DOI: 10.38146/BSZ.SPEC.2021.6.7

Ivett Nagy

Drug crime transformation under the effect of online platforms

Abstract

Many types of drug crimes are already known, but it is common to offender groups to implement them in an organised, coordinated, multi-level framework. Affected by online platforms, drug crimes are undergoing a transformation that presents new challenges for the authorities. Criminal groups also like to (re)take the opportunities offered by the Internet. Platforms that connect to the Dark Web, the Dark Internet (secret network form), have become increasingly popular over the past few years, thanks to the fact that there are also services available which are not available by traditional browsers. Coordinated cooperation between several countries, over several years, is needed to ensure successful detection in cyberspace. This is illustrated by a current EUROPOL report, published on 12 January 2021, which shows that a successful liquidation has occurred in the case of DarkMarket, one of the largest illegal marketplaces, requiring the cooperation of several European Union Member States and several non-European Union countries. In the face of the coronavirus epidemic, organised crime groups are still trying to remain active and resilient, which is not a challenge in the online space at this time, although drug delivery models needed to be changed, but they are trying to maintain the constant cycle of the market through their hiding methods. In my study, I am also looking for answers how the detection and recovery of criminal property is carried out at national and international level, in cases where drug crime takes place in the online space. What is the path of illegally acquired criminal property, how can financial profiling be carried out in these cases? In case of drug offences, we are talking about a special asset recovery where is no victim demanded, because there are very few known victims existing. With my study, I intend to capture the current topicality of drug crime, by detecting methods of committing crimes in the online space, internationally and domestically, and by exploring the current processes of asset discovery and recovery. In this way, I wish to provide results that can be used by the profession.[1]

1 The project TKP2020-NKA-09 was completed with the support of the National Research Development and Innovation Fund and financed by the Thematic Excellence Program 2020.

Keywords: cybercrime, dark web, drug markets, asset recovery, coronavirus pandemic

About organised crime and the link between drugs and crime

Organised crime is one of the most complex phenomena, the causal and other forms of which have long been dealt with by various experts, since the fight against organised crimes is constant, just as the typical characteristics of certain crimes of organised crime are considered to be constantly changing in the system (Szűcs, 2020). All organised crimes require serious logistics, consistency, trust and organisation from the perpetrator's side. Just think of how much resources it takes to run a people-smuggling network, which requires both material and human resources. The fight against organised crime is a priority for most countries. This is not different for Hungary, but the opportunities offered by the European Union also contribute greatly to successful action. In case of drug offences covered by organised crime, the need to act within the European Union appeared at a time when the Schengen Area was also established in 1985, allowing the free movement of capital, goods, services and persons without control at borders. At the same time, however, a number of security risks have emerged in countries (in the member states of the European Union) that have not been seen before. At the end of the 1980s, restrictions were introduced to curb the free movement of drugs within the European Union. The emergence of regulations for new synthetic drugs (known by their name: for example, crocodile, crystal) was also urgent in the legislation. As a result, new authorities were created within the European Union and within the United Nations which include the EMCDDA[2] or the UNODC[3], but there have also been a number of forward-looking models with the establishment of EUROPOL[4], CEPOL[5], or EMA[6]. Some statistics show the importance of the topic in the European Drug Report published in 2021:

'In 2019, an estimated 1.5 million drug law offences were reported in the European Union, an increase of almost a quarter (24 %) since 2009. Most of these offences (82 % or 1.2 million) are related to personal use or possession.'

2 European Monitoring Centre for Drugs and Drug Addiction.
3 United Nations Office on Drugs and Crime.
4 European Union Agency for Law Enforcement Cooperation.
5 European Union Agency for Law Enforcement Training.
6 European Medicines Agency.

'Of the estimated 1.5 million drug law offences, the drug mentioned in the offence is reported in just over 1 million offences, of which 826 000 were for possession or use, 176 000 were for supply related offences and 7 500 were for other types of offence.' (URL1)

In addition to the above, the European Union's ambitions are illustrated by the part related to the supply of drugs within the drug strategy issued for the following period. *'In the field of drug supply reduction, the objective of the EU Drugs Strategy 2013-2020 is to contribute to a measurable reduction of the availability of illicit drugs, through the disruption of illicit drug trafficking, the dismantling of organised crime groups that are involved in drug production and trafficking, efficient use of the criminal justice system, effective intelligence-led law enforcement and increased intelligence sharing. At EU level, emphasis will be placed on large-scale, cross-border and organised drug-related crim*e.' (URL2). Strategies however do not mention drug crimes in cyberspace back in2012. The links between drugs and crime are part of another area of research, but I think it is important to note that the important thing for the investigation is that drug-related crimes are carried out depending on the motivations of the perpetrators, which may have different outcomes. Where production, trafficking and consumption of drugs take place in an organised framework, it can be said that other crimes, including corruption offences, also take place during these processes. But there are other identifiable crimes in which it is common that they occur in parallel with drug offences, such as economic crimes (fraud, embezzlement, money laundering, typically white-collar crimes) or crimes committed for profit, which can even happen on an occasional basis (burglary, robbery, theft) (URL3). In contrast, the study will also present, among other issues, typical cases of drug offences in the online space.

The boundless cyberspace

Cyberspace as a concept has been enriched with countless interpretations in recent times, depending on the area in which we deal with the subject. Cyberspace crimes, also known as cybercrimes, are considered important for the study. Since the emergence of the Internet people's lives have become easier, the flow of information and globalization have accelerated as well. When it comes to the benefits of them, it is enough to think only about the pandemic period, when you did not even have to go out and yet everything was 'available' over the Internet. In terms of disadvantages, it can be observed that organised crime groups are also increasingly present in cyberspace, thus creating threats and an increase

in the number of victims. The following three categories of cyber-crime can be distinguished (URL4):

'I. 'Classic cybercrime': phishing, cyberattacks, internet scams, online banking scams
II. Online sexual exploitation of children: child pornography, other crimes against sex (sexual blackmail, recruitment) and sexual morality
III. Credit card crime' (Gyaraki, 2017).

The above-mentioned crimes may also be committed by using the most commonly used web browsers, such as Google Chrome or Internet Explorer. In particular, a classic internet scam may be carried out on social media platforms as well, which – however - do not fully ensure the identity of the perpetrator. Although he wishes to be anonymous (registering with a fictional profile hiding an IP address), he is still unable to do such thorough work. The investigating authorities are using all means at their disposal to ensure that anonymity is broken. A much more hidden side of cyberspace is the deep web. *'Anonymous networks: Different sub-networks of the Internet, such as Tor, Freenet and I2P, inside of which the users' identities and locations are masked and all the communication is encrypted. Also referred to as the Darknet or the Dark Web.'* (URL5). One of the main features of deep web is that it is not indexed by search engines, which allows users to browse networks that are not present on other networks. The use of the darknet gives perpetrators access that is anonymous and untraceable, yet the investigating authorities have the methods by which this can be overturned. One of the best known among the perpetrators is the deep web search engine TOR[7], but in addition to that, there are many other networks, such as I2P and Freenet. Perpetrator groups treat these networks as marketplaces where goods are traded that are typically illegal (such as weapons, drugs, various services). On the international outlook, I would like to mention some successful investigations. One of these successful investigations was the FBI[8]'s dismantled Silk Road in 2013 (also known as 'Amazon to drugs' or 'Ebay of drugs'), one of the most well-known online drug markets of that period. In terms of revenue, it was about USD 22 million. The site's operator, 'Dread Pirate Roberts,' was arrested and charged with multiple crimes (such as computer hacking and money laundering conspiracy). The FBI said that in addition to all this, Bitcoins worth of USD 3.6 million were seized, which also meant that cryptocurrency trading

7 The Onion Router.
8 Federal Bureau of Investigation.

was already in full swing in 2013 (URL6). In connection with that, it is to be noted that several types of cryptocurrencies are known, but one of the most well-known is Bitcoin, which is also a popular currency on black markets because it is not necessary to reveal the identity of the bitcoin owner for trade. As regards the concept of bitcoin can be summarized as *'Bitcoin is a decentralized digital currency that you can buy, sell and exchange directly, without an intermediary like a bank. Bitcoin's creator, Satoshi Nakamoto, originally described the need for an electronic payment system based on cryptographic proof instead of trust.'* (URL7). As illustrated by a more recent example, on 12 January 2021 the EUROPOL report was published, which reads that a successful unmasking took place on DarkMarket, one of the largest illegal marketplaces, it was a successful reconnaissance requiring cooperation from several European Union Member States and several non-European Union countries (e.g., Ukraine, the United States of America, Australia), resulting, inter alia, in the arrest of the suspected operator of DarkMarket. The illegal marketplace DarkMarket had almost 500,000 users, trading drugs, stolen credit card data, and malicious codes suitable of launching cyberattacks, among other things. In addition, 320,000 illegal transactions were carried out (URL8). Through successful detection, it became clear that there had been a rise in drug crime that had hitherto been unknown to the authorities.

Ways of committing drug crimes online

Anyone can browse the various search engines (in addition to other browsers) mentioned above, which are called the 'Surface Web'. The question arises, observing the realizations of drug crimes in recent years, whether it is the conceivable deep web that could be the new way to trade drugs? In addition to this, anonymous systems have been created on the black market to which access is granted without an IP address, i.e., identification by the investigating authorities is made difficult. According to an article of June 2019, the big drug lords and drug traffickers known to everyone, who have accumulated billions of dollars, are nothing compared to the revenues of cybercriminals. *'By 2021, cybercrime is expected to cost the world $6 trillion yearly, making it more profitable than the global illegal drug trade, according to data provider Cybersecurity Ventures.'* (URL9) Furthermore, according to some researchers, there is a growing industry in terms of cybercrime. Offenders target people who live in a jurisdiction other than their own. Another interesting point is that central countries for cybercrimes include India, Vietnam, Brazil and North Korea (URL10).

With regard to Hungary, the crime of drugs in the online space has become more and more frequent in recent times. According to the experts, this is not related to the coronavirus pandemic, although it was considered important to point out in connection with the study that the crime is increasingly shifting towards the online space.

At the beginning of the research, the question arose how and from what source the investigating authorities would become aware of drug offences committed in the online space. During discussions with professionals, they said that in the vast majority of cases, there are three sources of suspicion, one based on signals from the co-authorities, information from human intelligence, and, most rarely, real sources of information from whistle-blowers who call incognito. The rarest method, used after becoming aware of it, is to create a profile that is suitable for trading on the dark web, or at least a potential buyer. In these cases, however, the investigating authority makes use of the possibility that, when employing an undercover investigator, there is a greater chance that the perpetrator may be identified in the future. Let's look at how this will ensure the success of the investigation. *'The Hungarian solution is, in fact, the continental equivalent of public authority defense in American law: under U.S. law, a formally illegal act does not constitute a crime if it is committed by a police officer for law enforcement reasons and is proportionate to the objective pursued.'* (Mészáros, 2019). As described above, the investigating authorities shall endeavour to make sufficient use of the possibilities provided by law which may subsequently be suitable for reasonable suspicion. Because browsers within the dark web are available to anyone, they can be used indefinitely, the use of which is not considered a criminal offence, but if someone engages in illegal activity over the dark web, they can be held liable for crime. However, experts in the field have said that despite the fact that there are all options for creating a 'fake profile', search engines running on the dark web are constantly filtering profiles, so they are trying to filter out users who may even be present through some kind of law enforcement activity. For example, you always get to search for products, but you never order goods, or any other profile that poses a risk to them is filtered out. Therefore, it is typically for this reason that the authorities choose other possible sources, such as human intelligence and co-administration signals. All of these may provide a basis and a suspicion that reconnaissance will also take place in cyberspace, but it is almost certain that reconnaissance will also have a physical realization. The indications of the co-authorities are cases such as the realization carried out by a district or city precinct, where the drug consumer tells in his suspect's testimony that he ordered the drug from the Internet and can even tell the origin of the drug. Then the seized equipment may be used to

verify what he has said, and from there a search for an unknown culprit begins in cyberspace. I would like to mention here that some types of drug offences carried out in Hungary, which are relevant to the study, i.e., in cases of international organised involvement, provided by a specialised unit of the Rapid Response and Special Police Services National Bureau of Investigation, the Drug Crime Division (Készenléti Rendőrség Nemzeti Nyomozó Iroda Kábítószer Bűnözés Elleni Osztály). This does not mean that they do not cooperate with other departments or units (such as Cybercrime Division or Asset Recovery Office) for a successful investigation, since the detection of a crime committed in cyberspace also requires a specialized expertise, similar to property discovery, asset recovery, analysis-evaluation work, and the work of the forensics, since they are responsible for information that can be extracted from mobile phones or laptops. Therefore, it can be said that the investigation of drug offences requires a deep, coordinated cooperation between all police units. It is surprising according to professionals, that typical elements of organised crimes in the classical sense do not materialise in cyberspace, and we can hardly even talk about organised crime. However, this also requires at least the same logistics as in the classical sense of drug smuggling, so that the shipment from one part of the world to another arrives. Among the drugs, the new psychoactive drugs typically come from China, which can be ordered via the dark web, just as cocaine and heroin typically come from South America, and other amphetamine derivatives can also be found, under production, in the form of powder or tablets. But it remains a popular drug route when it comes to smuggling in the Balkans. Some of the steps of drug trafficking in the online space are well known to the investigating authorities, but they are not able to respond to this, given that they are not present at the time of the order at all. All the information they have is ex post, deducible information that they can no longer respond to. In connection with drugs ordered on the Internet, the question also arises how it is sent to the customer, what are the most common methods of successful purchase. Nowadays, the market has expanded with services that bring not only positive results, but also negative ones. While in the past smuggling was carried out by couriers, who were at great risk, (e.g., drug runners from Africa were quick to travel on a flight to take risks, but they realised that it was a much simpler method if smuggling was carried out legally). Therefore, drug shipments arrive by boat or plane (whether cocaine shipments from South America or new psychoactive substances from China) to Spain or Portugal, and from there through courier services that deal with delivery around the world, such as DHL Express[9]

9 Dalsey Hillblom Lynn: it is a German logistic company.

as an international courier service, a popular means of getting the drug to the drug buyer. The packages are designed to use the best possible hiding, and it is also important that when you reach the parcel courier, the shipment is customs-cleared, so you will no longer pass further checks if the smuggling at the airport or on the boats has been successful. In the vast majority of cases, DHL Express drivers know nothing about what might be in the package, delivering between 18,000 and 20,000 packages a week. In addition, all other means of transporting drugs are suitable to ensure passage through countries, so any road transport company can be suitable. Then the package is picked up by the customer and he has already got the drugs he ordered. Again, why do domestic consumers/traders choose this method of access to drugs? There are several reasons for this, which according to Hungarian scouts have made this popular in recent years, one reason is that they have cheaper access (for example, online ordering is better directly from Turkey), the other is that there is a greater choice on the dark web and a lower risk of getting caught, since it hardly requires personal contact, and the customer also tries to secure his identity in the online space in the same way, as a trader. So, this is already a relatively proven method, that the drug manufacturer does not send a courier, but mails the package. In the course of the study, as I became more and more immersed in drug crimes committed in the online space, question followed question how big the latency might be in this area, whether there was any information, data, or study available that had already addressed this. I also asked the professionals (at the Drug Crime Division) what they assume the latency might be (however this is not part of the study, but it is important when we talk about drug crimes committed in cyberspace). To which the answer was that it is huge, we cannot imagine it, and then they said that for Hungary, in previous statistics, there are about 200 regular consumers who need 5g of cocaine a week (and thus, according to them, they have underestimated the consumption volume), so in a total of one year only cocaine consumption is 52 kg (for these 200 people). In comparison, let's look at the amount of cocaine seizures in Hungary in the past, which shows exactly which latency we are talking about. On the basis of the high latency, it is also clear that in the vast majority of these cases the investigating authorities can only realise if there is some certain information that a parcel shipment is arriving in Hungary and the place and time of arrival of the package is expected. Then searches, seizures and suspect interrogations will take place (if necessary, in more than one location) at the property of the person ordering the package in order to obtain as much information as possible about the sender of the package. Another method used in practice is to establish the identity of the perpetrator in cyberspace, via digital profile identification, which

means that any information in the communication between the seller or the buyer that refers to the seller may be suitable for searching further databases. If you have an e-mail address, phone number, nickname, or anything else, you can start searching the available databases. The SIENA (Secure Information Exchange Network Application) channel is most commonly used by the Hungarian authorities, but also by other countries within the European Union, which, as a kind of e-mail system (developed by EUROPOL), ensures the exchange of information between member states and can therefore be considered as a database. If any authority has information on a drug offence committed in a cyberspace, it may share that information with other Member States, trusting that they will provide a relevant response. If the information is not related to a Member State, it may be worth contacting Interpol (The International Criminal Police Organization), who also has an office in other countries of the world, so it is possible that a reply will be received via Interpol in connection with a South American country. It is important to know at which point the most information is generated from the processes of drug crime committed in cyberspace. As far as the language of communication is concerned in the darkweb, it is typically in English or possibly French between the seller and the customer (according to the experience of professionals), and Telegram Messenger and Viber are also commonly used interfaces, which is also a difficulty for the investigating authorities, since their observation is hindered.

Detection and recovery of criminal property, especially in cyberspace (Is it possible to carry out financial profiling in the online drug market?)

With the practice of organised crime, criminal groups make a huge fortune, which they try to hide in a way that does not give the investigating authorities any basis for suspicion. On the one hand, they try to manage the process in such a way that it can be reinvested in their activities and the other part is hidden (typically tax and customs). The discovery of criminal property has been increasingly pronounced in recent years by the Hungarian authorities, which is also an investigative act carried out in parallel with the opening of the investigation. The detection of property and its way is different for certain crimes. I have already dealt with the techniques used by perpetrator groups, whether we are talking about drug crimes or not. The most commonly used techniques include, for example, buying real estate, buying a car, setting up fictitious companies, saving criminal property abroad, hiding cash at a relative, and using

cryptocurrencies. Prior to the study, the above question is one of the questions that I formulated in myself and searched for the answer with the help of professional investigators. Although the question may seem realistic, given that the investigating authorities carry out financial profiling in parallel with the investigation, given that in the case of organised crime, the recovery of income and property is also in the interests of the victim or the state. It is important that, from the very beginning of the investigation, special attention should be paid on how and where the criminal property was hidden. Part of this financial profiling is whether, for example, the perpetrator/perpetrators has/have bank accounts, motor vehicles, real estates or other movable property, or whether other major investments have been made in the past. In case of a drug crime, as with other property-generating crimes, they make significant profits, but in case of classic drug crimes (drug offences requiring personal links, i.e., not in the online space), financial profiling is easier for the investigating authorities. In addition to the fact that it is already possible to know what asset-making techniques are preferred by a particular group of perpetrators, for example, couriers from Africa store the illegal income in cash. The process of financial profiling is more complex than drawing conclusions based on characteristics specific to a particular group of perpetrators. Specific investigative measures are necessary in order to establish a financial profile of a particular perpetrator. In addition, OSINT (Open-Source Intelligence) puts emphasis on open-source data collection, which can be carried out independently by investigating authorities if they know what information they need and from which interfaces they want to obtain that information. In this case, data collection can be carried out through social media platforms, online news portals, online media service providers or blogs, which can be part of asset discovery, so that the investigators can get a more comprehensive picture of the perpetrator, his assets, investments, or savings. In case of cybercrime, it is possible to collect open-source data when the investigators can already establish something specific, for example, from a conversation between a drug seller and a buyer. Requests and observations should be used, and in the available databases such as the vehicle register, Takarnet system (Hungarian system, where the real estate is registered) is justified to conduct searches that can provide information in the future and thereby ensure the extent of the assets subject to confiscation. Another term associated with the aforementioned digital profile identification is the digital clues used by OSINT Company. This should be thought of as the fact that in today's world, there is no one who does not leave behind a digital footprint. Any information can be a digital clue, it advances the effectiveness of the investigation, so it even leaves its mark through a shopping application. Why is important that it is

a source of information that ensures you to know the financial background? This is also linked to the term electronic investigation (e-investigation), *'e-investigation means that the investigating authority requests information from databases directly or indirectly available for detection and proof, where it uses tactical recommendations to ensure the success of the investigation'* (Nyitrai, 2020). The answer to the question formulated at the beginning of the research is clear, that financial profiling is almost impossible. There are speculations and conclusions, but they do not know anything specific (exact amount, location of the property drop) until, after the online return, the execution of investigative activities takes place in the offline space. For example, a specific procedure can be realized, in which data arise on a computer, laptop or phone that the trade, as an example, took place in cryptocurrency, or the type of currency is expressed in a telephone conversation. On the online drug black market, trading with cryptocurrency is also practised because, just as anonymity is ensured on the dark web, cryptocurrencies such as Bitcoin ensure that the identity of the perpetrator is not possible. For the above reasons, the recovery of property as a whole proves impossible. What happens if the research reveals that the trade was conducted in cryptocurrency? One is that in the property, for example, a so-called Bitcoin wallet is invented, which is very similar to a flash drive. Bitcoin is stored in it, but they are encoded, access codes are required to determine how much it is at all. If the bitcoin wallet owner owns the login codes, then the situation is simpler. The Bitcoin account itself is the perpetrator's account, but just as other accounts held for individuals or companies have a banking system in the background, in these cases there is no banking system, but the transaction itself has value, which constantly changes in relation to the market prices. So, if the criminal property is seized, it is perfect for the withdrawal of assets, but if the investigators want to reinvest it in the systems of public finances, it is cumbersome, even almost impossible. Because as long as a drug is invested in cash, it can be paid in the required official form, that is not the case with Bitcoin. If Bitcoin would also be seized, the question arises how much it is expressed in Hungarian Forint, what is the exchange rate, since in the case of a Bitcoin account seized 3-4 years earlier, the amount can be worth more than 10 million Hungarian Forints more than the time being seized. In the oral conversations with staff at the Rapid Response and Special Police Services National Bureau of Investigation Asset Recovery Office for an earlier investigation, they said that there was a need to establish a proper legislation or to amend the law that governs exactly how to proceed if cryptocurrency arises as criminal property. Previous precedents have tried to follow similar procedures, but for the time being their work is made significantly more difficult by the fact that it is not regulated,

despite the fact that more and more individuals and companies are investing their assets in cryptocurrency. In addition, a foreign financial service provider may store the cryptocurrency (e.g., Kraken, Bitfinex, Binance). There is another asset-making technique that is also very popular not only among drug dealers, but also in other wealth-generating crimes, called Revolut, which is a company that provides banking services at a much cheaper price than other banks. From the point of view of the investigating authorities, it is a challenge if the perpetrator has a Revolut account, since it has no branches, no regional offices, and no ATMs. In the event that information had to be obtained from Revolut, it is almost impossible, they do not respond to official requests, there is no official communication channel, as with other banks, if it is necessary to establish for the purposes of the investigation to whom the account is managed by the credit institution.

Impact of the COVID-19 pandemic on the online black market

The coronavirus pandemic has had a big impact on every single area of life. Life had to be reorganized in such a way that the usual lifestyle, standard of living was maintained or felt less. It was not different with crime. If we look back to spring 2020, it seems as if everything has stopped at the same time, in addition to the sudden measures introduced. Citing my previous note on this, in July 2021, I asked three prosecutors how they see the impact of the coronavirus on organised crime after more than a year. According to what they said, the stoppage and the decrease in the number of crimes were felt in the spring of 2020, as seen from the investigating authorities, but there was a reason to perform other duties there. Nevertheless, organised crime groups had lost their usual income, so immediately after a month or two of downtime, they started to assess the market for what was needed, and then began to deal with the claims depending on it. It is alleged that the drug traffickers were the earliest to react to the consequences of the virus. According to prosecutors, there were also organised crime groups who chose another activity instead of the usual one, or at least adapted to the situation, in order to make the most profit possible. The transport of drugs was the biggest challenge for the perpetrators, as border checks and mandatory antigen tests did not make their situation easier. Therefore, the drugs were hidden in trucks, refrigerated cars, train wagons that ran across borders on a daily basis without any other more comprehensive controls, which has also become a feature and is expected as crime has moved into virtual space. However, the

black market for drugs is said to be flexible and highly adaptable. Although in the summer of 2020 the summer festivals, which had been held every year until then, were cancelled, the drugs offered for sale there decreased. According to EUROPOL's report of 30 April 2020, which specifically relates to the COVID-19 situation and its effects on serious and organised crime, it can be read that the trade in cocaine, heroin and cannabis continued during the epidemic, albeit at a lower level (McGuire, 2012). With regard to prices, it can be said that there is expected to be an increase in the drug market, given, among other things, cumbersome care. In addition, due to economic difficulties, it is also expected that people will find it easier to go into job offers that are already criminal in order to ensure their earnings are secured, so they go to work on cannabis plantations or as drug runners. As far as cybercrime is concerned, also referring to the EUROPOL report (European Drug Report 2021: Trends and Developments), most of the crimes were carried out in cyberspace, whether it be organised crime, or a crime committed by a person. As the epidemic progressed, cybercriminals' methods of committing crimes became more sophisticated and they even recruited to help them overcome the initial problems. There has been an increase in cyberattacks, phishing[10] (URL11). The coronavirus pandemic has not been an obstacle to drug crimes, smuggling has not ceased, the number of online orders has only increased in recent times. It is clear that crime has clearly shifted towards the online space, but there has not been significant impact on drug offences committed in the online space.

Proposals for the future

In the course of the short but concise research necessary for the preparation of the study, I have come across several unexpected facts that cannot be compared with my partial research carried out so far. It is definitely interesting that organized crime, which is drug-related in cyberspace, is not typically encountered. Furthermore, before the investigating authorities dealing with this in Hungary, an area that requires much more knowledge than the current expertise is IT, and technical tools is still another area. The discovery takes about half a year (based on personal conversations with professionals), the greatest result of which is the identity of the customer and the drug ordered by the perpetrator. I also asked the professionals what kind of things they could mention, which are

10 This is also social engineering, when the attacker sends a false (forged) message, which is intended to persuade the human victim to obtain data and personal information.

factors that would significantly help their work and contribute to the efficiency and effectiveness of the investigation. the technical equipment. The technical equipment was first highlighted be, since if they could work with more advanced tools than those they currently have, they think it would be easier to work on a daily basis. In case of drug crimes committed in cyberspace, analytical thinking is needed very much, that can support well-founded suspicion. As an example, it has been mentioned that companies or different brokerage firms (such as e Toro) operating in Hungary, that deal with customers investing in Bitcoin, are strongly motivated to have closer relations with the Hungarian police departments, and there have even been examples of a training course on Bitcoin for investigators, given that this is a relatively complicated new system and its understanding is essential in the work of the investigating authorities (Clough, 2015). What makes these companies want to strengthen cooperation? It is to provide support to investors in revealing those who invest in Bitcoin for illegal activity, in order to filter out these illegal businesses. Training would be needed to equip these authorities with analytical skills, which would be one of the most usable capabilities in reconnaissance. What has been highlighted is that there is a pressing need for an elaborate description about cryptocurrencies, on the basis of which they can act professionally. As to what cooperation is needed with neighbouring countries and whether it is necessary to cooperate with other countries in the event that the drug is ordered in the online space, it has been established that cooperation in this area is also essential, where, fortunately, the cooperation with the surrounding member states is good. However, what is surprising that cooperation with the repositories of countries such as the Netherlands, Spain or Portugal is not working effectively enough, in the opinion of domestic scouts, this may be due to the fact that the aim for them is to make as many drug seizures and realizations as possible, so it is not of utmost importance for them to cooperate with our country in the detection of small quantities of drugs arriving in Hungary. In my opinion, the investigators with expertise in the profession have indeed made proposals that contribute to the effectiveness and success of the investigation. In addition, it would be necessary to provide further training to support the methodology of cyberspace investigations, as this is a truly rapidly changing type of behaviour where it is necessary to take action. As far as the recovery of property is concerned, it is certainly justified to cooperate with the partner bodies, since without their expertise the work was complicated, but it is also important that the investigating authorities continue to seek for recovery of the criminal property in parallel with the discovery.

Summary

Drawing the conclusion and summarizing what was described in connection with the study and the investigation that preceded it, it can be said, we are talking about a complex set of crimes when trying to decipher the investigation, success and effectiveness of drug crime committed through cyber space. In the study, I received answers to the research questions that I had previously formulated, but in the light of the answers, it can be said that further research is needed on the basis of the established facts, and it would also be useful for the profession to provide suggestions for solving the problems raised. I believe that the involvement of appropriate professionals, whether civilians or companies or banking sectors, in the near future would make the methods of revealing crimes easier and more understandable for the investigating authorities. It is also important that the co-authorities, within the country but also in other countries, are in constant communication, and that the authorities have information on new crime trends as soon as possible. What is sad to say, that the cooperation of the Member States within the European Union has not continued to deepen, and here I mean the countries of Western Europe. I believe that EUROPOL also has an important role to play in this, in order to disband the existing interests between the Member States, because all countries must fight for the same aim. The free flow of information is also important between partner authorities within the country and the investigative bodies outside the countries. Information obtained by a given authority should not be kept from others, if it is relevant to others, only if it is needed to carry out a successful investigation. After all, the basis of the investigation are also communication and cooperation, which is especially important for a crime that is also involved at international level. That is why the authorities of our country have good relations with the surrounding countries, which will also need to be strengthened with other countries in the interests of law enforcement. As far as the legal environment and background are concerned, the laws currently in force provide the legal framework necessary for certain investigative activities to take place according to the law in force during the investigation. In addition, it would be necessary to regulate the management of cryptocurrencies during the procedure for the reasons mentioned above. I think the profession needs this very much. The coronavirus pandemic has reinforced how much more comfortable the online space can make our days, as well as the lives of criminals, so it can be said that the intention to shift the number of crimes towards the online space has been reinforced. No other influencing factors have been observed whose effects are already measurable or even felt. The online space carries a number of threats

that need to be brought to the attention of all segments of society. Although the victim role is not always present in drug offences, it still poses a risk in other areas. As regards the search for criminal property, the investigating authorities are trying their best to ensure that, in addition to establishing the identity of the perpetrator, the recovery of property is also successful, since drugs are means of crime that generates wealth, and in the case of a criminal offence that generates wealth, huge accumulated assets, which must be considered in the course of an investigation. It is important to take into account that organised crime, and other crimes do not stop, they do not pause, even though there was an epidemic threat or restrictions, the last almost two years have been a precedent that this has not been an obstacle for the perpetrators. Efforts should be made to make law enforcement more effective matched to an accelerated world.

References

Clough, J. (2015). *Principles of Cybercrime.* Cambridge University Press. https://doi.org/10.1017/CBO9781139540803

Gyaraki, R. (2017). A nyomozóhatóság és a katasztrófavédelem feladata a kiberbűncselekmények vonatkozásában [The role of the investigating authority and disaster management in relation to cybercrime]. *Szakmai Szemle, 15*(4), 113-127.

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

Mészáros, B. (2019). *Fedett nyomozó alkalmazás a bűnüldözésben* [Covered detective application in law enforcement]. Dialóg Campus.

Nyitrai, E. (2020). A bűncselekményből eredő vagyon visszaszerzése [Recovery of the property resulting from the crime]. *Ügyészek Lapja, 25*(4-5), 39-53.

United Nations Office on Drugs and Crime (2020). *In Focus: Trafficking over the Darknet - World Drug Report.*

Online links in the article

URL1: *European Drug Report 2021: Trends and Developments.* https://www.emcdda.europa.eu/publications/edr/trends-developments/2021_en

URL2: *EU Drugs Strategy for the period 2013-2020.* https://ec.europa.eu/home-affairs/whats-new/evaluations-and-impact-assessments/evaluation-eu-drugs-strategy-2013-2020-and-eu-action_en

URL3: *Célpontban a kábítószer.* https://www.emcdda.europa.eu/attachements.cfm/att_44774_HU_Dif16HU.pdf

URL4: *Cybercrime.* https://www.unodc.org/unodc/en/cybercrime/index.html
URL5: *Drug related cybercrime and associated use of the Internet.* https://snpf.org/wp-content/uploads/2015/09/Drug-related-cybercrime-and-associated-use-of-the-internet.pdf
URL6: *Deepweb and Cybercrime It's Not All About TOR.* https://www.trendmicro.ae/media/wp/deepweb-and-cybercrime-whitepaper-en.pdf
URL7: *What Is Bitcoin And How Does It Work?.* https://www.forbes.com/advisor/investing/what-is-bitcoin/
URL8: *DarkMarket: world's largest illegal dark web marketplace taken down.*
https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down
URL9: *Cybercrime is bigger than the drug trade: Why small- and medium-sized businesses are more susceptible to online threats.* https://www.bizjournals.com/buffalo/news/2019/06/05/cybercrime-is-bigger-than-the-drug-trade-why-small.html
URL10: *Pablo Escobar is old school. Modern global criminal is a hacker.* https://www.mcclatchydc.com/news/nation-world/national/national-security/article201399274.html
URL11: *Europol: Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU, 30 April 2020.* https://www.europol.europa.eu/sites/default/files/documents/report_beyond_the_pandemic.pdf

Reference of the article according to APA regulation

Nagy, I. (2021). Drug crime transformation under the effect of online platforms. *Belügyi Szemle, 69*(SI6), 107-123. https://doi.org/10.38146/BSZ.SPEC.2021.6.7

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROJECT FINANCED FROM THE NRDI FUND