European Journal of Political Science Studies
ISSN: 2601 - 2766
ISSN-L: 2601 - 2766
Available on-line at: www.oapub.org/soc

DOI: 10.46827/ejpss.v4i1.935 Volume 4 | Issue 1 | 2020

ORGANISED CRIME: UNDERGROUND ECONOMY AND REGULATIONS TO COMBAT CYBERCRIME

Fulvio Greco[1],
Gianpiero Greco[1,2i]
[1]Ministry of the Interior,
Department of Public Security,
State Police, Italy
[2]orcid.org/0000-0002-5023-3721

Abstract:
Criminal organizations, with the advent of new information technologies, have found additional ways and spaces through which to commit crimes, especially in online hidden markets and through new means of laundering illicit proceeds. The opening of these new illegal markets has helped to increase the capital of criminal organizations which, if spread and rooted in the territory, can influence the various spheres of politics and decision-making processes of an entire country. Despite the seriousness of the threat, organised crime is not sufficiently understood. Although regulatory interventions and actions to prevent and combat cybercrimes perpetrated by organised crime have been implemented, through the international collaboration of the police forces with the various investigative agencies, the individual states intend to maintain full sovereignty in the area of criminal justice; all this leads to a lack of uniformity between both national and European institutions in the area of organized crime, while adequate regulation is still lacking in the dark web. In the light of the exponential increase in online criminal activity in recent years and even 25% between the first and second quarter of 2020 due to the coronavirus emergency, it is therefore essential that the individual Member States put aside uncertainties, exploiting the European Union as a fulcrum in the fight against transnational organised crime. A common solution would be to criminalize access to some areas of the Onion Routing, integrate the provisions of the article 416 of the Penal Code to apply them also to the digital context and establish the crime of mafia-type criminal association in the European legislative landscape as explained in article 416-bis of the Italian Penal Code.

Keywords: Interpol; Europol; Postal police; Criminal law; Darknet

[i] Correspondence: email gianpierogreco.phd@yahoo.com

1. The organised cybercrime

Organized crime is a form of associated delinquency which presupposes a stable organization of several people to commit multiple crimes, to obtain, directly or indirectly, financial or material advantages. Over the years, organized crime has diversified, become global and has reached macroeconomic proportions: illicit goods come from one continent, are trafficked in another, and traded in a third. Crime is fuelling corruption, infiltrating business, and politics, hindering development and governance by empowering those who operate outside the law. Despite the seriousness of the threat, organized crime is not sufficiently understood (Costa, 2010). In many cases, a lack of international understanding of terminology can cause incorrect legislative responses at the national level, which limit the effectiveness of crime control and prevention measures (Eu Parliamentary question, 2018). For example, the mafia should not be confused with a criminal association but represents an entity parallel to the public authority aiming to "*replacing them*" (Falcone, 1991). Yet, this distinction, made explicit in article 416-bis (Crime of Mafia-type association) of the Italian Penal Code, remains a unique case in the European legislative landscape. Thus mafia-type criminal organizations take advantage of softer legislation to transfer their business and interests there.

The danger highlighted by investigators, across Europe, is the conditioning these organizations have on the economy, the market and free competition. The expansion of the new means of communication enabled by network technologies has meant that connections, alliances, and commercial relationships have been established by optimizing and expanding the operations of criminal organizations around the globe. The digital revolution has also allowed organised crime to evolve, adapting to new technologies and innovating. Criminal groups today are decentralized and with the help of technology, they create channels and relationships in different countries with more actors, more means, using cutting-edge payment methods. Mafias around the world exploit information and communication in the same way as legitimate businesses and use cybercrime to finance their traditional operations (IOCTA, 2019).

The world of cybercrime, especially in recent years, is home to a multiplicity of actors of different kinds: from cyber-terrorists to individual hackers, from old criminal organisations to new specialised groups committing offences on the net. Organised crime groups operate on the net with different functions and social impacts (McGuire, 2012). An increasing number of academic studies and reports from cybersecurity companies demonstrate the varieties of organizational structures that are involved in cybercrime and have expanded the notion of organized crime to profit-related criminal phenomena occurring completely or partially in cyberspace (Leukfeldt, Lavorgna, & Kleemans, 2017). There are in fact forms of crime that operate exclusively online, others that operate in a mixed manner and still others, mainly offline (Leukfeldt et al., 2017). The digitized organized criminal groups act in a specific way in the cryptocurrency relationship and anonymous networks, playing three key roles to carry out the various illicit activities.

a) Criminal organizations can become *'suppliers of products and services'* by acting through the *'.onion'* sites in the Darknets that lend themselves to proliferating illicit

businesses. The multiple products sold range from drugs to weapons, malware and illegally acquired personal data and information and then resold on online markets. Another traditional activity under the influence of organized crime is the online gambling which manages huge volumes of transactions and cash flows which unfortunately can hide and mask money laundering (Romiti, 2014). Suffice it to say that the number of unauthorized sites exceeds by more than ten times that of operators who are (Romiti, 2014). Many of these sites, if not most (Choi, 2018), operate in the Darknets allowing payments through cryptocurrencies. These methods thus make illegal gaming portals protected by anonymity. All goods and services made available in the Darknets can be purchased through cryptocurrency and it is, therefore, necessary for organizations to invest in bitcoin or other types of virtual currencies to kick-start such mechanisms.

b) Furthermore, criminal organizations can become *'cryptocurrency investors'*. In addition to the misuse of it in Darkmarkets, there are several reasons why organized crime wants to invest in cryptocurrencies (that is, a digital payment method based on blockchain technology and cryptographic procedures such as hash functions and digital signatures). Not being supported by any central government or authority, they are not subject to the political or economic pressures that regulate central bank and private money issuing authorities (Matonis, 2012). Transactions can be carried out across borders without the limits that come from the extensive authorization process required for the use of credit cards (J.P. & G.T., 2011). This combination of elements makes crypto-currency highly attractive to criminal organizations, not only to operate illicit online markets but as a means for other criminal purposes and investments. One of the main purposes of criminal organizations is to remove money from its illicit origins, hindering the traceability of the origins of the proceeds. Cryptocurrencies are a new way of hiding the identity of illegally generated proceeds, and a way of hiding the identity of the user. The use of cryptocurrencies in the context of cyber money laundering is an activity that has entered the practice of many criminal organizations (Irwin & Milad, 2016); money can be laundered faster through virtual currencies than traditional means, having the ability to divide the capital into multiple accounts. Finally, organized crime would be investing in the stock exchange and Bitcoin (Cipolla, 2018), precisely to pursue purposes related to money laundering.

c) Finally, criminal organizations interface with the Onion Routing (i.e. the technique that makes network communications anonymous) and cryptocurrencies through direct involvement in a cyber action *'acting as a guiding hand'* in certain operations. These actions are perpetrated through the recruitment of personnel qualified in the use of IT techniques or by real cybercriminal groups that act exclusively online. Forms of organized cybercrime take the opportunity to carry out numerous attacks aimed at destroying, abusing, or blocking computer systems (IOCTA, 2019). In addition to viruses or malware that cause serious damage to databases, software or websites, a crime particularly perpetrated by cybercriminals is extortion through computer networks (IOCTA, 2019). Extortion on computer networks has become a regular practice in recent years and many organized groups follow this example through the

help of DoS (i.e. Denial-of-Service that persists in an attempt to prevent legitimate users to access information or services within your system) or malware, using cryptocurrencies and anonymity to make you lose track of your work. Through skimming, phishing, banking Trojans (program intent on spying on a banking computer) or other online fraud, the carders acquire credit card numbers or violate banking systems and then resell all the material on the dark web. The explanation for this behaviour is that it seems easier to sell stolen credit cards than to use them. The Darknets markets ensure the anonymity of transactions allowing carders to remain safe.

2. The underground economy of organised crime in the digital age

The underground economy of cybercrime is extremely vast, and its size and structure are often difficult to understand. Today the 'Darkmarkets' host a multiplicity of participants and are constantly changing due to their illegal nature. Despite this, over time the black markets of the network have established themselves, creating their ever-growing clientele (IOCTA, 2019). A market of this kind is nothing more than a hidden service implemented by anonymous software, such as the Onion Routing that makes users' IP addresses untraceable. Illegal trade is enabled by the sites loaded on such services which allow buyers and sellers to interact and trade anonymously. The 'Darknets' markets allow payments through cryptocurrencies by obfuscating transactions. There are currently two types of dark web commercial entities: 'crypto-markets' and so-called 'vendor shops' (Paoli et al., 2017), single sellers, connected or linked to markets.

Crypto markets bring together multiple sellers managed by a group of market administrators (i.e. of the web page) in exchange for a commission on sales, an activity that mirrors what happens in the 'Clearnet' with Amazon and eBay. The services offer exchange methods that allow transactions to be made, using cryptocurrency, followed by feedback (on a scale from 0 to 5 stars) linked to each purchase, with aggregate scores and viewable on the marketplace to guide the customers in the selection of reliable suppliers and highly qualified products (Van Hout & Bingham, 2013). Precisely this system makes crypto-markets unique, offering a bilateral reputation mechanism that instils trust in both merchants and buyers, protecting the anonymity of both and facilitating repeated transactions (Hardy & Norgaard, 2016). Crypto-markets tend to specialize primarily in the sale of illegal drugs (Aldridge & Décary-Hétu, 2014) or related products, but they also offer listings linked to other fraudulent activities, including stolen credit cards, identity information, and firearms, less commonly available for sale than the other categories (Paoli et al., 2017).

The other type of activity available in darknets is the so-called *vendor shop*, also known as a 'single seller shop', pages created directly by the supplier of the product or service, which in many cases trades in parallel on a crypto-market. Vendor shops on the dark web are positioned as points where specialized products are sold, with particular attention to the arms trade (Paoli et al., 2017), as opposed to crypto markets that offer many products and services.

This underground economy must not be understood as a unitary system, on the contrary, the Darkmarkets differ from each other especially about the country of origin (Trend Micro, 2015). Today, the expansion of the phenomenon of online darkmarkets is enormous and tends increasingly using new technologies to refine. Being a constantly changing reality in a vast world like that of the web, despite the differences that exist between the different markets, cybercriminals collaborate, sharing tools, information, know-how and best practices aimed at improving illegal trade in the network. The most selected product categories in the darkmarkets are drugs, fake documents, counterfeit banknotes, credit card or bank account data, weapons, and explosives, as well as malware and other hacking tools. Thus, to prevent any risks associated with controls, there are various techniques for hiding products, discussed, and implemented on dedicated forums, both on the dark web and on clearnets (Paoli et al., 2017). One of the most used techniques is to ship products together with others, such as those associated with consumer electronics: printers, smartphones, televisions, or in instrument cases with a double bottom (Paoli et al., 2017). The commercial system of the crypto-markets ensures as well as the guarantee of product quality through feedback, quality and safety in shipping or prior agreements or pre-established rules, creating a structured model with a monthly turnover of tens of millions of euros (EMCDDA, 2019).

One of the most perpetrated activities in Darkmarkets, usually immediately after the sale of drugs, is the supply of false documents (Europol, 2017), such as passports, identity documents, driving licenses, birth certificates, etc. On the Darkmarkets, from their creation to the present day, the buying and selling of stolen account information, bank accounts and credit card numbers continues. Personal and bank data are often the second or third category of 'raw materials' listed in the darkmarkets and one of the most common products highlighted by law enforcement (IOCTA, 2019). In the Darkmarkets, in addition to weapons and explosives, ammunition, knives, ordnance equipment and digital products for support are sold, such as eBooks that provide instructions for the manufacture and assembly of explosives and weapons (IOCTA, 2019).

Another type of weapons, particularly fashionable in the digital age, sold in dark networks are 'malware': malicious programs ranging from simple frequency recording software to steal sensitive data from the user to sophisticated and professional software that can intercept, alter or hijack the victim's data (IOCTA, 2019). Research on the topic highlights the growing distribution of these digital tools, among the biggest sellers are 'ransomware' (Broadhurst et al., 2018), a program that disables a victim's device until a ransom is paid which frees the system from the block. In addition to these, we find the distribution of Trojans or viruses such as *'exploits'* (i.e. crime-ware to extort money or sensitive data from PC) and *'botnets'* (i.e. nets composed of devices infected with specialized malware, called bots or zombies) capable carry DoS (Denial-of-Service) attacks or related DDoS (Distributed Denial-of-Service) attacks, particularly harmful. Every banking institution, company or public administration uses computerized systems that can be an easy target by malicious people intent on blocking a system for the purpose not only of extorting sensitive information but of destabilizing entire IT structures dedicated to providing essential services.

Another growing activity, especially in recent years, is the online gambling industry (Choi, 2018) which, with the use of cryptocurrencies, is exploited for money laundering purposes (Fiedler, 2013). Millions of transactions take place daily on the Internet and criminal organizations have been taking advantage of this for more than two decades to launder illegally acquired funds through secret and anonymous online transactions (Richet, 2013). Cyber money laundering depends on the use of various types of transactions and financial service providers, ranging from bank transfers, cash deposit/withdrawal to e-money and cryptocurrency transactions (EAG, 2014). An incisive push towards the digitalization process of money laundering was the introduction of virtual currencies and subsequently of cryptocurrencies (UIF, 2018).

3. Regulations and public policies in the fight against the underground economy of digitised organised crime

As previously highlighted, the expansion of digital media has meant that organized crime has evolved, adapting to new technologies and innovating; therefore, criminal organizations have evolved from traditional crimes to 'cybercrimes'. By *cybercrime* we mean a set of crimes (Cadoppi et al., 2019) that can be configured: *a)* when the computer is used as a target (e.g., abusive access to a computer to collect or eliminate data (e.g., DoS and DDoS), dissemination of viruses and malware to lock down the system or other hacking functions); *b)* when using the computer as a means or tool used to commit any criminal conduct (e.g., the different types of telematic fraud (i.e., carding, phishing, etc.) or online harassment); *c)* when the computer is used as an accessory for crime, that is, all those activities that would have been carried out equally but that can be helped by the use of the computer (e.g., child pornography, money laundering, or trade online). Cybercrime occurs in a split second and can spread with surprising speed (Brenner & Clarke, 2004). Law enforcement and security agencies must therefore act quickly and be able to collect and store digital evidence for use in criminal proceedings. However, information and communication technologies are unfamiliar to the traditional world of criminal justice and, therefore, practitioners must constantly retrain the sector by requiring well-trained personnel in new techniques in the investigation phase, during criminal proceedings and in the courts (Chaikin, 2006). Furthermore, to effectively address cybercrime repression problems, different national criminal justice systems need to update their legislation and law enforcement systems as they are unable to cope with the investigation and prosecution of the crime phenomenon.

3.1. An International overview

There are several international agreements including the 'Budapest Convention' also known as 'The Cybercrime Convention' and the 'Framework Decision 2013/40 /EU' related to complementary operational bodies (such as police forces acting at national and supranational level), which they seek to provide new tools and improve international cooperation. The International Criminal Police Organization, *Interpol*, is committed to being a global coordinating body for the detection and prevention of digital crimes.

Interpol through the Global Complex for Innovation (2014) aims to share skills and avoid duplication of activities already underway, so that law enforcement agencies can effectively focus their resources on the fight against cybercrime, collaborating with others stakeholders to develop a coordinated response to this growing threat. The countries of the G7 (G8 from 1998 to 2014) (UNIDIR, 2020) during the various meetings went to emphasize more and more the danger represented by cybercrime, while the OECD (Organization for Economic Cooperation and Development) hosts within it, one of the most effective organizations for intergovernmental coordination of law enforcement agencies, offering models for transnational cooperation against cybercrime: the International Financial Action Group. It is an intergovernmental organization whose goal is the implementation of legislative and regulatory reforms necessary to combat money laundering.

3.2 A European overview

Within the European Union, several supranational institutions are included that address the challenges posed by international cybercrime by adopting common positions, directives, and other tools to combat a wide range of criminal activities. The decision, following the ratification of the Budapest Convention, is the beginning of a path of harmonization of the legislation aimed at the fight against cybercrime in the various member states of the European Union. Precisely to increase cooperation in the judicial sense, which goes beyond a network of contacts, in 2002, the *Eurojust* was set up by the Council of Ministers of the European Union, a body which brings together the judicial institutions of the various countries with the aim of criminal cooperation. One of the results of the Eurojust meetings was the foundation, in 2016, of the *Eurojust European Judicial Cybercrime Network* (EJCN, 2016), a network aimed at fostering contacts between professionals and specialists in countering the challenges posed by cybercrime. Fully integrated into the European Union, with the Council decision 2009/371/JHA on 6 April 2009, is *Europol*, that is the EU police office which today represents one of the reference bodies for the fight against cybercrime; Parliament adopted a new regulation (2016/794) on 11 May 2016 to allow Europol to intensify its efforts to combat terrorism, cybercrime as well as organized crime and serious forms of crime. The Decision also went to strengthen the European commitment against serious forms of organized crime as described in the working document on organized crime (2012). Thus, an attempt was made to facilitate the exchange of information, provide analyses, strategic reports on trends and patterns of criminal activity, exchanging technical expertise for ongoing investigations within the EU.

In 2013 Europol established the *European Cybercrime Centre*, an operational body that deals with cybercrime, basing its work on operational, technical, and analytical support for Member States' investigations. The centre, the result of Directive 2013/40/EU promulgated by the Parliament and the Council, has as its task the fight against cybercrimes committed by organized groups, in particular those that generate large profits such as online fraud, the sexual exploitation of minors online, cyber-attacks targeting critical European infrastructure systems and trade in dark networks, including

cyber money laundering. The group is engaged every year in drafting a strategic report on key discoveries, emerging threats and developments in cybercrime called 'Internet Organized Crime Threat Assessment' (IOCTA). The document provides key recommendations for law enforcement and policymakers to enable them to respond to cyber threats effectively and in concert (IOCTA, 2019). The fundamental role played by this set of institutions, however, remains severely limited, lacking an autonomous power of initiative in the criminal field. This may be due to a certain reluctance of Member States to deprive themselves of a part of sovereignty as important and linked to the territory as that deriving from the exercises of the police forces.

3.3 An Italian overview

In Italy, a step forward was made by the Decree of the Minister of the Interior of 28 April 2006, entitled *"Reorganisation of the speciality sectors of the Police Forces"*. The Decree determined the *Postal Police* as a body specializing in combating crimes perpetrated through the Internet and the use of computerized electronic means, thus making the body the major national actor in the fight against cybercrime. With a further ministerial decree dated January 9, 2008, the CNAIP, the *National Cybercrime Centre for the Protection of Critical Infrastructures*, was officially established, a non-executive level organizational unit, based on the Postal Police service. A few months later, the 2001 Budapest Convention was officially ratified, with the law of 18 March 2008, n. 48, among which the main changes added to the Italian Penal Code is article 615-quinquies "*Dissemination of equipment, devices or computer programs aimed at damaging or interrupting a computer or telematic system*" (also referring to those who wish to spread different types of malware or programs aimed at committing a crime on the Internet through the dark web). Over time, the Postal Police has tried to limit activities in the Darknet by helping to refine methods and tools shared in the context of international police collaboration with various foreign investigative agencies and making use of the coordination of Europol's European Cybercrime Centre (J-CAT, 2020). The central problem, about investigations on the matter, remains the anonymity which in its evolution is showing more and more impermeability to intrusion attempts by the security bodies. By not allowing the traceability of criminals operating in the Darknets, the police forces cannot impute those responsible.

3.4 Developments in Criminal Law

In addition to the various initiatives undertaken (i.e., Global Complex for Innovation and European Cybercrime Centre of Europol), we must think of a coercive regulatory response that knows how to put a margin both on the disproportionate use made by the hidden services of darknets and on the spread of criminal organizations, traditional or otherwise, in the network scenario. The process of harmonization of national laws, coming from the EU institutions, is the ideal tool of Community law to trace this path. The laws of the Member States are different, and these differences can hinder the achievement of the objectives set out in the Treaties. Harmonization is how to eliminate or reduce these disparities. Since the Maastricht Treaty, criminal justice issues have been

considered the exclusive domain of the Member States, considering the need for harmonization of criminal law to be marginal. After more than ten years, to face the challenge of cross-border crime, the Treaty of Lisbon (2007) introduced the possibility for the European Union to legislate in criminal matters through the use of the directive; an instrument that binds the Member States to achieve a certain result, leaving the possibility for national bodies to choose the form and means with which to implement it. The abolition of the pillar structure of the Amsterdam Treaty allowed the Parliament and the Council to become decision-makers also in criminal matters, making Europol fall within the legal framework of the Union. In particular, in the fourth chapter of the Treaty on the Functioning of the European Union (TFEU, 2012), entitled *"Judicial Cooperation in Criminal Matters"*, article 82 traces the framework of competences of the European Union in the field of criminal procedure (such as mutual admissibility of evidence between the Member States) and article 83 performs a similar task in the field of substantive criminal law. The latter provides that the European Union may, using directives, dictate *"minimum regulations relating to the definition of crimes and sanctions in particularly serious crime areas that have a transnational dimension deriving from the character or implications of such crimes or from a particular need to fight them on a common basis"*. Among the areas of crime considered are present in the article: *"terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, cybercrime and organized crime"*.

Up to now, the current influence of the European integration model about the criminal field has been limited and well below the potential offered by Article 83 of the TFEU (2012). This is because there is still no real desire for judicial harmonization in the broad sense extended to all member states of the European Union. In addition to the mutual recognition of cooperation between judicial and police forces, common problems must be reacted with common solutions, especially in the digital age, in which national borders are not enough to contain the new threats coming from the net. A common solution could be to criminalize access to some areas of the Onion Routing, discouraging customer access to Darkmarkets. The Onion Routing allows users to create sites, exactly like those on the web on the surface, acting as a server. These 'hidden services' are the technology behind Darkmarkets and other commercial activities through which organized criminals carry out numerous illegal acts. It is therefore important both nationally and internationally that access to certain hidden services be criminalized so that the police can use them in the processual phase. Another solution could be to harmonize European legislation on the criminal association as provided for in article 416 of the Italian Penal Code, both online and when it comes to *criminal organizations* of the mafia type. Since article 416 of the Penal code was written at a time when digital communications did not exist, the criteria to be used to verify its application in the virtual context appear uncertain today. It is thus necessary to integrate the provisions of article 416 of the Italian Penal Code to ensure that they can also be applied to the virtual context. If our operating systems become "domiciles" it is right to make the owners responsible for controlling them. The Supreme Court has expressed in this regard that the violation of an IT system is equal to the violation of domicile (Penal Cassation no. 36338/2015), with

reference to article 615-ter of the Penal Code, *"Unauthorized access to an IT or telematic system"*. The new digital means that provide access to the net are potential weapons through which organized groups can commit electronic fraud, abusive access or publish child pornography, and it is right that they are linked to the legitimate responsible owner. In Europe, the contrast of mafia-type criminal associations remains a debated and evolving issue. The starting point of any response originates from the provisions provided by the Italian criminal law system, from article 416-bis of the Penal Code which establishes the *criminal association of the mafia type*.

4. Conclusions

Criminal organizations exploit the Internet, as a vast unregulated space, to transfer their activities online, using anonymity techniques to guarantee immunity. Criminal networks, with the arrival of new network technologies, have found further ways and spaces through which to commit a crime, especially in online darkmarkets and through new means of laundering illicit proceeds. Furthermore, the organizations engaged in these commercial activities have expanded their sales sphere to an increasingly large international clientele, thus increasing their earnings prospects and exploiting new means of payment such as cryptocurrencies to launder money, evading many of the controls imposed on financial institutions by anti-money laundering laws. The opening of new illegal markets has helped to increase the turnover of organized crime by billions of euros (UNODC, 2011). Such huge sums of money, the result of illicit sales, are invested in building contracts, bars, restaurants, shops and betting centres, which in addition to having the function of cleaning up dirty money, increase the capital of criminal organizations which, if widespread and rooted in the territory, they can influence the various spheres of politics and decision-making processes of an entire country.

To try to understand what the responses are aimed at combating these new criminal phenomena, a regulatory framework and institutions have been outlined to combat illegal activities in the Darknet. Although progress has been made in trying to keep digitised organised crime under control, there is still a lack of uniformity between national and European institutions in this area, while there is still no adequate regulation of the dark web. Articles 82 and 83 of the TFEU (2012) give the Union's decision-making bodies powers in criminal matters, but these powers today remain unexercised. One of the main causes remains the willingness shown by States to maintain full sovereignty in criminal justice, especially in the current crisis of the European institutions. However, in the light of the exponential increase in online criminal activity in recent years and even 25% between the first and second quarter of 2020 due to the coronavirus emergency (Zorloni, 2020), it is therefore necessary that the individual Member States put aside uncertainties, using the European Union as a fulcrum in the fight against transnational organized crime. A common solution could be to criminalise access to certain areas of the Onion Routing and integrate the provisions of article 416 of the Penal Code (criminal association) to ensure that they can also be applied to the digital context. Furthermore, it would be desirable that the crime of mafia-type criminal association be finally established

as specified in article 416-bis of the Italian Penal Code, as it is still a case unique in the European legislative landscape.

Conflict of interest

The authors declare no conflicts of interest.

Authors' contribution

Both authors contributed equally to the conception and writing of the manuscript.

References

Aldridge, J., & Décary-Hétu, D. (2014). *Not an 'Ebay for Drugs': the Cryptomarket 'Silk Road' as a paradigm shifting criminal innovation.* Available at SSRN 2436643.

Board meeting joint cybercrime action taskforce (J-CAT) (2020). Available at https://www.commissariatodips.it/notizie/articolo/board-meeting-joint-cybercrime-action-taskforce/index.html

Brenner, S. W., & Clarke, L. L. (2004). Distributed security: Preventing cybercrime. *John Marshall Journal of Computer & Information Law*, *23*, 659.

Broadhurst, R., Lord, D., Maxim, D., Woodford-Smith, H., Johnston, C., Chung, H. W., ... & Sabol, B. (2018). *Malware trends on 'darknet' crypto-markets: Research review.* Available at SSRN 3226758.

Cadoppi, A., Canestrari, S., Manna, A., & Papa, M. (2019). *Cybercrime*. Vicenza: UTET Giuridica.

Chaikin, D. (2006). Network investigations of cyber-attacks: the limits of digital evidence. *Crime, Law and Social Change*, *46*(4-5), 239-256.

Choi, S. (2018). *Illegal Gambling and Its Operation via the Darknet and Bitcoin: An Application of Routine Activity Theory.* In BSU Master's Theses and Projects. Item 64. Available at https://vc.bridgew.edu/theses/64/?utm_source=vc.bridgew.edu%2Ftheses%2F64&utm_medium=PDF&utm_campaign=PDFCoverPages

Cipolla, A. (2018). *Antimafia: "Così la Camorra guadagna con la Borsa e i Bitcoin".* Available at https://www.money.it/antimafia-camorra-guadagna-borsa-bitcoin

Costa, A.M. (2010). *The Globalization of Crime - A Transnational Organized Crime Threat Assessment, preface by executive director p. iii. UNODC Report.* Retrieved from https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

Decree of the Minister of the Interior of 28 April 2006. Retrieved from https://www1.interno.gov.it/mininterno/site/it/sezioni/servizi/old_servizi/legislazione/polizia/legislazione_769.html

Decree of the Ministry of the Interior of 9 January 2008. Retrieved from https://www.poliziadistato.it/statics/44/d.m.-9-gennio-2008-istituzione-cnaipic.pdf

Directive 2013/40/UE. Retrieved from https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX%3A32013L0040

EJCN (2016). Retrieved from http://www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx

EMCDDA, 2019. Retrieved from https://www.emcdda.europa.eu/edr2019_en

Eu Parliamentary question (2018). Retrieved from https://www.europarl.europa.eu/doceo/document/P-8-2018-005054_IT.html

Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) (2014). *Cybercrime and Money Laundering*. Retrieved from https://eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014_English.pdf

Eurojust (2002). Retrieved from http://www.eurojust.europa.eu/press/PressReleases/Documents/2018-04-26_Eurojust-FactSheet.pdf

European Cybercrime Centre (2013). Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Europol (2016). *Regulation (EU) 2016/794.* Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0794

Europol (2017). *Priority for the Eu policy cycle from 2018 to 2021. Document fraud*. Retrieved from https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact

Falcone, G. (1991). *Cose di Cosa Nostra*. Rizzoli.

Fiedler, I. (2013). *Online Gambling as a Game Changer to Money Laundering?* Available at SSRN 2261266

Hardy, R. A., & Norgaard, J. R. (2016). Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. *Journal of Institutional Economics*, *12*(3), 515-539.

Internet Organised Crime Threat Assessment (IOCTA) (2019). Report retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

INTERPOL Global Complex for Innovation. Retrieved from https://www.interpol.int/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors

Irwin, A. S., & Milad, G. (2016). The use of crypto currencies in funding violent jihad. *Journal of Money Laundering Control, 19*(4), 407-425.

J. P. & G. T. (2011). *Bits and Bob, The Economist: Babbage 13-06-2011.* Retrieved from https://www.economist.com/babbage/2011/06/13/bits-and-bob

Law n. 48 of 18 March 2008. Retrieved from https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2008-03-18;48!vig=

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, *23*(3), 287-300.

Matonis, J. (2012). ECB: Roots of Bitcoin Can be Found in The Austrian School of Economics. *posted to Forbes (online), November 3*, 2012.

McGuire, M. (2012). *Organised Crime in the Digital Age.* London: John Grieve Centre for Policing and Security.

Paoli, G. P., Aldridge, J., Ryan, N., & Warnes, R. (2017). Behind the Curtain: The Illicit Trade of Firearms. *Explosives and Ammunition on the Dark Web, RAND Corporation, Santa Monica, CA*.

Penal Cassation n. 36338/2015. Retrieved from http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snpen&id=./20150909/snpen@s10@a2015@n36338@tS.clean.pdf

Penal Code (2020). Retrieved from https://www.brocardi.it/codice-penale/

Richet, J. L. (2013). *Laundering Money Online: a review of cybercriminals' methods*. Available at https://arxiv.org/abs/1310.2368

Romiti, M. L. (2014). *Riciclaggio e gioco d'azzardo on line. Il dark web sfrutta i "casinò" in rete*. Retrieved from https://www.repubblica.it/economia/affari-e-finanza/2014/05/12/news/riciclaggio_e_gioco_dazzardo_on_line_il_dark_web_sfrutta_i_casin_in_rete-85884848/

Treaty of Lisbon (2007). Retrieved from https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:12007L/TXT

Treaty on the Functioning of the European Union (TFEU) - Consolidated version (2012). Available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:IT:PDF

Trend Micro (2015). *Cybercrime and the Deep Web - Forward-Looking Threat Research (FTR) Team*. Available at https://www.trendmicro.com/vinfo/it/security/news/cybercrime-and-digital-threats/qna-deep-web-anonymity-and-law-enforcement

UNIDIR (2020). *Cyber Policy Portal. Group of Seven (G7).* Retrieved from https://unidir.org/cpp/en/organization-pdf-export/eyJvcmdhbml6YXRpb25fZ3JvdXBfaWQiOiI2In0

Unità di Informazione Finanziaria per l'Italia (UIF) (2018). Casistiche di riciclaggio e di finanziamento del terrorismo. *Quaderni dell'antiriciclaggio, n.11.*

UNODC (2011). *Estimating Illicit Financial Flows Resulting from Drug Trafficking and other Transnational Organized Crime.* Research report retrieved from https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

Van Hout, M. C., & Bingham, T. (2013). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy*, *24*(5), 385-391.

Working document on organized crime (2012). Retrieved from https://www.europarl.europa.eu/meetdocs/2009_2014/documents/crim/dt/913/913961/913961it.pdf

Zorloni, L. (2020). *L'Europa lavora alle nuove regole sulla cybersecurity per alzare le difese*. Retrieved from https://www.wired.it/internet/regole/2020/09/17/cybersecurity-europa-direttiva-nis/