and financial institutions. The defendant hacked the computer system of the corporation. This illegal access enabled him to obtain passwords, which afforded him the opportunity to control the corporation's entire network. The defendant informed the corporation of his access and sought to extort money by threatening to damage the computer systems if he was not paid to assist the corporation in securing their systems. For his crimes, he was sentenced to four years' imprisonment and three years' supervised release after serving his sentence.[a]

When the defendant hacked the systems of the corporation and engaged in extortion, he was physically located in the Russian Federation. The court asserted that the United States had jurisdiction because the adverse impact of the defendant's actions occurred in the United States and because of the extraterritorial effect of the laws that he was charged with violating. Therefore, the United States claimed jurisdiction over an act that had had an impact on its territory, although the act had been perpetrated in a different country.

[a] United States Attorney, District of Connecticut, "Russian man sentenced for hacking into computers in the United States", press release, 25 July 2003.

B. Identification, tracing, freezing or seizure of assets and confiscation of proceeds of crime

In addition to the criminal convictions of offenders, the freezing or seizure[317] of assets (e.g., cash, movables, such as automobiles, boats, aircraft, businesses and shares) and confiscation[318] of the proceeds of the crime[319] are essential in order to prevent offenders from profiting from transnational organized crime. In the Phantom Secure case (see chap. IV), the founder and chief executive officer of the company received for his crimes a sentence of nine years of imprisonment and supervised release and was required to forfeit US$ 80 million, as proceeds of crime, as well as other identified assets (funds held in international bank accounts, a luxury automobile, real estate, virtual currencies (including cryptocurrencies) and gold coins).[320] In other cases included in this digest, the domain names were also seized and forfeited.[321] Technological devices

[317] According to article 2, paragraph (f), of the Organized Crime Convention, "freezing" or "seizure" refers to "temporarily prohibiting the transfer, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority".

[318] According to article 2, paragraph (g), of the Organized Crime Convention, "confiscation", which includes forfeiture where applicable, refers to "the permanent deprivation of property by order of a court or other competent authority".

[319] According to article 2, paragraph (e), of the Organized Crime Convention, the term "proceeds of crime" refers to "any property derived from or obtained, directly or indirectly, through the commission of an offence".

[320] *United States of America v. Vincent Ramos et al.* (2019). Fiat currency, bitcoin accounts, real property and vehicles, among other assets, were also seized and forfeited in other cases included in this digest (see, for example, *United States of America v. Beniamin-Filip Ologeanu et al.*, p. 31; *United States of America v. Sergey Medvedev*; *United States of America v. Valerian Chiochiu*.

[321] See, for example, United States District Court, District of Arizona, *United States of America v. Carl Allen Ferrer*, Case No. 18-CR-464, 5 April 2018; United States District Court, Southern District of New York, *United States v. Liberty Reserve*, 13 CR. 368, 23 September 2015.

(e.g., mobile phones, computers and SIM cards), firearms and other forms of property have also been forfeited.[322] Confiscation of the proceeds of crime is intended to deter transnational organized crime by removing the incentives for committing such crime.[323]

Regina v. Bradley David Rogers, Colin Martin Samuels, Geraldine French, Mark Julian Bell [2014] EWCA Crim 1680 (United Kingdom)

Four appellants, B.D.R., C.M.S., G.F. and M.J.B., were charged with and convicted for their roles in two advance fee frauds. Both frauds were orchestrated and organized by M. (not included in the appeal), who pleaded guilty to charges of conspiracy to defraud and was sentenced to seven years and five months of imprisonment.[a] M. employed nationals of the United Kingdom at call centres in Spain or Turkey in advance fee fraud schemes involving either debt elimination or escort services. The debt elimination and escort services were promoted and advertised online on websites and offline in the national press. Consumers in the United Kingdom responded to these advertisements and paid an advanced fee to receive the advertised services. In the fraud scheme involving escort services, the consumers were asked to pay a registration fee in order to secure a date and obtain escort services. Once the so-called registration fee was paid, the date with the escort was cancelled and no other dates were made available. The debt elimination fraud involved employees from the call centres cold-calling consumers in the United Kingdom from a list that the centres had purchased from data providers. For a fee, consumers were fraudulently promised the elimination of their debt.

Three of the appellants, C.M.S., G.F. and M.J.B. were charged with and convicted of conspiracy to defraud and received sentences of 5 years and 6 months of imprisonment, 6 years and 5 months of imprisonment and 6 years and 6 months of imprisonment, respectively. The other appellant, B.D.R., was convicted of converting criminal property contrary to the Proceeds of Crime Act 2002, for which he received a sentence of 2 years and 10 months of imprisonment. B.D.R. appealed his conviction, arguing that the Proceeds of Crime Act 2002 did not have an extraterritorial effect. The appellant argued that the acts that had led to the property becoming "criminal property" took place outside of the United Kingdom and had had impacts on victims outside the United Kingdom. The court disagreed; it held that the mechanics of the fraud had taken place in the United Kingdom and had had impacts on victims in the United Kingdom. If the mechanics of the fraud had occurred in Spain and had had impacts on Spanish victims, the court would not claim jurisdiction over the crime. However, that was not the case. The acts had predominantly taken place in England, including the deprivation of British victims' monies. The court thus held that there was jurisdiction to apply the provisions of the act, particularly the money-laundering provisions under section 340, paragraph (11) (d), of the Proceeds of Crime Act 2002. The funds that had been obtained pursuant to the advance fee frauds in the United Kingdom became criminal property[b] once they reached a bank account in the United Kingdom controlled by the conspirators, and those proceeds did not cease to be criminal property when they arrived in the appellant's bank account in Spain.[c] Accordingly, the court dismissed the appeal of B.D.R, as well as the appeals of the other appellants.

For more information on this case, see UNODC, SHERLOC case law database, Case No. GBRx095.[d]

[a] England and Wales Court of Appeal, *Regina v. Bradley David Rogers, Colin Martin Samuels, Geraldine French, Mark Julian Bell* [2014] EWCA Crim 1680, p. 1.

[b] According to section 340, paragraph (3) (a), of the Proceeds of Crime Act 2002, property is criminal property if it constitutes "a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly)".

[c] *Regina v. Bradley David Rogers, Colin Martin Samuels, Geraldine French, Mark Julian Bell*, p. 7.

[d] Available at https://sherloc.unodc.org/.

[322] See, for example, United States District Court, Western District Court of North Carolina, *United States of America v. Anthony Blane Byrnes*, Case No. 3:20-CR-109-KDB, p. 2; *United States of America v. Andrii Kolpakov; United States of America v. Fedir Oleksiyovich Hladyr*, Case No. CR17-276RSM. According to article 2, paragraph (d), of the Organized Crime Convention, "property" refers to "assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets".

[323] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime*, para. 330.

Article 12 of the Organized Crime Convention requires States parties to the Convention to establish measures to enable the confiscation of criminal proceeds and any "property, equipment or other instrumentalities used in or destined for use in offences". The recommendations of the Financial Action Task Force serve as a framework of measures that facilitate international cooperation on matters relating to criminal assets and proceeds, which authorities can implement in their own countries according to their national laws.[324] The Stolen Asset Recovery initiative, developed by the World Bank and UNODC, also provides guidance on how to respond to criminal proceeds.[325] The above-mentioned convention, recommendations, guidance and initiative identify the measures needed to investigate and prosecute transnational organized crime and to identify and confiscate the proceeds of such crime.

The Organized Crime Convention obligates States to adopt the measures needed to empower competent authorities to order that bank, financial or commercial records be made available or seized for the purpose of identifying and freezing assets and ultimately confiscating the proceeds of organized crime.[326] The Convention also requires States to respond to requests for the identification, tracing and freezing or seizure of such proceeds.[327] In addition, the Convention sets out the procedures that need to be followed in order to confiscate such proceeds.[328] Mutual legal assistance (see the discussion in chap. VI, sect. E.2) can be sought to obtain evidence and information relating to the identification, tracing, freezing, seizure and confiscation of proceeds of such crime.[329]

The freezing or seizure of value- or property-based assets that have been identified as being directly or indirectly derived from transnational organized crime, as well as the confiscation of the proceeds of such crime, is a complex process. This complexity arises from the variation in national laws and the methods and approaches taken by countries to identify, trace, freeze or seize assets, as well as the conditions that are in place to confiscate the proceeds of crime.[330] For example, the authorities that authorize freezing or seizure orders,[331] as well as the criteria and conditions that must be met for those orders to be issued, vary between countries. Variations also exist between countries with respect to data protection and controls regarding the disclosure of personal and financial information relating to the identification of criminals, their assets and the proceeds of their crimes.

C. Special investigative techniques

Special investigative techniques include electronic surveillance, undercover operations and controlled delivery. They are critical to the effective investigation and prosecution of cyber organized crimes. Special investigative techniques are deployed because of the transnational nature of such crimes, difficulty in infiltrating cyber organized criminal groups and difficulty in gathering information about such groups and evidence of their crimes for use in prosecutions. Such techniques enable law enforcement agencies to conduct investigations remotely and collect the evidence needed to ensure that the perpetrators are arrested and prosecuted for the crimes they commit.

Cyber organized crime predominantly transcends borders, requiring cooperative efforts between law enforcement agencies. Transnational investigations conducted for this type of cybercrime often involve the use of special investigative techniques. Because criminal procedure law and rules of evidence regulating special investigative techniques often differ from country to country, cooperation in investigations involving these techniques may be hampered.

---

[324] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (Paris, 2012–2020), updated June 2021.

[325] See **https://star.worldbank.org/**.

[326] Organized Crime Convention, art. 12.

[327] Ibid., art. 13.

[328] Ibid.

[329] Ibid., art. 13, para. 3.

[330] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime*, paras. 331–332; UNODC, *Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime* (Vienna, 2012).

[331] A "freezing order" refers to "an order (usually judicial) that leaves physical possession of the asset with the owner or a third party but imposes specific terms and conditions on their use of the asset, or prohibits any right to sell, lease, destroy or otherwise diminish the value of the asset while the order is in force". It is also called a "restraint", "blocking", "attachment" or "preservation" order in some jurisdictions (UNODC, *Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime*, p. 3).

Special investigative techniques are considered an important tool in the arsenal of measures that may be used to combat cyber organized crime. The techniques are labelled "special" because their use is often costly and complicated, requiring specialized expertise and sometimes advanced technological knowledge and instruments. Their use may in some cases pose ethical problems, while in others it may endanger the operators. It is important to keep in mind that the use of special investigative techniques may infringe on fundamental individual rights (e.g., the right to privacy).[332]

1. Electronic surveillance

Electronic surveillance involves the use of ICT to monitor and maintain surveillance of suspects and their movements and to intercept suspects' communications. Basically, the suspect's behaviours, movements and communications are kept under surveillance.[333] Electronic surveillance involves the use of ICT to monitor communications and movements, intercept telecommunications and electronic communications (telephone calls, email messages and other messages), track individuals and devices, create audio and video recordings, etc.

Electronic surveillance has been used by law enforcement agencies in cases involving cyber organized crime. This special investigative technique has been used during investigations of cyber-dependent crimes and cyber-enabled crimes.[334] Electronic surveillance is usually regulated by warrants.[335] The legal order is obtained prior to collecting electronic evidence in order to ensure that the evidence is admissible in a court of law. In the event that a warrant is not required for the surveillance, there are limiting factors to prevent its arbitrary and illegal use (e.g., privacy considerations, subject notification or the requirement to obtain non-judicial permission).[336]

Electronic surveillance is quite intrusive, and its legality varies by jurisdiction. Countries have different requirements for the use of various forms of electronic surveillance (e.g., audio, visual, tracking and data surveillance) and have statutory safeguards in place to ensure that the measures taken are respectful of the rule of law and human rights. Therefore, before using electronic surveillance, national laws, as well as regional and international laws, and human rights obligations (particularly with respect to the right to privacy) need to be considered.

If the investigation involves the monitoring of Internet chat rooms, social networking sites or other sites, the human rights implications of this monitoring may vary, depending on the privacy and security settings and law enforcement activities on those sites. If the content and activities that are monitored in chat rooms or social media or other sites are accessible to the public and if privacy and security settings have not been set to restrict access to content, then there is no reasonable expectation of privacy over this content.[337] If, however, privacy and security settings have been set to restrict access to content to specific persons, then the user has a reasonable expectation of privacy over their content and activities.[338] If law enforcement agents interact and/or otherwise engage with persons on these sites, countries often require a legal order (e.g., a search warrant) to authorize the gathering of information about the target through an undercover operation (for more information about undercover operations, see the subsection that follows).

---

[332] UNODC, *Digest of Organized Crime Cases: A Compilation of Cases with Commentaries and Lessons* (Vienna, 2012), para. 99.

[333] Ibid., p. 43.

[334] See, for example, Canada, Ontario Court of Justice, *R. v. Kalonji* and Germany, LG Limburg, Urteil vom 07.03.2019, 1 KLs - 3 Js 73019/18.

[335] See, for example, the Surveillance Devices Act of 2004 of Australia; the Criminal Procedure Code of Germany, sect. 100a; Interception of Communications and Surveillance Ordinance of Hong Kong, China, chap. 589, sect. 3; the Crimes Act 1961 of New Zealand, part 11A; the Code of Criminal Procedure of Poland, chap. 26; the Criminal Procedure Code of Serbia, arts. 226 and 228; the Code of Criminal Procedure of Slovakia, sect. 88; the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002, of South Africa; and the Regulation of Investigatory Powers Act 2000 of the United Kingdom (*Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime* (United Nations publication, 2009), p. 13).

[336] Ibid., p. 14.

[337] For further information, see United States, Global Advisory Committee, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* (February 2013); Maras, *Computer*; Berkman Center for Internet and Society, Harvard Law School, Berkman Online Lectures and Discussions, Privacy in cyberspace: module IV – governmental collection of data, part I. Available at **https://cyber.harvard.edu/privacy/module4.html**.

[338] Ibid.

BGH, Beschluss vom 15.01.2020, 2 StR 321/19

This case involved two darknet platforms (Elysium and the Giftbox Exchange) dedicated to the sharing of child sexual exploitation material. The four defendants (M., Mä., G. and P.) had been part of the online paedophile community before they joined several other separately prosecuted offenders to create private forums and chat rooms. After registering on these forums, the defendants and other unnamed conspirators undertook a number of tasks necessary for the operations of both the Elysium and the Giftbox Exchange sites. The purpose of these operations was to facilitate the exchange of child sexual abuse material involving children of different genders and ages between members of the sites.

The first site that was created was the the Giftbox Exchange. P. helped to create and manage it. Access to it was limited to registered users. In order to register, prospective users had to upload illegal material in order to minimize the risk of undercover law enforcement agents accessing the site. Likewise, users were required to publish child sexual abuse material at least once a month to have complete access to the content on the forum. The Giftbox Exchange platform had a strict hierarchical structure. There were several administrators of the site, one of them being P. The administrators, with full access to the boards, undertook administration and maintenance tasks to guarantee the faultless operation of the site on a technical and content-related scale. The administrators were supported in running the site by 10 moderators. Members that had risen to the ranks of administrator or moderator had the additional responsibility of posting illegal material on a monthly basis. The Giftbox Exchange chat rooms had a hierarchical structure comparable to that of the forum.

P. was responsible for programming relating to the chats, the recruitment of new members and the allocation of accounts, in addition to informing members of the forum rules and maintaining the Giftbox Exchange servers. G. was a chat moderator who was later "promoted" to lead chat moderator and then chat administrator, where he was responsible for all matters regarding the chat rooms, including the recruitment of chat room personnel. He acted as the point of contact for staff members. He also created the seasonally changing background graphics of the chat rooms. He also undertook other tasks in relation to the forum, including the translation of the rules into German. M. was a chat moderator who was responsible for user support and supervision, as well as the supervision of the chat rooms themselves, mainly to ensure compliance with the forum rules. In addition, M. worked on testing new chat scripts, together with P., and translated into German the security instructions of the forum. Mä. was a "registeredplus-member", and he exercised moderator functions if no other staff member was online. He could issue warnings and block users if necessary. Mä. also worked on testing chat scripts and translating the instructions by proofreading the translation created by M. As part of the posting and verification duties, defendants M., G. and P. posted child sexual abuse material and child sexual exploitation material in order to make the material accessible to users of the forums, as well as to encourage other users to share material.

In this case, the court of first instance discussed the composition of organized criminal groups on the darknet. In examining the roles of the defendants and their tasks, the court held that the defendants, as well as each member registered on the forums or the chat rooms of the platform, were considered members of an organized criminal group. The court held that the members of the platforms had implicitly joined the organized criminal group of the defendants by registering for the forums. The members came together with the intent to independently commit numerous, and at the time of registration, unknown offences of the same type of crime for a certain period of time in the future. Through their actions, the defendants, as well as all registered members, aimed at obtaining child abuse and exploitation material not yet in their possession and to exchange views on topics including paedophilia and child abuse. The court also held that the fact that the members of the organized criminal group did not know each other personally and communicated with nicknames or pseudonyms was irrelevant to their classification as an organized criminal group.

BGH, Beschluss vom 15.01.2020, 2 StR 321/19 (*continued*)

In the course of investigations, investigating police were able to associate the forum with an Australian hosting provider. In Australia, Task Force Argos of the Queensland Police Service was able to seize the data of the forum, including threads, postings and not yet deleted messages, and take over the operation of the platform. P. noticed that something was wrong and – via the darknet – warned users not to visit the Giftbox Exchange. Furthermore, he backed up the data of the platform and tried to close the server. The same persons responsible for running the Giftbox Exchange then created a new platform, Elysium, under the leadership of P. In order to log in to the platform and have unlimited access to content, registration was again required. The obligation to post material for verification purposes was, however, not introduced, which led to the registration of a large number of users within a short period of time.

After locating the server of the Elysium platform, law enforcement authorities conducted electronic surveillance of the server and of one defendant, M., as well as undercover operations. The surveillance measures included uploading avatar (or user profile) images to confirm the server location, as well as the monitoring of messages. This electronic surveillance helped to identify defendants M. and Mä., which subsequently led to the identification of P. In addition, the Federal Criminal Police Office of Germany obtained child sexual abuse images involving G., which ultimately led to the identification of G.

M. was charged with and convicted of ring-based dissemination of child sexual abuse material; procuring, for another, child sexual abuse material; production of child sexual abuse material; and aggravated child sexual abuse in conjunction with procurement of child sexual abuse material,[a] for which he received a sentence of 8 years' imprisonment. Mä. was charged with and convicted of ring-based dissemination of child sexual abuse material and possession of child sexual abuse material. He received a sentence of 3 years and 10 months of imprisonment. G. was charged with and convicted of ring-based dissemination of child sexual abuse material; procuring, for another, child sexual abuse material; production of child sexual abuse material; and aggravated child sexual abuse in conjunction with procurement of child sexual abuse material.[b] For those offences, he was sentenced to 9 years and 9 months of imprisonment; however, that sentence was reduced to 8 years and 7 months of imprisonment given the reversal of the conviction for aggravated child sexual abuse in conjunction with procurement of child sexual abuse material on appeal. Finally, P. was charged and convicted of ring-based dissemination of child sexual abuse material and ring-based procurement, for another, of child sexual abuse material.[c] He received a sentence of 6 years and 6 months of imprisonment.

For more information on this case, see UNODC, SHERLOC case law database, Case No. DEUx024.[d]

[a] In the court of first instance, M. was also charged with and convicted for the possession of child sexual abuse material. That conviction was subsequently reversed on appeal.
[b] G. was also charged with and convicted for other crimes. Those convictions were subsequently reversed on appeal.
[c] In the court of first instance, P. was also charged with and convicted for the possession of child sexual abuse material. That conviction was subsequently reversed on appeal.
[d] Available at https://sherloc.unodc.org/.

2. Undercover operations

An undercover operation involves the use of an undercover agent, an informant (i.e., a person who provides information about a crime or suspect) or some other person to infiltrate an organized criminal group. Informants may or may not be criminals. They are used in undercover operations because they can provide access to closed organized criminal groups, places or spaces where members of those groups gather and/or where the group members engage in and/or conspire to commit transnational organized crime. Undercover operations are difficult and risky for those involved, and they require a significant investment in time and in human, financial and technical resources.

The purpose of undercover operations is to gather evidence of crimes planned and those committed and to obtain insight into the structure, organization and roles and/or identities of members of the organized criminal group. In one case in the United States, a female victim of an international romance fraud notified law enforcement authorities of the incident.[339] An agent of Homeland Security Investigations, the investigative component of the Department of Homeland Security of the United States, posed as the victim and continued to communicate with the perpetrators. The communications helped criminal justice authorities to understand the nature and scope of the international romance fraud and ultimately led to the perpetrators of this fraud being brought to justice.

R v. Mara [2009] QCA 208 (Australia)

The defendant (D.R.M.), along with three others, made up the core members of a group that traded child sexual abuse material via Internet newsgroups. The core members were responsible for reviewing and admitting new members to the group. In addition, they served as "administrators" of the group, along with two other group members. The group's other members (i.e., those who were not part of the core group and did not serve as administrators) were known in the group as "the trustworthy".[a]

No member of the group knew the true identities of the other members – only the nicknames provided by the members. To avoid detection by law enforcement authorities, the nicknames of members and the location of the newsgroup were frequently changed, and members altered filename extensions of child sexual abuse material to hide the true nature of what was being traded. Members of the newsgroup also used encryption, and encryption keys were regularly changed. The child sexual abuse material was traded in the newsgroup as binary files that could not be accessed without a key.[b]

Despite being a member of a group that engaged in serious crime, the defendant was not charged with a crime associated with organized crime, such as participation in an organized criminal group. Instead, the perpetrator was charged with, pleaded guilty to and was sentenced for the following offences:[c]

(a) Use of a carriage service (the Internet) to access child pornography material between 6 January 2006 and 29 February 2008;

(b) Use of a carriage service (the Internet) to cause child pornography material to be transmitted to himself between the same dates;

(c) Use of a carriage service (the Internet) to transmit child pornography material between the same dates;

(d) Recording an indecent visual image of a child under the age of 16 years without legitimate reason between 31 December 2007 and 1 February 2008.

The defendant engaged in these crimes for his own sexual gratification and not for financial reasons. Nevertheless, financial contributions were made by some members of the group to other members when requests were made for custom-ordered child sexual abuse material.[d]

[339] *United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase and Rasaq Aderoju Raheem*, Case No. 17-60397, p. 2.

R v. Mara [2009] QCA 208 (Australia) (*continued*)

In 2006, law enforcement authorities infiltrated the group and conducted an undercover operation that lasted 26 months.[e] At the time of the investigation, there were 43 members of the group.f Even though the defendant cooperated with investigators, the identities of other members of the group could not be determined. The defendant was sentenced to six years' imprisonment. A subsequent appeal lodged by the defendant on the basis that the sentence was manifestly excessive was unsuccessful.

For more information on this case, see UNODC, SHERLOC case law database, Case No. AUSx208.[g]

[a] *R v. Mara* [2009] QCA 208, para. 6.
[b] Ibid., para.7.
[c] Ibid., para. 3.
[d] Ibid., para. 8.
[e] Ibid., para. 9.
[f] Ibid.
[g] Available at https://sherloc.unodc.org/.

Undercover operations can also involve the infiltration of an individual into an organized criminal group or illicit network to participate in its general criminal activity or in a specific illicit business.[340] For example, in the case of the DarkMarket site, an undercover FBI agent, posing as a cybercriminal, infiltrated the site and eventually became one of the site's administrators (i.e., Master Splyntr).[341] In the Phantom Secure case, the Royal Canadian Mounted Police purchased Phantom Secure devices, posed as drug traffickers and, through their undercover operations, were able to establish that the company had tailored its services to criminals.[342] Undercover agents in the United States also posed as drug traffickers, met with the founder and chief executive officer of Phantom Secure and were able to establish that the devices had been created to facilitate serious crime.[343]

The present digest includes many cases in which undercover operations were used, particularly in cases involving cyber-enabled crime.[344] The legality of undercover operations varies depending on the jurisdiction. In most jurisdictions, undercover officers are not allowed to encourage suspects to commit crimes that they would not ordinarily commit, either as an agent provocateur or through entrapment.[345] Countries also place restrictions on the manner in which an undercover operation is conducted and on what those involved in the operation can do (e.g., undercover law enforcement officers may not be allowed to commit any crimes, or they may be allowed to commit only certain crimes). The use of informants is also regulated in order to protect informants and to ensure that guidelines are in place on the use, management, supervision and, where relevant, payment of informants.

[340] UNODC, *Digest of Organized Crime Cases*, p. 42.

[341] United States, Federal Bureau of Investigation, "'Dark Market' takedown: exclusive cyber club for crooks exposed", 20 October 2008.

[342] *United States of America v. Vincent Ramos*, Case No. 3:18-CR-01404-WQH.

[343] Ibid.

[344] See, for example, *United States of America v. Gal Vallerius* (Dream Market); Germany, LG Limburg, Urteil vom 07.03.2019, 1 KLs - 3 Js 73019/18; *United States of America v. Eoin Ling Churn Yeng and Gal Vin Yeo Siang Ann*, Case No. 3:16 CR 00090; *United States of America v. Dylan Heatherly*, No. 19-2424 and *United States of America v. William Staples*, No. 19-2932. There are, however, exceptions. See, for example, *United States of America v. Aleksandr Andreevich Panin and Hamza Bendelladj*, Case No. 1:11-CR-0557-AT-AJB (SpyEye).

[345] CTOC/COP/WG.7/2013/2, para. 18.

3. Controlled delivery

Controlled delivery is defined in the Organized Crime Convention as a technique that allows "illicit or suspect consignments to pass out of, through or into the territory of one or more States, with the knowledge and under the supervision of their competent authorities, with a view to the investigation of an offence and the identification of persons involved in the commission of the offence".[346] This technique was initially used to combat drug trafficking. The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 regulates the use of this special investigative technique for investigating cases involving drug trafficking. In article 1, paragraph (g), of the Convention, "controlled delivery" is defined as a technique allowing illicit or suspect consignments of narcotic drugs, psychotropic substances, substances in Table I or II of the Convention (i.e., precursor chemicals) or substances substituted for them, to pass out of, through or into the territory of one or more countries, with the knowledge and under the supervision of their competent authorities, with a view to identifying persons involved in the commission of offences established in accordance with the Convention.

Controlled delivery is also used in the investigation of other forms of transnational organized crime. This special investigative technique has been used to identify and trace the origin, route and destination of illegal goods and trafficked wildlife. It has also been used where contraband is identified or intercepted in transit and then delivered under surveillance to identify the intended recipients or to monitor its subsequent distribution throughout a criminal organization.[347] While controlled delivery has also been used in cases involving the smuggling of migrants and trafficking in persons, its use for investigating those crimes is problematic and has usually been limited to exceptional circumstances, and it is used only if specific conditions are met (e.g., sufficient safeguards are in place to ensure protection of victims).[348] Overall, the methods that can be used involve intercepting illicit or suspect consignments and doing one of the following: *(a)* allowing them to continue to their destination intact; *(b)* replacing them in whole or in part and then allowing them to continue to their destination; or *(c)* removing the identified illicit or suspect consignments.[349] The legality, conditions and limits for the use of this special investigative technique vary by country.[350]

[346] Organized Crime Convention, art. 2, para. (i).

[347] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime*, para. 443.

[348] Ignacio Miguel de Lucas Martín and Cristian-Eduard Stefan, *Transnational Controlled Deliveries in Drug Trafficking Investigations Manual*, co-funded by the European Commission Directorate-General Migration and Home Affairs, as a result of the project "Enhancing the cooperation of European Union Legal Enforcement Agencies for successful drug controlled deliveries" (JUST/2013/ISEC/DRUGS/AG/6412), pp. 48–49.

[349] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime*, para. 451.

[350] CTOC/COP/WG.7/2013/2, pp. 6–7.

United States v. Anthony Blane Byrnes, Case No. 3:20-CR-192 (W.D.N.C. 2020) (United States of America)

The defendant (A.B.B.) conspired with an organized criminal group (i.e., a regional drug trafficking organization) to distribute and to possess with the intent to distribute controlled substances, such as stimulant and hallucinogenic drugs (e.g., DMT, lysergic acid diethylamide (LSD), 3,4-methylenedioxymethamphetamine (MDMA, commonly known as "ecstasy")).[a] According to the criminal complaint, he came to the attention of law enforcement authorities when United States Customs and Border Protection intercepted a package from Slovenia that was addressed to the defendant. The package was found to contain narcotic drugs. Law enforcement authorities arranged for the controlled delivery of the package to the defendant's address. After law enforcement officers observed the defendant collecting the package and bringing the package into his residence, they executed a search warrant for the defendant's residence. During the search of the defendant's residence, they found and seized different forms of controlled drugs, as well as a firearm and ammunition. The defendant revealed to law enforcement authorities that the controlled drugs had been purchased via the Empire Market darknet site. The defendant also revealed that he had facilitated the purchase of controlled drugs with bitcoins and used his mobile phone and certain phone applications to communicate with other conspirators and otherwise facilitate drug trafficking. He was sentenced to 5 years and 11 months of imprisonment.[b]

[a] United States District Court, Western District of North Carolina, *United States of America v. Anthony Blane Byrnes*, p. 1.
[b] United States Attorney's Office, Western District of North Carolina, "Huntersville, N.C. man is sentenced to prison for trafficking narcotics on the dark web using bitcoin ATMs & virtual wallets", press release, 10 September 2020.

4. Other techniques

Other special investigative techniques include the use of "exploits" (codes that take advantage of software vulnerability or security flaws to allow intruders to remotely access a network and gain elevated privileges), malware and hacking to access sites, servers and tools used by cyber organized criminal groups. Taking advantage of exploits in ICT, hacking and using malware are becoming more commonplace as special investigative techniques in some countries. This, in turn, has raised concern about the impact of these techniques in terms of respect for the rule of law and respect for human rights. One example is the law enforcement operation known as Trojan Shield, in which law enforcement agencies ran a sting operation providing mobile phones that performed a single function hidden behind a calculator app: sending encrypted messages and photographs.[351]

In the United States, these techniques have been labelled "network investigative techniques". Such techniques were used in Operation Pacifier, a law enforcement operation that shut down Playpen, one of the largest sites on the darknet, which had housed child sexual abuse material and child sexual exploitation material. Once the FBI gained access to the Playpen server, it was copied and the FBI continued to operate the Playpen website on its own server. After the FBI agents gained control of the server and the site, they placed malware on a link on the site. Once users clicked on the link, the malware was downloaded on their device and used to identify the IP addresses and ultimately other identifying data of those who had accessed the site and clicked on the link.

The so-called network investigative technique used in the operation that resulted in the Playpen site being shut down has been referred to as a "watering hole attack".[352] The network investigative technique

[351] Yan Zhuang, Elian Peltier and Alan Feuer, "The criminals thought the devices were secure, but the seller was the FBI", *The New York Times*, 9 June 2021.

[352] A "watering hole attack" involves infecting with malware sites most frequented by targets, in an attempt to gain access to the targets' systems, networks and/or data. (Maras, *Cybercriminology*, p. 382).

configured the target server to install software on the devices of users accessing the site.[353] Once downloaded on the user's device, identifying information about the user's device was relayed to the FBI.[354] The information collected from the use of the network investigative technique was used to effectuate the arrest of persons in various countries. In each of the countries, the law enforcement authorities utilized the information obtained using the network investigative technique to arrest perpetrators within their country's borders. Searches based on information obtained from the use of the network investigative technique were thus viewed as permissible by the authorities in those countries. In the United States, certain features of the source code of the network investigative technique are classified and requests to reveal the technique source code have been denied,[355] even when this denial has resulted in the dismissal of charges against defendants.[356] In addition to taking advantage of known software vulnerabilities and/or exploiting "zero-day vulnerabilities" (software vulnerabilities unknown to those interested in fixing them, including the vendor of the software), law enforcement agencies have also used malware such as keylogging software (software recording the keystrokes of users) in investigations of members of organized criminal groups.[357]

D. Collection and use of electronic evidence

There are several challenges to the collection and use of electronic evidence (also known as digital evidence) in criminal proceedings. Before it can be introduced as evidence in a court of law, its authenticity and integrity must be established by examining the processes, methods and tools used in the collection, acquisition, preservation and analysis of the electronic evidence. The volume, volatility, velocity and fragility of data serve as obstacles to introducing the data as evidence in court. Moreover, given the cross-border nature of cyber organized crime and the different legal systems around the world, the rules of evidence vary between countries. This variation serves as an obstacle to the collection, requesting and use of electronic evidence in national courts. What also varies between countries are the conditions and safeguards for the collection and use of electronic evidence in courts of law in a manner that respects the rule of law and human rights. The conditions and safeguards for the collection and use of electronic evidence predominantly require judicial or other independent supervision and delineate and place limits on the procedures, processes, methods and tools used to collect, acquire, preserve and analyse electronic evidence. National laws include provisions on rules of evidence, investigative powers and criminal procedure that relate to data collection and use. Some of these investigative powers and rules are discussed below, particularly the expedited preservation of data, production orders, the real-time collection of data and the interception of content data.

1. Expedited preservation of data

Data preservation seeks to maintain data that are already stored, in order to prevent their deletion or alteration. Data preservation, however, does not require data that are not already being stored to be kept in the future. The stored data sought during an investigation of cyber organized crime may not exist for various reasons. For example, they may not be stored because storing them was deemed unnecessary for business reasons; they may have been deleted; or they may have been overwritten. Data protection laws may also require the deletion of specific data after a period of time. To address these issues, the investigative power of requesting the preservation of data was introduced into multilateral, regional and national laws.

[353] United States District Court, District of South Carolina, *United States of America v. Jamison Franklin Knowles*, 207 F. Supp. 3d 585, 14 September 2016.

[354] Ibid.

[355] See, for example, United States Court of Appeals, Seventh Circuit, *United States of America v. Neil Kienast*, 907 F. 3d 522, 23 October 2018.

[356] See, for example, United States District Court, Eastern District of Virginia, *United States of America v. Gerald Andrew Darby*, Case No. 2:16CR36, Government's response to defendant's motion to compel, 16 June 2016; and United States District Court, Western District of Washington, *United States of America v. Jay Michaud*, Government's unopposed motion to dismiss indictment without prejudice (2017).

[357] United States District Court, District of New Jersey, *United States of America v. Nicodemo S. Scarfo et al.*, 180 F. Supp. 2d 572, 26 December 2001.

The expedited preservation of data applies to stored data, not to the real-time collection of traffic data (i.e., data about communications)[358] or content data (i.e., written or spoken words in communications). Here, only a request is made for the data to continue to be stored. Generally, preserved data cannot be accessed by criminal justice authorities pursuant to this request but a legal order is required in order to access preserved data (i.e., a subpoena, court order or search warrant). Preservation orders do not exist in some countries. In such countries, data can only be preserved and ultimately collected through the use of production orders (discussed in chap. VI, sect. D.2, below) or searches and seizures. Requests for the preservation and production of data may be met with non-compliance, especially if there are concerns about the breadth of the requests (e.g., the requests may not be for data on specific individuals but are blanket requests for data) and their legality (e.g., concerns relating to privacy or other human rights).

To protect the privacy of the subjects of the preservation order, the preserved data are maintained for a limited period of time. This time period varies by country. For example, in Kenya, preserved data are to be maintained for a period of 30 days, whereas in Sri Lanka, they are to be preserved for a period of 7 days.[359] These periods can be extended in many jurisdictions, often with a legal order (e.g., a court order). The Council of Europe Convention, which is intended to serve as a guideline for national legislation and a framework for international cooperation, provides for the preservation of data for a maximum period of 90 days, with the possibility of extension (see art. 16).

2. Production orders

A production order compels the recipient of the order to provide and/or grant access to information (or material) to those requesting it within a specific period of time. The recipient of the order can be an individual within a territory, a service provider[360] within a territory or a service provider that provides services within that territory. Georgia, for example, has an international production order that may be used to empower a Georgian judge to issue a production order in respect of persons or entities outside of the territorial jurisdiction of Georgia if the following conditions are met: agreement of the person who is the subject of the order with the voluntary disclosure of electronic data; and permission from the host country of the foreign entity for such disclosure through its laws or executive policies.[361] Like a preservation order, a production order only applies to data already stored and does not require data about future communications to be stored. The data referred to in the production order are computer data and/or subscriber data (i.e., information held by a service provider that relates to subscribers of its services).[362]

The authority that can compel disclosure of subscriber data varies by country. Some countries (e.g., Australia, Denmark, Finland and the United Republic of Tanzania) provide law enforcement agencies with the authority to order the disclosure of this information, while other countries (e.g., Azerbaijan, Bosnia and Herzegovina, Jamaica and Romania) require prosecutorial or judicial authorization to compel disclosure.[363] Some countries have designated persons or specialized agencies that compel disclosure of subscriber data (e.g., specialized directorates and departments of the state agency in Bulgaria and the State Attorney in

[358] According to article 1, paragraph d, of the Council of Europe Convention on Cybercrime, "traffic data" refers to "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". Similar descriptions are included in national laws, such as the Computer Misuse and Cybercrimes Act, 2018, of Kenya and Republic Act No. 10175 of the Philippines (also known as the Cybercrime Prevention Act of 2012).

[359] Kenya, Computer Misuse and Cybercrimes Act, 2018; Sri Lanka, Computer Crime Act No. 24 of 2007; A/74/130, paras. 349–361.

[360] A public or private entity that provides telecommunication and electronic communication services.

[361] A/74/130, para. 109.

[362] According to article 18, paragraph 3, of the Council of Europe Convention on Cybercrime, the term "subscriber information" refers to 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 geographical address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; and (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. Similar descriptions are included in national laws, such as the Computer Misuse and Cybercrimes Act, 2018, of Kenya and the Cybercrime Prevention Act of 2012 of the Philippines.

[363] Cybercrime Convention Committee, *Rules on Obtaining Subscriber Information,* report adopted by the Cybercrime Convention Committee at its 12th Plenary (Strasbourg, France, 2–3 December 2014), pp. 17–20; United Republic of Tanzania, Cybercrimes Act of 2015; Jamaica, Cybercrimes Act of 2015.

Croatia).[364] In other countries (e.g., Austria), the authorizing agency depends on the type of subscriber data.[365] Some countries have different requirements for obtaining communication traffic data (e.g., rather than police obtaining access to such data, judicial authorization is required).[366] These countries view the interference with the rights of individuals to be substantially different when obtaining subscriber information than when obtaining communication traffic data. For this reason, different rules apply for obtaining such information.[367] Overall, the conditions for compelling disclosure and/or obtaining subscriber information and communication traffic data differ from country to country.

Tribunal Penal del Tercer Circuito Judicial de San José, Causa penal número 15-001824-0057-PE & Causa Penal número 19-000031-0532-PE (Operación R-INO) (Costa Rica)

A criminal group (R.Z.R., L.G.G., J.M.R.F., V.V.C., E.D.S.C. and J.T.N.R.) with a structured division of roles and with members from Brazil, Costa Rica and Mexico was dedicated to producing, disseminating and commercializing child sexual abuse material and child sexual exploitation material on different websites. The members of the criminal group in Mexico (R.Z.R., L.G.G. and J.M.R.F.) were Mexican nationals. R.Z.R. was the head of the organization in Mexico. L.G.G., his wife, was in charge of making payments (through a well-known money transfer service) to E.S.C., who was located in Costa Rica, for the logistics of the production of child sexual abuse material. J.M.R.F. was in charge of transferring money obtained from the commercialization of the child sexual abuse material and child sexual exploitation material on their websites to accounts in Texas and to bank accounts in Mexico City. V.V.C., a Mexican national operating from Brazil and Mexico, was in charge of recruiting victims and producing child sexual abuse material and/or child sexual exploitation material. The recruitment of victims, mostly minors, took place through a modelling agency, promoting castings through social networking sites. Several photographers conducted auditions with minors and produced child sexual abuse material involving girls for distribution on websites. The other two members, E.D.S.C. and J.T.N.R., were located in Costa Rica. E.D.S.C. was responsible for creating and registering different websites, whereas J.T.N.R. was responsible for recruiting victims and producing child sexual abuse material and/or child sexual exploitation material.

The members of the organized criminal group created various pages redirecting users to other sites to ensure that the web pages of the sites containing child sexual abuse material and/or child sexual exploitation material were restricted in the public IP addresses assigned to Costa Rica so that they could be accessed only from abroad. In this way, they tried to control their visibility and cover the traces of the crime. Membership rights to access the content were paid through a separate website (**www.support-gurus.com**) via encrypted online transactions. The membership cost was US$ 30 a month for accessing material that included child sexual abuse and exploitation images and video recordings.

The investigation was carried out by the human trafficking and migrant smuggling unit of the judicial investigation agency of Costa Rica. The investigation of the Internet domains resulted in the identification of 41 websites on which material involving the sexual abuse of girls from Brazil, Costa Rica and Mexico was commercialized. Some of the websites were registered by individuals from those three countries, which allowed each of the members of the organized criminal group to be identified. The sites on the dark web were accessed using Tor, due to geo-blocking (technology that restricts access to Internet content on the basis of the user's geographical location). An undercover agent used a fictitious email address to create an account and access the sites. A significant amount of child sexual abuse material and child sexual exploitation material was downloaded and used as evidence for the case.

[364] Cybercrime Convention Committee, *Rules on Obtaining Subscriber Information*.
[365] Ibid.
[366] Ibid., pp. 26–28.
[367] Ibid., p. 28.

Tribunal Penal del Tercer Circuito Judicial de San José, Causa penal número 15-001824-0057-PE & Causa Penal número 19-000031-0532-PE (Operación R-INO) (Costa Rica) (*continued*)

For the first time in Costa Rica, raids were carried out on websites by means of a court order (decision made by a judge of the Republic).

On 2 February 2017, an application was sent to the Ministry of Public Security for authorization by the computer crime section of the judicial investigation agency to enter the investigated websites. Subsequently, a request was made to extend the authorization to allow access to and the examination and collection of child sexual abuse material and/or child sexual exploitation material. This is referred to as the jurisdictional order of the criminal judge of San José for authorization to access, examine and obtain material with child pornographic content from Internet websites. This request indicated the reasons why it was necessary to expand the search and obtain the material.

On 15 March 2017, a fiscal request and jurisdictional order of the criminal judge of San José was submitted by the Ministry to the criminal court to allow sexual abuse material to be accessed on and obtained from the websites. The request was approved and ordered by the judge.

Only two members of the organized criminal group were prosecuted in Costa Rica (E.D.S.C. and J.T.N.R.). E.D.S.C. was sentenced to 39 years' imprisonment for several charges relating to criminal association, trafficking in persons, child sexual abuse and production and distribution of child sexual abuse material and child sexual exploitation material, among other offences. J.T.N.R. received 149 years and 4 months of imprisonment for several charges relating to criminal association, production and distribution of child sexual abuse material and child sexual exploitation material, and trafficking in persons, among other offences. J.T.N.R.'s sentence was subsequently reduced to 28 years' imprisonment.

For more information about this case, see UNODC, SHERLOC case law database, Case No. CRIx007.[a]

[a] Available at https://sherloc.unodc.org/.

3. Real-time collection of communication traffic data

Real-time collection of communication traffic data involves obtaining currently generated communications at the time the communications are taking place. A copy of the data is made during the collection process. The real-time collection of data lasts for a specific period of time.[368] This process does not prevent data from reaching the intended recipients. The targets of the real-time collection of such data are not notified of the surveillance, at least not when the surveillance and investigation are still in progress.[369] Several national laws include provisions that require service providers and other individuals involved in the investigation, collection and provision of data to keep confidential the investigation, surveillance, targets of the data collection and/or the type of information sought.[370] Service providers are only required to collect data in real time if they have the technical and human capabilities to do so.[371]

[368] Generally, the period of time is included in national laws. For example, in Pakistan the period of time for real-time collection of data is set at seven days (see section 36 of the Prevention of Electronic Crimes Act of 2016).

[369] Certain countries have provisions in law to contact the targets of the collection after the fact (for example, Georgia, the Republic of Moldova, and Ukraine). For more information, see Council of Europe experts under the Cybercrime@EAP III project, *Conditions and Safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership* (May 2018).

[370] See, for example, Sri Lanka, Computer Crimes Act No. 24 of 2007, sect. 24; United Republic of Tanzania, Cybercrimes Act of 2015, sect. 21; and Pakistan, Prevention of Electronic Crimes Act of 2016, sect. 38.

[371] See, for example, Mauritius, Computer Misuse and Cybercrime Act 2003, sect. 15, para. 1.

The real-time collection of communication traffic data affects the privacy rights of those targeted by this investigatory power. Privacy is a fundamental human right that is enshrined in human rights treaties, such as the Universal Declaration on Human Rights (art. 12), the European Convention on Human Rights (art. 8), the International Covenant on Civil and Political Rights (art. 17) and the American Convention on Human Rights (art. 11). An important element of this right is data protection. Traffic communication data can reveal private information, especially when the data are consolidated. For this reason, many countries have implemented limits and safeguards regarding the use of these powers (for more information, see chap. VI, sect. D.4, below).

United States v. Steven W. Chase, Case No. 5:15-CR-00015 (W.D. North Carolina, 8 May 2017) (United States of America)

The defendant, S.W.C., created and served as the administrator for Playpen, a darknet bulletin board and website dedicated to trade in child sexual abuse material. Users of Playpen were able to anonymously exchange and purchase illicit material via bulletin boards and communicate with other users via forums, subforums and private messaging. On the site, child sexual abuse material was organized by age and gender of the victim (including male and female toddlers, prepubescents and pubescents) under different "boards".

As an administrator of the site, S.W.C. ran the site and was responsible for tasks such as handling the technical needs of the site, hosting the site, developing and enforcing the rules of the site, admitting new members and deleting existing members.[a] Playpen also had moderators who were responsible for deleting content deemed to be not relevant or inappropriate, moving content to the appropriate forum if it was posted in the wrong location and banning users for violating the rules of the site.[b]

S.W.C. was charged with and tried and convicted for engaging in a child exploitation enterprise (United States Code, Title 18, sect. 2252A (g)), advertising child sexual abuse material (Title 18, sect. 2251 (d) and (e)), transporting child sexual abuse material (Title 18, sect. 2252A (a), para. (1), and (b), para. (1)), and possessing child sexual abuse material that involved a prepubescent minor or a minor under 12 years of age (Title 18, sect. 2252A (a), para. (5)(B), and (b), para. (2)).[c] He was sentenced to 30 years' imprisonment for engaging in a child exploitation enterprise and for advertising child sexual abuse material and to 20 years' imprisonment for transporting child sexual abuse material and possessing child sexual abuse material involving a prepubescent minor or a minor under 12 years of age.[d] Since his sentences run concurrently, he will serve 30 years' imprisonment for his crimes. Another administrator of the site (M.M.F) and a so-called "global moderator" (D.B.), who pleaded guilty to engaging in a child exploitation enterprise, likewise received lengthy terms of imprisonment (i.e., 20 years).[e] Other members of the site have also been prosecuted in separate cases.[f]

After S.W.C's arrest, the server in North Carolina, where Playpen was hosted, was seized by the FBI and a copy of the server was made on a government-controlled server located in Virginia. The FBI also obtained legal authorization – a search warrant – to use a network investigative technique. The FBI further received judicial authorization in the form of a wiretap authorization (i.e., a "Title III[g] authorization") to monitor Playpen site users for a limited period of time. The court-authorized network investigative technique enabled the FBI to identify users of the site – their identities and locations. To assist in the identification of the users of the devices that accessed Playpen by entering the site through their registered account (as well as the users' location), IP addresses and media access control addresses (in addition to other information) were collected.[h] The monitoring of all of Playpen's postings and messages was conducted by the FBI in accordance with Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[i] These court authorizations, therefore, legally enabled the FBI to obtain real-time communication traffic data and content data (for more information on the real-time collection of content data, see chap. VI, sect. D.4, below).

***United States v. Steven W. Chase*, Case No. 5:15-CR-00015 (W.D. North Carolina, 8 May 2017) (United States of America) (*continued*)**

For further information about this case, see UNODC, SHERLOC case law database, Case No. USAx151.[j]

[a] United States District Court, Western District of North Carolina, *United States of America v. David Lynn Browning*, Case No. 3:15MJ279, Affidavit of Karlene Clapp in support of complaint and arrest of David Lynn Browning, 29 July 2015, para. 10.
[b] Ibid.
[c] United States District Court, Western District of North Carolina, *United States of America v. Steven W. Chase*, Case No. 5:15-CR-00015-001.
[d] Ibid., p. 1.
[e] United States District Court, Western District of North Carolina, *United States of America v. David Lynn Browning*, Case No. 5:15 CR 15-RLV, Plea Agreement, 10 December 2015; *United States of America v. Michael Fluckiger*, Case No. 5:15 CR 15-RLV, Plea Agreement, 24 November 2015.
[f] See, for example, United States Court of Appeals, Fifth Circuit, *United States of America v. Daryl Pawlak*, Case No. 17-11339, 15 August 2019.
[g] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (also known as the Wiretap Act).
[h] United States District Court, Eastern District of Virginia, *In the matter of the search of computers that access upf45jv3bziuctml.onion*, Case No. 1:15-SW-89, 20 February 2015, p. 25.
[i] United States District Court, Western District of North Carolina, *United States of America v. Steven W. Chase*, Case No. 5:15-CR-15-RLV, 1 September 2016, p. 9.
[j] Available at https://sherloc.unodc.org/.

4. Interception of content data

In some countries, a distinction is made between real-time collection of communication traffic data and real-time interception of content data. Several countries distinguish between real-time collection of these two types of data by requiring different legal prerequisites to authorize the use of investigatory powers for the real-time collection of traffic data and content data.[372] Certain countries even stipulate the crimes for which these investigatory powers would be authorized.[373] Generally, real-time interception of content data is authorized only for serious crimes, as defined in national laws. Other countries[374] do not distinguish between real-time collection of traffic data and interception of content data and do not have different legal requirements for the real-time collection of traffic data and content data.

The interception of content data interferes with the privacy of communications. Because it is a privacy-invasive measure, safeguards and limits have been placed on its use in investigations in national law. Important limits that have been identified in national law and human rights case law are: the time limits placed on the use of these powers; restriction of the use of these powers to certain serious crimes; limiting the use of these powers to specific individuals being investigated for serious crimes; and the use of these powers as a last resort, when other less invasive means are not as effective.[375] Essential safeguards in national law for the use of this investigatory power are legal orders (i.e., search warrants and wiretaps) and judicial or other independent supervision.[376] In Australia, for example, safeguards include requirements for the judicial authority to exercise power, parliamentary reporting requirements, the right of defendants to challenge the admissibility of evidence and the right of review, and the oversight of all telecommunications warrants

[372] For more information, see Council of Europe experts under the Cybercrime@EAP III project, *Conditions and Safeguards under Article 15 of the Convention on Cybercrime.*

[373] Ibid.

[374] For example, Armenia and Azerbaijan (see Council of Europe experts under the Cybercrime@EAP III project, *Conditions and Safeguards under Article 15 of the Convention on Cybercrime*).

[375] For example, the time limit in Georgia and the Republic of Moldova is one month; in Ukraine, two months; and in Armenia and Azerbaijan, six months. Provisions in law also enables the extension of the period of interception under certain circumstances (Council of Europe experts under the Cybercrime@EAP III project, *Conditions and Safeguards under Article 15 of the Convention on Cybercrime*).

[376] See, for example, national laws in Belarus, Georgia and Sri Lanka (Council of Europe experts under the Cybercrime@EAP III project, *Conditions and Safeguards under Article 15 of the Convention on Cybercrime*; Sri Lanka, Computer Crime Act No. 24 of 2007).

by the Commonwealth Ombudsman.[377] Both the real-time collection of communication traffic data and the interception of content data are considered special investigative techniques (see chap. VI, sect. C, above).[378] In some countries,[379] notification for the real-time collection of traffic data and/or the interception of content data is not required.

Tribunal de grande instance de La Roche-sur-Yon, 24 septembre 2007 (France)

In 2006, an organized criminal group consisting of six identified members perpetrated a romance scam using dating websites. Members of the group would pass as a woman having recently inherited money and needing help to get the money from Nigeria to France. They would offer 25 per cent of the inheritance in exchange for help in obtaining a suitcase containing the inheritance in banknotes that had been physically darkened for protection from theft. The group would forge documents showing that the suitcase had passed customs and would arrange to meet the victims in person to hand over the suitcase. The leader of the group would pretend to be a diplomat, while other group members would cover different roles functional to the scam, acting as, for example, his chauffeur (A.O.), his secretary (V.E.) and handlers of the banknotes (C.E. and A.O.). Another member (M.C.) would act as the director of a chemical company and show the victims how to bleach the darkened banknotes in order to return them to their original state. The group would then ask the victim for €50,000 in exchange for the chemicals to bleach the banknotes.

During the investigation, F.A. was arrested and placed in pretrial custody. The real-time collection of content data (in particular, telecommunications data) as a result of the wiretapping of members of the group revealed that M.C. had taken the lead and continued the scam while F.A. was in custody. M.C. and A.O were subsequently arrested and placed in pretrial custody. A European arrest warrant was issued for C.E., one of the members of the group, but as authorities were not able to locate him, he was tried in absentia.

Of the six defendants arrested in this case, five were charged with and sentenced for committing fraud as part of an organized criminal group (F.A., A.O., V.E., M.C. and C.E.). One of the defendants (V.E.) had her sentence suspended. The remaining defendants were sentenced to five years' imprisonment (F.A., M.C. and C.E.) and three years' imprisonment (A.O.), in addition to being ordered to pay varying amounts of compensation to the victims. The sixth defendant (A.A.) was charged with receiving money obtained from the fraud but was ultimately acquitted by the court.

[377] **A/74/130**, para. 28.

[378] See, for example, Republic of Moldova (Council of Europe experts under the Cybercrime@EAP III project, *Conditions and Safeguards under Article 15 of the Convention on Cybercrime*, pp. 51–52).

[379] For example, Armenia and Azerbaijan (Council of Europe experts under the Cybercrime@EAP III project, *Conditions and Safeguards under Article 15 of the Convention on Cybercrime*).

5. Destruction of evidence and interference with law enforcement investigations

Perpetrators of cyber organized crime use a variety of techniques to interfere with the availability and collection of evidence relating to their crimes. In particular, they use numerous techniques to hide, obfuscate, delete or destroy digital data. To hide the data, they use encryption, which blocks access to the data from those who do not have access to the relevant encyption key, such as law enforcement agencies.[380] Privacy-enhancing technologies, such as virtual private networks and Tor, are also used.[381] Digital data can be obfuscated by using tactics such as the use of proxy servers to mask or hide IP addresses.[382] Finally, the deletion and destruction of digital data can be done by manually deleting data and destroying hardware.[383] Members of the Bored group, an international child sexual exploitation group (see the box in chap.V, sect. B.6), deleted data from their devices and drilled holes in hard drives.[384] In *Regina v. Reece Baker and Sahil Rafiq*, the appellants had deleted content from their computers, and one defendant wiped their computer once he had been informed that he was under investigation.[385] In *United States of America v. Paras Jha* (the Mirai botnet case), the defendant not only securely erased the virtual machine used to run Mirai on his device, but also posted the Mirai code online, in order to create plausible deniability if law enforcement authorities found the code on computers controlled by the defendant or the other conspirators.[386] Data can also be damaged and destroyed through the use of software that is designed to wipe data from digital devices. For example, one of the defendants in the Infraud case wiped data from his smartphone and used a tool to erase data from his hard drives before he surrendered them to the authorities.[387] All of the aforementioned tools are called "anti-forensic" tools because they are designed to remove, alter, disrupt or otherwise interfere with evidence of criminal activities on digital systems, similar to how criminals would physically remove evidence from crime scenes.[388] These anti-forensic tools can be used to obstruct justice by destroying and concealing evidence from law enforcement authorities.

E. International cooperation

International cooperation involves countries working together to achieve common goals. Cooperation between criminal justice authorities in different countries can include the sharing of information and human, technical and/or financial resources during investigations and prosecutions of cyber organized crime. International cooperation is dependent on existing relationships between countries. This type of international cooperation can be informal or formal. Informal international cooperation is based on criminal justice actor cooperation between countries. Formal international cooperation can be based on multilateral, regional or bilateral treaties. The Organized Crime Convention can serve as a basis for formal international cooperation as it includes provisions on mechanisms to facilitate such cooperation. States parties to the Convention are required to take measures that facilitate various forms of international cooperation, including extradition, mutual legal assistance, law enforcement cooperation and joint investigations. Each of these measures is discussed in the present section.

[380] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 17; *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard members used encryption).

[381] Europol, *Internet Organised Crime Threat Assessment 2020*, p. 17.

[382] *United States of America v. John Doe #1, Edward Odewaldt, et al.* (Dreamboard members used proxy servers).

[383] United Kingdom, Royal Courts of Justice, *Regina v. Reece Baker and Sahil Rafiq* [2016] EWCA Crim 1637, 2016 WL 06476265.

[384] *United States of America v. Caleb Young*, p. 15.

[385] *Regina v. Reece Baker and Sahil Rafiq* [2016] EWCA Crim 1637.

[386] *United States of America v. Paras Jha*, chap. II, sect. C, para. 8.

[387] United States District Court, District of Nevada, *United States of America v. Valerian Chiochiu*, 10 April 2019; *United States of America v. Valerian Chiochiu*, Case No. 2:17-CR-306-JCM-PAL, Plea Agreement, 31 July 2020.

[388] Kevin Conlan, Ibrahim Baggili and Frank Breitinger, "Anti-forensics: furthering digital forensic science through a new extended, granular taxonomy", *Digital Investigation*, vol. 18 (2016), p. 67.

R v. Ionut Emanuel Leahu [2018] EWCA 1064 (Crim) (United Kingdom)

The appellant, I.E.L., along with other defendants in the case (P., B. and M.), men from the Republic of Moldova and Romania, were part of an organized criminal group that obtained unauthorized access to automatic teller machines (ATMs) in Great Britain by infecting the systems with malware that was then used to remove large sums of money from them. On one long weekend in May 2014, the group obtained unauthorized access to 51 ATMs. The appellant identified the ATMs that malware could be loaded onto and subsequently accessed the machines so that they could be infected with the malware.

A few days after the bank fraud was perpetrated, the appellant and M. were arrested, interviewed and subsequently released on bail. Following their release, they left the country, travelling on flights to the Republic of Moldova (M.) and Romania (the appellant). Following the issuance of European arrest warrants for both individuals, they were extradited to England.

The appellant pleaded guilty to conspiracy to defraud and was sentenced to 4 years and 10 months of imprisonment. M. was sentenced to 2 years and 10 months of imprisonment for the same offence. The other conspirators (P. and B.) received sentences of 5 years' imprisonment and 7 years' imprisonment, respectively, for their roles in the fraud. The appellant's subsequent appeal against his sentence was unsuccessful.

For more information on this case, see UNODC, SHERLOC case law database, Case No. GBRx096.[a]

[a] Available at https://sherloc.unodc.org/.

1. Extradition

Extradition involves the return of wanted fugitives to the country requesting extradition. Extraditions are made possible with bilateral and/or regional treaties. Pursuant to the extradition treaty that the United States has with Israel, for example, the administrator of Card Planet was arrested at an airport near Tel Aviv and subsequently extradited to the United States from Israel, after having lost several appeals to prevent his extradition.[389]

Extradition is governed by the domestic law of the States concerned, as well as any applicable bilateral or multilateral treaties. Article 16, paragraph 4, of the Organized Crime Convention provides a legal basis for extradition in respect of offences covered by that article in cases where there is no extradition treaty between the States. Instruments governing extradition determine, among other things, the conditions for extradition and any mandatory or discretionary grounds for refusal. Dual criminality is generally a prerequisite for extradition; the aim is to ensure that the State in the territory of which a person is present will not extradite him or her unless the offence for which the person is wanted is qualified as a crime in both States.[390]

Some national laws concerning cybercrime expressly address extradition. A case in point is the Cybercrime and Computer Related Crimes act of Botswana, adopted in 2007. Article 29 of the act holds that an offence under the act shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act, 1990. Without extradition treaties, a country has no obligation to extradite a wanted fugitive to the requesting country. Nonetheless, even the existence of extradition treaties does not guarantee that a wanted fugitive will be extradited to the country requesting the extradition.

[389] *United States of America v. Aleksei Yurievich Burkov*.

[390] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime*, paras. 473 and 492.

ÚS 530/18 ze dne 27. 3. 2018 (Czechia)

In October 2020, Y.A.N., a Russian national, was sentenced to 88 months' imprisonment in the United States for hacking into social networks, including a well-known social network for professionals, and a file hosting service based in the United States and selling the information stolen from this unauthorized access. He was extradited to the United States from Czechia.[a] He had challenged a decision by the municipal court of Prague, as well as the rejection by the high court of his appeal of the decision, to extradite him to the United States. He filed a complaint pursuant to the Constitution, the Charter of Fundamental Rights and Freedoms of Czechia and the Convention for the Protection of Human Rights and Fundamental Freedoms (the European Convention on Human Rights).

The municipal court of Prague ruled on the proposal of the office of the public prosecutor regarding the extradition of the complainant for two criminal prosecutions in different countries pursuant to the Act on International Judicial Cooperation in Criminal Matters of Czechia, as amended. The municipal court ruled that the extradition for both prosecutions was allowed and that the complainant could, therefore, be extradited to the United States (to be prosecuted for unauthorized access to systems and data) and to the Russian Federation (to be prosecuted for the theft of property over the Internet within an organized criminal group). The municipal court held that the alleged acts that were the subject of the prosecutions in the Russian Federation and the United States were considered crimes under Czech law. The municipal court also concluded that the due process rights of the complainant would be respected in both countries. From the materials provided by the foreign authorities, the municipal court held that the extradition was not prohibited under the Act on International Judicial Cooperation in Criminal Matters.[b] According to the municipal court, the complainant was a young, healthy man, and it could not be assumed that his extradition would cause him disproportionate harm.

It is important to note that the complainant did not object to his extradition to the Russian Federation. The complainant objected to his extradition to the United States. The municipal court did not find any reason to object to the extradition of the complainant to the United States. Furthermore, the municipal court held that the complainant's objection to the extradition to the United States, specifically, on the grounds that he would be subjected to a disproportionate penalty were unfounded, especially since in the United States sentences for several crimes could be served concurrently.

The complainant appealed the decision of the municipal court to the high court in Prague. After reviewing the decision of the municipal court and the evidence presented by the complainant, the high court rejected the appeal and similarly found that there were no grounds for prohibiting the extradition of the complainant. The high court echoed many of the conclusions of the municipal court, concluding that there were no facts presented that illustrated the risk of human rights violations and disproportionate sentencing of the complainant if he was to be extradited to the United States. With regard to the latter, the high court rejected the complainant's argument that he was at risk of receiving a penalty of up to 54 years' imprisonment in the United States. In rejecting this claim, the high court noted that the penalty that he could receive for the alleged crimes ranged from 12 to 14 years of imprisonment.

The Constitutional Court held that the decisions of the municipal court and the high court met constitutional requirements. The Court held that Czechia was obligated to comply with its international obligations in the field of criminal law, unless other stronger international obligations (usually in the field of protection of human rights) or the basic values of the Czech constitutional order took precedence. The task of the courts in proceedings under section 95 of the Act on International Judicial Cooperation in Criminal Matters was, in essence, to determine whether the request for extradition met the basic requirements of this Act and whether extradition was not hindered by any legal obstacle. The Constitutional Court concluded that the municipal court and the high court had

fulfilled this task. The Constitutional Court also held that differences in the approach of countries with respect to criminal penalties were not in themselves grounds for non-compliance with international obligations, as long as the penalties and the treatment of offenders were in line with human rights obligations. Ultimately, the Constitutional Court ruled that the constitutional complaint of the applicant was manifestly unfounded.

When Y.A.N. was extradited to the United States and tried by a jury, he received a sentence of 7 years and 4 months of imprisonment for his offending.[c]

For more information on this case, see UNODC, SHERLOC case law database, Case No. CZEx002.[d]

[a] United States Attorney's Office, Northern District of California, "Russian hacker sentenced to over 7 years in prison for hacking into three Bay Area tech companies", press release, 30 September 2020. For information about the case and charges against the defendant, see United States District Court, Northern District of California, *United States of America v. Yevgeni Nikulin*, Case No. 16-CR-0440-WHA, Indictment, 20 October 2016.

[b] This Act includes criteria that would prohibit the extradition of an individual to a foreign country.

[c] He was sentenced for selling stolen usernames and passwords, in violation of Title 18, section 1029 (a)(2), of the United States Code; installing malware on protected computers, in violation of Title 18, section 1030 (a)(5); conspiracy, in violation of Title 18, section 371; computer intrusion, in violation of Title 18, section 1030 (a)(2)(C); and aggravated identity theft, in violation of Title 18, section 1028A (1) (United States Attorney's Office, Northern District of California, "Russian hacker sentenced to over 7 years in prison").

[d] Available at https://sherloc.unodc.org/.

2. Mutual legal assistance

Mutual legal assistance is a crucial tool for international cooperation, enabling countries to receive and provide assistance in the investigation, prosecution and adjudication of transnational organized crime. In *United States of America v. Eric Eoin Marques*, for example, the FBI was able to obtain information that confirmed the location of the Freedom Hosting server and, via a request to France for mutual legal assistance, identified evidence that the subscriber to the Freedom Hosting server account was the defendant (E.M.).[391] When the server was seized, more than 8.5 million images and video recordings of suspected and/or confirmed child sexual abuse material were found, almost 2 million of which were unknown to law enforcement authorities at the time of the seizure.[392]

National laws and bilateral, regional and multilateral treaties, agreements and arrangements have been enacted that permit mutual legal assistance between countries. These instruments establish the nature and scope of the cooperation, the type of mutual legal assistance to be provided, the rights and responsibilities of those requesting and providing mutual legal assistance, and the procedures to be followed. Article 18 of the Organized Crime Convention provides for the establishment of a comprehensive regime for mutual legal assistance. In paragraph 3 of article 18, it is stated that mutual legal assistance to be afforded in accordance with that article may be requested for any of the following purposes:

(a) Taking evidence or statements from persons;

(b) Effecting service of judicial documents;

(c) Executing searches and seizures, and freezing;

(d) Examining objects and sites;

(e) Providing information, evidentiary items and expert evaluations;

(f) Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records;

[391] United States District Court, District of Maryland, *United States of America v. Eric Eoin Marques*, Case No. TDC-19-200, Plea Agreement, 28 January 2020.

[392] Ibid.

(g) Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes;

(h) Facilitating the voluntary appearance of persons in the requesting State party;

(i) Any other type of assistance that is not contrary to the domestic law of the requested State party.

Mutual legal assistance can be denied for several reasons, including if one or more of the conditions for mutual legal assistance are not met and/or compliance with the request would violate human rights obligations.[393] In the absence of mutual legal assistance treaties, agreements or conventions that can be used in lieu of such treaties and agreements, mutual legal assistance can be provided if reciprocity is guaranteed by the requesting country.[394]

Apelação Criminal 5492-CE, 5a Região da TRF (2004.81.00.018889-0) (Brazil)

S.S., one of the leaders of an organized criminal group in Germany known as the Brazil Club, along with others, O.F.G., F.C.L.O. and F.S.M., created and maintained websites (www.brasil-club.de and www.brasil-club.com) that facilitated sex tourism. Others in the organized criminal group (O.F.G. and F.C.L.O.) also contributed to the enterprise by recruiting victims and obtaining naked and/or sexualized images of women for use on the websites in order to advertise the women and the services offered. As part of the criminal activity, clients were solicited to purchase sexual services and women were recruited from Brazil to participate in international sex tourism and offer sexual services to paying clients in Germany. Arrangements were also made for Brazil Club's clients in Germany to travel to Brazil to engage in sexual activities with Brazilian women. Brazilian women were also solicited to travel to Europe to engage in sex work. The organized criminal group also recruited some female minors.

During the investigation and prosecution of the case, S.S. could not be located by Brazilian authorities. S.S. became aware of the criminal proceedings against him when he was in Germany. He subsequently hired a lawyer, pleaded not guilty and argued that Brazilian courts had no jurisdiction over the case. Under Brazilian criminal procedure, a defendant's testimony is compulsory (with few exceptions), even if it only concerns an affirmation to remain silent. Because S.S. was not in Brazil, a letter rogatory was used to inform him of the criminal case and to obtain his testimony pursuant to article 368 of the Code of Criminal Procedure of Brazil.[a] Ultimately, S.S. was not tried in a Brazilian court – not because Brazil did not have jurisdiction, but because a trial in Germany would be more efficient.

[393] See, for example, article 2 of the European Convention on Mutual Assistance in Criminal Matters; article 25, paragraph 4, of the Council of Europe Convention on Cybercrime; article 4 of the Economic Community of West African States Convention on Mutual Assistance in Criminal Matters; UNODC, Education for Justice University Module Series, Cybercrime, Module 3: legal frameworks and human rights, "International and regional instruments"; Module 7: international cooperation against cybercrime, "Formal international cooperation mechanisms"; and UNODC, Education for Justice University Module Series, Organized Crime, Module 11: international cooperation to combat transnational organized crime, "Mutual legal assistance". Available at www.unodc.org/.

[394] See UNODC, Education for Justice University Module Series, Cybercrime, Module 7: international cooperation against cybercrime, "Formal international cooperation mechanisms"; and UNODC, Education for Justice University Module Series, Organized Crime, Module 11: international cooperation to combat transnational organized crime, "Mutual legal assistance".

Like S.S., one of the defendants (O.F.G.) appealed his conviction, claiming that the websites were pornographic and that no international treaty existed between Brazil and Germany regarding the maintenance of pornographic websites. The court of appeals rejected this claim, arguing that his conviction, which was supported by evidence, was not for maintaining pornographic websites but for facilitating prostitution and international trafficking in persons for the purpose of sexual exploitation.[b] He received a sentence of 10 years and 6 months of imprisonment for international trafficking in persons for the purpose of sexual exploitation and facilitating prostitution or other forms of sexual exploitation, among other crimes. Other members of the criminal organization were sentenced for the same crimes.[c]

For further information about this case, see UNODC, SHERLOC case law database, Case No. BRA004.[d]

[a] Article 368 of the Code of Criminal Procedure of Brazil holds that "If the accused is abroad, in a known place, he will be *summoned* by letter rogatory...".
[b] Brazil, Tribunal Regional Federal da 5a Região, Apelação Criminal 5492-CE, 5a Região da TRF (2004.81.00.018889-0).
[c] F.S.M. received a sentence of 11 years and 10 months of imprisonment for those crimes, and F.C.L.O. received a sentence of 8 years and 9 months of imprisonment, as well as being charged with an offence relating to child sexual abuse material (see UNODC SHERLOC case law database, Case No. BRA056. Available at https://sherloc.unodc.org/).
[d] Available at https://sherloc.unodc.org/.

3. Law enforcement cooperation

Law enforcement cooperation occurs in accordance with national criminal law and criminal procedure law. These laws enable countries to determine the scope and means of such cooperation, as well as to deny requests for cooperation that contravene national laws.[395] Regional and multilateral treaties, conventions and agreements also enable international cooperation between law enforcement agencies. Article 27 of the Organized Crime Convention provides for measures that facilitate cooperation, such as establishing and/or improving police-to-police communication channels and guidance on the type of police cooperation sought (e.g., the identity, location and activities of persons and the location of property). The manner in which this cooperation is to occur may vary from country to country. Law enforcement cooperation may involve direct contact between law enforcement agencies or contact through a specific designated agency. There are legal and practical issues associated with law enforcement cooperation, including variation in national laws and procedures regarding such cooperation and the efficiency of those channels. The purpose of this type of law enforcement cooperation is to provide an alternative to the lengthy mutual legal assistance process.

[395] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime*, p. 175.

Danmark B(R), ref. 9-3441/2015, domfældelse 14 December 2015 (Denmark)

Operation Hvepsebo (Wasp Nest case)

Operation Hvepsebo concerned an organized criminal group engaged in trafficking in persons for the purpose of exploitation (in particular, forced labour). The male victims were recruited in Romania. Their recruiters fraudulently advertised work in Denmark. When the Romanian victims arrived in Denmark, however, they were exploited and forced to engage in unlawful acts, committing a wide variety of fraudulent activity online and offline. After the victims' arrival, members of the organized criminal group would take each victim to a municipal office to receive a Danish personal identification number. This identification was needed for the victims to be able to legally work in Denmark and to pay taxes. To obtain the identification number, the victims provided their authentic Romanian identification documents along with fake employment contracts and home addresses. Members of the organized criminal group used the identifying information of the victims, including their Danish personal identification numbers, to perpetrate a wide variety of illicit activities both online and offline (credit card fraud, tax fraud, etc.), as well as to create new companies to perpetrate some of the illicit activities. The defendants had victims open up bank accounts and obtain debit cards, credit cards and loans, in addition to having the victims turn over their identity documents and data to the defendants, which they used, unbeknown to the victims, to perpetrate various forms of fraud. The defendants would accompany victims to establishments such as banks and stores and would speak on behalf of the victims (since the victims did not know the language) and would have the victims sign documents that they could not read and could not understand. The victims never actually worked in the jobs they were promised. The victims were provided short-term work assignments by the defendants or they worked for the defendants for no payment or a very modest payment.

This case involved three members of the group. For the crimes perpetrated by the three defendants, their sentences ranged from 3 to 8 years of imprisonment. These defendants were not Danish citizens and were deported from Denmark and banned from re-entering the country.

This case highlights successful cross-border police cooperation in a case involving cyber organized crime. In addition to showing the successful cooperation between law enforcement agencies in two countries (Denmark and Romania), this case involved the creation of a multidisciplinary team that worked together on the case. The team included a Danish non-governmental organization (the Centre against Human Trafficking), the Danish Immigration Service and a tax agency (Skattestyrelsen), as well as police and prosecutors from Denmark and Romania.

4. Joint investigations

Another form of international cooperation is a joint investigation. Agreements or arrangements between countries are made to enable and facilitate the creation of joint investigative bodies.[396] When these agreements and arrangements are absent, joint investigations may be conducted on a case-by-case basis.[397] The *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime* includes two models for joint investigations:

(a) The first model identified consists of parallel, coordinated investigations with a common goal, assisted by a liaison officer network or through personal contacts and supplemented by formal mutual legal assistance requests in order to obtain evidence. The officials involved may be "non-co-located" and be able to work jointly on the basis of long-standing cooperative practices and/or existing mutual legal assistance legislation depending on the nature of the legal systems or systems involved;

(b) The second model consists of integrated joint investigation teams with officers from at least two jurisdictions. These teams can be further divided and characterized as either passive or active. An example of a passively integrated team would be the situation where a foreign law enforcement officer is integrated with officers from the host State in an advisory or consultancy role or in a supportive role based on the provision of technical assistance to the host state. An actively integrated team would include officers from at least two jurisdictions with the ability to exercise operational powers (equivalent or at least some powers) under host State control in the territory or jurisdiction where the team is operating.[398]

There are certain legal and practical issues associated with joint investigations, including trust between law enforcement agencies, differing criminal procedural issues and rules of evidence, and/or the absence of agreement on organization, roles, responsibilities, leads and supervision in the joint investigation and/or mechanisms for resolving conflicts.[399]

[396] See article 19 of the Organized Crime Convention.

[397] Ibid.

[398] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime*, para. 596. For further information, see UNODC, *Model Legislative Provisions against Organized Crime* (Vienna, 2012), pp. 87–93.

[399] UNODC, *Legislative Guide for the Implementation of the United Nations Convention against Transnational Organized Crime*, para. 597.

United States of America v. Bryan Connor Herrell, Case No. 1:17 CR00301 (E.D. California, 2 September 2020) and *United States of America v. Ronald L. Wheeler III*, Case No. 1:17-CR-377 (N.D. Georgia, 15 November 2017) (United States of America)

AlphaBay (darknet site)

AlphaBay operated as a criminal enterprise with "employees" serving as security administrators, moderators, public relations specialists and scam watchers (whose primary duty was to identify and remove fraudulent listings). "Employees" received their salaries in bitcoin. AlphaBay employees have been identified and prosecuted for their crimes. For example, B.C.H., a moderator for the site, settled disputes between buyers and vendors on AlphaBay.[a] He pleaded guilty to conspiracy to engage in a racketeer-influenced corrupt organization, receiving a sentence of 132 months' imprisonment.[b] In addition, R.L.W. III, who served as a public relations specialist for AlphaBay, not only on the darknet site but also on the clearnet, in an AlphaBay online community on a well-known social media website.[c] He was charged with and pleaded guilty to conspiracy to commit access device fraud. For his crime, he received a sentence of 3 years and 10 months of imprisonment and 3 years of supervised release.[d]

AlphaBay and another major darknet market, Hansa Market, were shut down following a joint investigation involving the FBI, the Drug Enforcement Administration of the United States, the national police of the Netherlands and other European law enforcement agencies acting through Europol.[e] The national police of the Netherlands had taken over Hansa Market and had monitored and run the site unbeknown to the users, enabling the police to identify users and disrupt illicit activity on the site. AlphaBay was shut down while the national police were running Hansa Market. The coordinated shutting down of AlphaBay enabled the national police to obtain information identifying the users from AlphaBay who had joined Hansa. Once that information was collected, Hansa Market was shut down and its seizure by law enforcement agencies was made public.

For more information on this case, see UNODC, SHERLOC case law database, Case No. USAx191.[f]

[a] United States District Court, Eastern District of California, *United States of America v. Bryan Connor Herrell*, Case No. 1:17 CR00301, Indictment, 2 September 2020.

[b] Ibid.; United States Attorney's Office, Eastern District of California, "Colorado man pleads guilty to racketeering charges related to darknet marketplace AlphaBay", press release, 28 January 2020.

[c] United States District Court, Northern District of Georgia, *United States of America v. Ronald L. Wheeler III*, Case No. 1:17-CR-377, Criminal Information, 15 November 2017.

[d] United States Attorney's Office, Northern District of Georgia, "AlphaBay spokesperson sentenced to federal prison", press release, 1 August 2018.

[e] Europol, "Massive blow to criminal dark web activities after globally coordinated operation", press release, 20 July 2017.

[f] Available at https://sherloc.unodc.org/.

CHAPTER VII.

CONCLUSIONS AND LESSONS LEARNED

VII. CONCLUSIONS AND LESSONS LEARNED

The present digest shows how criminal justice systems throughout the world have responded to cyber organized crime by analysing concluded judicial decisions from more than 20 jurisdictions. The research for this digest predominantly involved a review of primary sources, supplemented by secondary sources. The cases referred to in the digest are not the only ones that concern the subject of this digest. The cases included were chosen because of *(a)* their relevance; *(b)* the substantive and procedural elements of cyber organized crime that were covered; and *(c)* the need to ensure that a variety of jurisdictions were represented in the digest. Accordingly, the findings of this digest are not generalizable because the cases included in the digest cannot be considered a representative sample of all cases involving cyber organized crime in all countries. Nevertheless, the cases included in the digest may help to shed some light on a largely unknown and understudied form of cybercrime. This last chapter provides concluding remarks and lessons learned from the cases analysed in the digest.

Overall, cases of cyber organized crime were not easily identifiable across jurisdictions. The identification of such cases is challenging because the cases are not recorded as cyber organized crime and perpetrators of these crimes may not be charged with and/or convicted of organized crime and/or participation in an organized criminal group. Research on cyber organized crime is thus hampered by the fact that the concept of cyber organized crime is not frequently deployed in such cases, making the cases harder to identify and analyse. Although the cases included in this digest were not prosecuted and adjudicated as cyber organized crime, they were identified as a form of cyber organized crime through a careful, time-consuming review of court documents. The language limitations of the researchers and drafters working on the digest represented a challenge to efforts to identify cases of cyber organized crime. An additional challenge was the lack of access to publicly available court documents in many jurisdictions.

While the digest predominantly includes cases that involved participation in an organized criminal group, there were some cases where cybercrime was perpetrated by an organized criminal group that operated exclusively online, operated both online and offline, or utilized only the Internet and digital devices to facilitate the crimes. To a lesser extent, there were cases that met the definition of cyber organized crime but the court documents mentioned neither an organized criminal group nor participation in an organized criminal group in the analysis of the cybercrimes.

Most of the court documents analysed for this digest did not provide enough information to determine the structure of cyber organized criminal groups, particularly whether such groups could be classified as swarms, hubs, clustered hybrids and/or extended hybrids. The most difficult structure to identify in the court documents was a swarm. More information is needed about the structure of cyber organized criminal groups and even the roles of individuals within those groups.[400] When available, critical procedural information relating to the investigation and prosecution of cyber organized crime was also found in affidavits, criminal information, complaints and indictments, as well as in requests for extradition. Information about the gender dimensions of cyber organized crime was also limited and was largely based on the cases of cyber organized crime that were identified. The information provided in this digest about the gender dimensions of cyber organized criminal groups and cyber organized crime are not generalizable. Gender information about victims was not often identified in the court documents of the cases in the digest, exceptions being the cases that involved child sexual exploitation and abuse, trafficking in persons and, to a lesser extent, romance scams and sextortion.

It would be useful to receive such information about the structures and organization of cyber organized criminal groups and the roles of individuals within those groups, as well as the gender of participants in cyber organized crime and victims of cyber organized crime, from criminal justice professionals through court documents. This information would enable the identification of trends and patterns that could be shared with criminal justice agencies around the world to help them improve their efforts to detect, investigate, prosecute and adjudicate cyber organized criminal groups and those who participate in cyber organized crime. This information would also provide criminal justice professionals with a better understanding

[400] The limited information that was identifiable about the structure and roles of cyber organized criminal groups were primarily (but not exclusively) found in United States court documents (i.e., criminal complaints and indictments).

of cyber organized criminal groups, their tactics, targets, techniques, tools, members, associates and methods of operation, as well as the ways in which these groups evolve in response to countermeasures.

In the cases included in this digest, variations were observed with respect to sentences for similar offences across and even within jurisdictions. These variations were also observed between different offences. A case in point were sentences for offences relating to child sexual exploitation and abuse. In some jurisdictions the penalties were quite severe, while in others the penalties were low, depending on the type of offences involving child sexual exploitation and abuse.[401] Moreover, in one jurisdiction, perpetrators of a romance scam received a more severe penalty than perpetrators of child sexual exploitation and abuse, both within the country and outside of that country.

Furthermore, the cases in this digest revealed that international cooperation, harmonized approaches to the investigation and prosecution of cyber organized crime, as well as the existence of sufficient national human, technical and economic resource capacities to investigate and prosecute cyber organized crime, played a critical role in the successful adjudication of cyber organized crime. In view of that, attention needs to be paid to the deficit in national capacities to investigate, prosecute and adjudicate cyber organized crime. This would enable more jurisdictions to take a leading role in prosecuting offences involving cyber organized crime.

Ultimately, the findings of the digest illustrate the need to harmonize approaches with respect to the collection and recording of information relating to cyber organized crime in court and other documents across jurisdictions, as well as the need to train criminal justice professionals on cyber organized crime and the ways to successfully detect, investigate, prosecute and adjudicate cyber organized crime, cyber organized criminal groups and participation in cyber organized crime. It is hoped that the digest will lead to the collection and recording of information and the training of criminal justice professionals on cyber organized crime, as well as future research on cyber organized crime, which will help to inform policymakers and other stakeholders regarding the courses of action to be taken to reduce, control, prevent and/or mitigate this form of cybercrime.

[401] See, for example, Argentina, Tribunal Oral Federal de Jujuy, Causa FSA 8398/2014/TO1; Costa Rica, Tribunal Penal del Tercer Circuito Judicial de San José, Causa penal número 15-001824-0057-PE & Causa Penal número 19-000031-0532-PE (Operación R-INO); Canada, *R v. Philip Michael Chicoine* [2017] S.J. No. 557, 2017 SKPC 87; *United States of America v. Caleb Young*, Case No. 18-20128, 11 May 2018; *United States of America v. Dylan Heatherly*, No. 19-2424 and *United States of America v. William Staples*, No. 19-2932; *United States of America v. John Doe #1, Edward Odewaldt, et al*., Case No. 10-CR-00319, 16 March 2011; Republic of Korea, Seoul Central District Court (Criminal Department I-I), 2018NO2855, 2 May 2019 (Welcome to video); Australia, *R v. Mara* [2009] QCA 208; Germany, LG Limburg, Urteil vom 07.03.2019, 1 KLs - 3 Js 73019/18.

ANNEX

ANNEX

List of cases involving cyber organized crime

Argentina

Poder Judicial de Córdoba -"Emiliozzi, Arturo Osvaldo y otros PSSAA Estafa, etc." - Expediente SAC No. 2654377
Tribunal Oral Federal de Jujuy, Causa FSA 8398/2014/TO1

Australia

Hew Raymond Griffiths v. United States of America, 143 FCR 182 (2005), 2005 WL 572006
R v. Mara [2009] QCA 208

Belgium

Tribunal correctionnel d'Anvers, Antwerpen, 2 mai 2016

Brazil

Apelação Criminal 5492-CE, 5a Região da TRF (2004.81.00.018889-0)

Canada

R v. Philip Michael Chicoine [2017] S.J. No. 557, 2017 SKPC 87
R. v. Kalonji, 2019 ONCJ 341
R v. Pitts, 2016 NSCA 78

Chile

Fiscalía Metropolitana Sur, Chile. Rol Único de Causa No.1700623543-3 (Zares de la Web)

China

Hong Kong

HKSAR v. Chan Pau Chi [2019] HKEC 1549

Costa Rica

Tribunal Penal del Tercer Circuito Judicial de San José, Causa penal número 15-001824-0057-PE & Causa Penal número 19-000031-0532-PE (Operación R-INO)

Czechia

ÚS 530/18 ze dne 27. 3. 2018

Denmark

Danmark B(R), ref. 9-3441/2015, domfældelse 14 December 2015

Dominican Republic

Segundo Juzgado de Instrucción del Distrito Nacional – Proceso No. 058-13-00719

El Salvador

Tribunal de Sentencia de Santa Tecla, 139-1U-2018

Fiji

State v. Naidu et al [2018] FJHC 873

France

Cour de cassation, chambre criminelle, 21 mars 2012, 11-84437
TGI Lille, 7e ch. corr., jugement du 29 janvier 2004
Tribunal de grande instance de La Roche-sur-Yon, 24 septembre 2007
Tribunal de grande instance de Paris, 13e chambre correctionnelle, 20 novembre 2018

Germany

BGH, Beschluss vom 06.07.2010, 4 StR 555/09
BGH, Beschluss vom 19.04.2011, 3 StR 230/10
BGH, Beschluss vom 31.05.2012, 2 StR 74/12
BGH, Beschluss vom 30.08.2016, 4 StR 194/16
BGH, Beschluss vom 15.01.2020, 2 StR 321/19
LG Bonn, Urteil vom 07.07.2009, 7 KLs 01/09
LG Duisburg, Urteil vom 05.04.2017, 33 KLs - 111 Js 32/16 - 8/16
LG Hamburg, Urteil vom 21.03.2012, 608 KLs 8/11
LG Karlsruhe, Urteil vom 19.12.2018, 4 KLs 608 Js 19580/17
LG Leipzig, Urteil vom 14.06.2012, 11 KLs 390 Js 191/11
LG Limburg, Urteil vom 07.03.2019, 1 KLs - 3 Js 73019/18
LG München, Urteil vom 07.06.2017, 19 KLs 30 Js 18/15

India

Rajesh and others v. State of Rajasthan, Division Bench Appeal No. 178, 122 and 123 / 2016
State of Maharashtra v. Opara Chilezien Joseph

Italy

Cassazione penale, sezione III, 12 Febbraio 2004, No. 8296, & Tribunale di Siracusa, 19 Luglio 2012, No. 229
Cass., 31 Marzo 2017, No. 43305
Cassazione penale, sezione VI, sentenza No. 11356, 8 Novembre 2017
Cassazione penale, sezione feriale, sentenza No. 50620, 12 Settembre 2013

Mexico

Tribunal de Enjuiciamiento del Distrito Judicial Morelos – número de juicio 38/2020

Nigeria

Federal Republic of Nigeria v. Harrison Odiawa, Suit No ID/127c/2004

Philippines

Regional Trial Court of Misamis Oriental, 10th Judicial Region, Branch 41, CRIM Case No. 2009-337

Republic of Korea

Seoul Central District Court (Criminal Department I-I), 2 May 2019, 2018NO2855

Samoa

Police v. Zhong [2017] WSDC 7

Senegal

Tribunal de grande instance hors classe de Dakar, 14 janvier 2020, 30/2020

Singapore

Public Prosecutor v. Law Aik Meng [2006] SGDC 243

United Kingdom of Great Britain and Northern Ireland

England and Wales

R. v. Nicholas Webber [2011] EWCA Crim 3135
Regina v. Sunday Asekomhe [2010] EWCA Crim 740
Regina v. Reece Baker and Sahil Rafiq [2016] EWCA Crim 1637, 2016 WL 06476265
Regina v. Jake Levene, *Mandy Christopher Lowther*, *Lee Childs* (2017), Crown Court Leeds, T20177358
Regina v. Ionut Emanuel Leahu [2018] EWCA 1064
Regina v. Bradley David Rogers, Colin Martin Samuels, Geraldine French, Mark Julian Bell [2014] EWCA Crim 1680

Northern Ireland

Queen v. Paul Mahoney [2016] NICA 27, 2016 WL 03506240.

United States of America

United States of America v. Brandon Arias, Case No. 18-CR-30141-NJR-2 (S.D. Illinois, 16 July 2019)
United States of America v. Oladimeji Seun Ayelotan, Femi Alexander Mewase, and Rasaq Aderoju Raheem, Case No. 17-60397 (5th Circuit, 4 March 2019)
United States of America v. Silviu Catalin Balaci, Case No. 19-877 (D. New Jersey, 2017)
United States of America v. Ramiro Ramirez-Barreti et al., Case No. 4:19-cr-47 (E.D. Virginia, 14 August 2019)
United States of America v. Svyatoslav Bondarenko et al., Case No. 2:17- CR -306-JCIVI-PAL (D. Nevada, 30 January 2018)
United States of America v. David Lynn Browing, Case No. 5:15 CR 15-RLV (W.D. North Carolina, 10 December 2015)
United States of America v. Aleksei Yurievich Burkov, Case No. 1:15-CR-245 (E.D. Virginia, 4 February 2016)
United States of America v. Anthony Blane Byrnes, Case No. 3:20-CR-192 (W.D.N.C. 2020)
United States of America v. Steven W. Chase, Case No. 5:15-CR-00015 (W.D. North Carolina, 8 May 2017)
United States of America v. Valerian Chiochiu, 2019 U.S. Dist. LEXIS 133555 (D. Nevada, 10 April 2019)
United States of America v. Jael Mejia Collado, et al., Case No. 13 CR 259 (KAM) (E.D. New York, May 2013)
United States of America v. Dennis Collins et al., Case No. 11-CR-00471-DLJ (PSG) (N.D. California, 16 March 2012)
United States of America v. Gary Davis, Case No. 1:13-CR-950-2 (S.D. New York, 26 July 2019)
United States of America v. David Paul Dempsey and Edgar Jermaine Hosey, Case No. 2:18-CR-1022 (D. South Carolina, 14 November 2018)
United States of America v. John Doe #1, Edward Odewaldt, et al., Case No. 10-CR-00319, (W.D. Louisiana, 16 March 2011)

United States of America v. Jimmy Dunbar, Jr., and Mitchlene Padgett, Case No. 2:18-CR-1023 (D. South Carolina, 14 November 2018
U.S. v. E-Gold, Limited Criminal Action No. 07-109 (RMC) (D.D.C., 20 July 2007)
United States of America v Brian Richard Farrell, Case No. 2:15-CR-29-RAJ (W.D. Washington, 17 January 2015)
United States of America v. Carl Allen Ferrer, Case No. 18 Cr. 464 (D. Arizona, 5 April 2018)
United States of America v. Ercan Findikoglu, Case No. 1:13-CR-00440 (E.D. New York, 24 June 2015)
United States of America v. Michael Fluckiger, Case No. 5:15 CR 15-RLV (W.D. North Carolina, 24 November 2015)
United States of America v. Matthew Brent Goettsche, Russ Albert Medlin, Jobadiah Sinclair Weeks, Joseph Frank Abel, and Silviu Catalin Balaci, Case No. 19-CR-877-CCC (D. New Jersey, 5 December 2019)
United States of America v. Martin Gottesfeld, 319 F. Supp. 3d 548 (D. Mass. 2018)
United States of America v. Dylan Heatherly, Case No. 19-2424 (3d Circuit 2020)
United States of America v. Bryan Connor Herrell, Case No. 1:17 CR00301 (E.D. California, 2 September 2020)
United States of America v. Cristian Hirales-Morales, Marcos Julian Romero and Sergio Anthony Santivanez, Case No. 19-CR-4089DMS, Indictment (S.D. California, 10 October 2019)
United States of America v. Fedir Oleksiyovych Hladyr, Case No. CRl7-276RSL (W.D. Washington, 25 January 2018)
United States of America v. Alexandru Ion, Case No. 5:18-CR-81-REW-MAS-6 (E.D. Kentucky, 10 October 2019)
United States of America v. Aleksey Vladimirovich Ivanov, 175 F. Supp. 2d 367 (2001)
United States of America v. Paras Jha, Case No. 3:17-CR-00164 (D. Alaska, 5 December 2017)
United States of America v. Ijaz Khan, Case No. 17-4301 (4th Circuit 2018)
United States of America v. Alexander Konovolov et al., Case No. 2-19-CR-00104 (W.D. Pennsylvania, 17 April 2019)
United States of America v. Michael Lacey, James Larkin, Scott Spear, John "Jed" Brunst, Dan Hyer, Andrew Padilla and Joye Vaught, 18 Cr. 422 (D. Arizona, 28 May 2018)
United States of America v. Liberty Reserve, Case No. 13-CR-368 (DLC) (S.D. New York, 23 September 2015)
United States of America v. Salvatore Locascio et al., 357 F. Supp. 2d 536 (2004)
United States of America v. Andrew Mantovani et al., Case No. 2:04-CR-0078 (D. New Jersey, 28 October 2004)
United States of America v. Hidalgo Marchan, Case No 1:15-CR-20471 (S.D. Florida, 23 June 2015)
United States of America v. Eric Eoin Marques, Case No. TDC-19-200 (D. Maryland, 28 January 2020)
United States of America v. Antwine Lamar Matthews, Malcolm Cooper, Andreika Mouzon, and Flossie Brockington. Cr. No. 2:18-1024 (D. South Carolina, 14 November 2018)
United States of America v. Sergey Medvedev, Case No. 2:17-CR-306-JCM-VCF (D. Nevada, 26 June 2020)
United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus, Case No. 1:16-CR-00224 (N.D. Ohio, 8 July 2016)
United States of America v. Yevgeni Nikulin, Case No. 16-CR-0440-WHA (U.S. District Court of Northern California, 20 October 2016).
United States of America v. Adeyemi Odufuye and Stanley Hugochukwu, Case No. 3:16R232 (JCH), Indictment (D. Connecticut, 20 December 2016)
United States of America v. Obinwanne Okeke, Case No. 4:19-mj-00116 (E.D. Virginia, 2 August 2019)
United States of America v. Beniamin-Filip Ologeanu, Case No. 5:19-CR-10, Superseding Indictment (E.D. Kentucky, 6 February 2019)
United States of America v. Rakeem Spivey and Roselyn Pratt, Case No. 2:18-cr-0018 (D. South Carolina, 14 November 2018)

United States of America v. Vincent Ramos et al., Case No. 3:18-CR-01404-WQH (S.D. California, 15 March 2018)
United States of America v. Daniel Palacios Rodríguez, Alexandra Guzmán-Beato, Elvis Pichardo Hernández, José David Reyes- González, Juan Rufino Martínez-Domínguez, and Fátima Ventura Pérez, Case No. 1:19-MJ-286 (E.D. Virginia, 24 June 2019)
United States of America v. Aleksandr Andreevich Panin and Hamza Bendelladj, Case No. 1:11-CR-0557-AT-AJB (N.D. Georgia, 26 June 2013)
United States of America v. Melissa Scanlan, Case No. 18-CR-30141-NJR-1 & Case No. 19-CR-30154-NJR-1 (S.D. Illinois, 20 October 2019)
United States of America v. Aaron Michael Shamo, Drew Wilson Crandall, Alexandrya Marie Tonge, Katherine Lauren Anne Bustin, Mario Anthony Noble, and Sean Michael Gygi, Case No. 2:16-CR-00631-DAK (D. Utah, 31 May 2017)
United States of America v. William Staples, Case No. 19-2932 (3d Circuit 2020)
United States of America v. Andre-Catalin Stoica et al., Case No. 5-18-CR-81-JMH (E.D. Kentucky, 5 July 2018)
United States of America v. Kristjan Thorkelson, 14-CR-27-BU-DLC (D. Mont., December 10, 2018)
United States of America v. Vladimir Tsastsin, Andrey Taame, Timur Gerassimenko, Dmitri Jegorov, Valeri Aleksejev, Konstantin Poltev, and Anton Ivanov, Case No. 1:11-CR-00878 (S. D. New York, 14 October 2011)
United States of America v. Ross William Ulbricht, Case No. 15-1815 (2d Circuit 2017)
United States of America v. Joshua Aaron Vallance, Case No. 20 Cr. 08 (E.D. Kentucky, 28 May 2020)
United States of America v. Gal Vallerius, 2018 U.S. Dist. LEXIS 85620
United States of America v. Ronald L. Wheeler III, Case No. 1:17-CR-377 (N.D. Georgia, 15 November 2017)
United States of America v. Wendell Wilkins, Jalisa Thompson, Tiffany Reed, Brandon Thompson and Laben McCoy, Case No. 2-18-CR-101 (D. South Carolina, 14 November 2018)
United States of America v. Nathan Wyatt, 4:17CR00522 RLW/SPM (E.D. Missouri, 8 November 2017)
United States of America v. Eoin Ling Churn Yeng and Gal Vin Yeo Siang Ann, Case No. 3:16 CR 00090 (D. Oregon, 23 February 2016)
United States of America v. Caleb Young, Case No. 18-20128 (E.D. Michigan, 11 May 2018)

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 263-3389, www.unodc.org

V.21-05344