Summary

Organised crime and IT
Empirical results of the fifth round of the Dutch Organised Crime Monitor

This study provides empirical insight into how organised crime uses IT and how it affects criminal operations. We do not focus on cybercrime alone. Instead, we explore the use of IT and its consequences in a broad range of types of organised crime, i.e. from ‘traditional’ types of organised crime such as offline drug smuggling to cybercrime.

The massive use of the internet, and more generally the effect of IT on all segments of society, entails new opportunities for organised crime. However, there is only a limited amount of empirical research into how criminals use these options and what consequences the use of IT has for how criminals operate (Leukfeldt et al., 2017a). A number of studies have recently been published. Odinot et al. analysed criminal investigations in the field of cybercrime (Odinot et al., 2017; Bulanova-Hristova et al., 2016). Leukfeldt et al. also conducted empirical research into cybercrime, focusing in particular on the processes of origin and growth and modi operandi of cyber networks (Leukfeldt et al., 2017b, 2017c, 2017d). Finally, Oerlemans et al. (2016) looked into how money is laundered in banking malware and ransomware cases. In our study, we build on the work of these and other researchers by both broadening and deepening their work. The broadening consists of the fact that we do not just focus on cases of cybercrime. We investigate the use of IT and its consequences within organised crime in a broader sense. In addition, we deepen our study by analysing the use of IT and its consequences in relation to three essential aspects of criminal operations: criminal cooperation, logistics and handling money flows.

Organised crime and IT: new theoretical and empirical questions

The use of IT in relation to organised crime raises several interesting questions. This is especially true when new forms of crime such as cybercrime, or the use of new technology in traditional organised crime, are linked to existing knowledge, concepts and theories in the field of organised crime.

For example, it is worthwhile to consider what the advent of the internet means for the way in which organised crime groups are formed and developed. Earlier studies stress the importance of social capital; to participate and succeed in organised crime, you have to know the right people, producers, clients, facilitators, and so on (Kleemans & Van de Bunt, 1999; Morselli, 2009). Currently, the growth of the internet is opening up new horizons, at least in theory. Physical and other boundaries need no longer pose an obstacle to making contacts. One could ask whether the internet has diminished the importance of real-life social capital. Has ‘knowing the right people’ transformed into ‘knowing your way on the deep web’ (Lavorgna, 2013; Przepiorka et al., 2017; Töttel et al., 2016, pp. 28–30; Leukfeldt, 2017)?

Another interesting issue is the role of IT in the logistics of organised crime. Any form of organised crime can be described as a logistical process in which a number

---

72 Of course, this paragraph does not provide a comprehensive overview of the literature. The most important outcomes of other studies are discussed in Section 4.
of necessary steps must be taken (Cornish & Clarke, 2002). In the case of international drug trafficking, these steps may include production/purchase of drugs, transport and storage, crossing border controls, and sales, among other things. Communication between criminals (for example, in order to coordinate activities) is also a common prerequisite for the successful completion of organised crime activities. In what way do criminals use IT to improve the logistical process and does the use of IT potentially lead to new logistical bottlenecks? Handling money flows is a specific type of bottleneck for every successful offender. Organised crime is motivated – at least in part – by financial gain. However, criminal earnings bring certain risks, especially if your criminal operations are successful and generate a lot of money. Criminal earnings and the spending of those earnings may raise suspicion, which in turn could lead to arrest and confiscation of your assets. How and to what extent do offenders use IT-facilitated possibilities, such as bitcoin, to launder their money?

Research questions, methods and data

This research is part of the Dutch Organised Crime Monitor. A well-founded approach to organised crime is only possible when there is sound insight into the nature of organised crime. The Organised Crime Monitor provides that insight by making use of the knowledge gained during large-scale criminal investigations. This report is the result of the most recent, fifth round of the Monitor (for previous reports, see Kleemans et al., 1998, 2002; Van de Bunt & Kleemans, 2007; Kruisbergen et al., 2012). To consider specific themes in greater depth, we have chosen to develop the fifth round into three separate sub-reports. The first sub-report was published in October 2017 (Van Wingerde & Van de Bunt, 2017). This report focused on the punishing of organised crime offenders. You are reading the second sub-report, which focuses on organised crime and IT (information technology).

The following research question will be addressed:

How do organised crime groups use IT and how does this use change the ways in which they operate?

We will divide the research question into three subthemes:
- the use of IT in relation to the processes of origin and growth of organised crime groups;
- the use of IT in relation to the logistics chain of criminal processes;
- the use of IT in relation to handling criminal money flows.

Our empirical data consist of large-scale criminal investigations into organised crime. These cases are part of the Dutch Organised Crime Monitor (DOCM). The DOCM is an ongoing research project into the nature of organised crime in the Netherlands. In five data sweeps, 180 cases of organised crime are analysed. Each case includes several and sometimes dozens of individual suspects. For each of the cases, the police files are analysed. The police files contain the results of all police activities that were deployed in a case, such as wiretapping, monitoring of internet traffic, undercover policing, interrogations of suspects, confiscation of goods and financial information. For this paper, we used the thirty cases that were analysed in
the fifth and most recent data sweep. These thirty cases cover various types of organised crime, such as different types of drug trafficking, illegal arms trade, human trafficking, fraud and money laundering, and cybercrime.

We distinguish four categories of cases, depending on the role that IT plays. The first category comprises 23 cases of traditional organised crime; in other words, cases without a strong IT component. These include cases of offline drug trafficking (cases 158, 159, 161–164, 167, 169–172, 175 and 176), human smuggling/trafficking (case 160), money laundering (cases 157, 166, 168, 177, 178 and 180), and other/combined crimes (cases 165, 174 and 179).

The second category concerns three cases of traditional organised crime with IT as an important innovative element in the modus operandi. One of these cases concerns an offender group that manipulates the handling of incoming containers by means of a hack in the network of a port terminal (case 151). A second case concerns people involved in a dark web market through which drugs are traded, among other things (case 152). The final case revolves around a modern variant of money laundering. It entails bitcoin exchangers who helped their customers exchange bitcoins for cash anonymously. Available information indicated that these customers earned their bitcoins via online drug trafficking (case 173).

The third category comprises two cases of organised low-tech cybercrime. One case concerns a variant of ‘skimming’ (also known as ‘shimming’) in which the magnetic strip of a bank card is not copied; instead, the data traffic between the so-called EMV chip on the card and the terminal in which it is used is intercepted (case 154). A second case concerns phishing operations, in which criminals seek to obtain people’s online banking credentials, among other things (case 156).

Finally, the fourth category includes two cases of organised high-tech cybercrime. Both cases focus on banking malware, i.e. criminals manipulate payments made via internet banking through malicious software (cases 153 and 155).

Conclusions

Criminal cooperation and the use of IT

Previous reports based on the DOCM, which focused entirely on traditional, non-IT-related organised crime, provided a clear picture of criminal networks engaged in ‘transit crime’, international smuggling activities in which the Netherlands can be either a country of destination, a transit country, or a production country (Kleemans et al., 2002). Analyses of the traditional cases of organised crime studied in the fifth and most recent round of the DOCM do not produce different results in terms of composition and structure. Although there is no mafia-like pyramidal organisational structure, the criminal networks may be more or less structured, with key players and facilitators on whom others depend. There is also a well-known pattern in terms of involvement mechanisms in these cases. Existing social relationships, such as family and friendships, are crucial to the formation and growth of criminal networks. Where existing social relationships fail, ‘outsiders’ are deployed (Kleemans & Van de Bunt, 1999).

In cases of traditional organised crime as well as in cybercrime cases, we see that most networks have a more or less stable group of core members who work together over a longer period. There are also more and less important suspects and dependency relationships within most networks.

We thank Geralda Odinot, Maite Verhoeven, Ronald Pool, and Christianne de Poot for sharing five cases related to cybercrime (Odinot et al., 2017).
Cybercrime cases are characterised by the importance of technical knowledge and skills. Interestingly, core members of cybercrime networks in our cases often do not have much technical knowledge themselves. However, they do know how to find technically capable facilitators. In the case of low-tech cybercrime (phishing, skimming), criminals make use of their contacts in the offline criminal environment; by contrast, in high-tech cybercrime cases (banking malware), core members acquire the necessary technical expertise through the use of internet forums. The search for technical knowledge thus takes place via offline interactions in the former case and via online interactions in the latter case.

In general, it is clear from the cases in the fifth round of the DOCM that offline social contacts play an important role in involvement mechanisms. Core members in particular know each other due to their network in the offline world and share, for example, the same local and/or social background (see also Lusthaus & Varese, 2017). Money mules are sometimes found in their home environment as well. However, there are also examples where social media platforms and online games are used to make contacts. As we have seen, especially in high-tech cybercrime networks, online forums play an important role in finding technical expertise that is lacking among the core members.

**Logistics and the use of IT**

Every form of organised crime consists of a logistical process in which a number of necessary steps must be taken (Cornish & Clarke, 2002). An important part of every criminal business process in organised crime is communicating with fellow criminals. This communication is necessary, among other things to coordinate the various partial steps in complex activities such as large-scale international drug trafficking. IT offers criminals important new opportunities in this respect. In various cases, for example, criminals make frequent use of phones with so-called ‘PGP encryption’ (which stands for: Pretty Good Privacy). Another option used by criminals to reduce the perceived risk of interception is to meet their accomplices at physical locations which they presume to be safe. These ‘offender convergence settings’ may include catering establishments, commercial premises, or homes.

Furthermore, we analysed the use of IT with regard to specific logistical bottlenecks. An important logistical challenge in various forms of transit crime, such as drug trafficking, is to safely pass contraband across borders. The key role played by IT in controlling and managing traffic flows at airports and seaports has increased the importance to criminals of having access to automated systems. They may obtain such access either through the cooperation of staff or, as in one case, by hacking into the relevant computer networks. One of our cases concerns a group of drug traffickers who recruited IT professionals to hack into the computer network of a container terminal at a large European port (case 151). Keyloggers and malware allowed them to manipulate the time and place of unloading containers. The criminals placed the drugs in a regular cargo container destined for a company that knew nothing about the smuggling, a widely used modus operandi. By using the hack, the criminals were able to collect the container via a dedicated PIN code before the regular company had a chance to do so. Safely connecting supply and demand in criminal markets is another logistical bottleneck. IT has led to major innovations in this area. For example, buyers and suppliers of drugs can meet anonymously behind a computer screen. On a dark web market they can carry out transactions by using a cryptocurrency such as bitcoin, which is anonymous to a certain extent as well. Case 152 focuses on a dark web market where drugs were traded, among other things. After an online transaction is concluded, the drugs are sent by post. However, some transactions and deliveries, especially those involving larger quantities, are carried out during a physical meet-
ing with a customer. The Dutch drug traffickers who operate on this dark web market seem to focus mainly on nearby European countries (see also Kruithof et al., 2016).

Finally, digitisation has also increased the potential reach of criminals to commit payment fraud. Cases 153 and 155 (both banking malware), 154 (skimming/shimming) and 156 (phishing) belong to this type of offence. Cybercriminals, especially where it involves a phishing email or banking malware attack, can target many victims at once and wait to see who does or does not take the bait. However, cashing the proceeds—which is the last link in the logistics chain of phishing or banking malware attacks—is still a largely physical process. Often, money mules are used in these cases, who make their accounts available so the money of a phishing or malware attack victim can be transferred to them. The money is then withdrawn from the money mule account in cash (see also the section on 'Money flows and the use of IT'). This cashing process proofs to be a bottleneck. For this reason, money mules run a high risk, as banks are alert to this trick and the types of transactions associated with it.

**Money flows and the use of IT**

For an important part, criminal money flows often seem to remain invisible to investigators, both in cases of traditional organised crime and in cases of cybercrime. Nevertheless, the 30 cases analysed also generate important insights into this area. As regards the spending of criminal proceeds, in terms of both consumption and investment (assets found), the analyses show neither major differences compared to previous research nor major differences between traditional crime and cybercrime. Earlier research showed that organised crime offenders predominantly invest in their country of origin or in their country of residence, which investments consist of tangible, familiar assets such as residences, other real estate, and mostly small companies. In many cases, the available information indicated that the companies in which offenders invest were used for criminal activities such as transport or money laundering (Kruisbergen et al., 2015). Analyses of the 30 cases in the fifth round of the DOCM produce similar results. Investments in the legal economy often concern real estate and companies, much of which is used by offenders to facilitate their criminal operations. Offenders mainly invest in companies within well-known sectors such as wholesale and retail, hotels and restaurants, and transport. Some cybercrime cases include offenders who are involved in IT-related companies.

When it comes to concealing criminal earnings, we do see important differences between traditional organised crime on the one hand and IT-related crime on the other. The 23 cases in the area of traditional organised crime include various money laundering arrangements as described in previous publications, such as the concealment and transfer of cash. We also see more complex money laundering constructions, such as faking legal profit or salary, loan-back schemes, or the channelling of money through foreign legal entities (Kruisbergen et al., 2012). In addition to the ‘traditional’ ways of money laundering, use can also be made of new payment methods enabled by IT, such as cryptocurrencies and prepaid cards. In principle, a cryptocurrency such as bitcoin is not only useful for cybercriminals. For example, criminals who are active in traditional, offline drug trafficking could use the purchase of bitcoins either in a construction to protect their money flows from detection or as a speculative investment. In the 23 cases of traditional organised crime, however, we do not see the use of bitcoins or other cryptocurrencies (although in one of the cases the criminals made use of prepaid cards (case 165)).

In IT-related crime, unlike many forms of traditional organised crime, the proceeds are often digital in nature. People selling drugs on a dark web market (case 152) often receive the proceeds of their merchandise in a cryptocurrency such as bitcoin.
The perpetrators of phishing and malware attacks (cases 153, 155 and 156) gain control over the online payment transactions of their victims, which take place in digital euros. In the cyber cases that we analysed, these euros were subsequently withdrawn in cash through the use of money mules, or they were subsequently used for the purchase of bitcoins, WebMoney, prepaid cards/vouchers and/or goods, among other things. The use of new forms of money laundering in these cases also involves the use of ‘new ‘services, facilitators and straw men, such as bitcoin ‘mixing services’, which conceal the link between the sending and receiving address of bitcoins, money mules, and bitcoin exchangers.

The central role of cash is a predominant shared feature of the cases that we studied, in the field of both traditional and IT-related organised crime. Criminals hide cash, make sure that cash ends up in other countries, and buy expensive goods and services with cash. It is striking that cash also plays a dominant role in cybercrime cases (see also Europol, 2015; Oerlemans et al., 2016). For example, we see offenders of phishing and banking malware attacks using money mules to cash their digital euros. Furthermore, we see criminals who earn bitcoins from online drug trafficking exchanging at least part of their cryptocurrency for cash euros, for which they rely on private bitcoin exchangers.

**Synthesis**

IT brings new possibilities for organised crime. Offenders use these possibilities for purposes of criminal cooperation, for logistics, and for handling money flows. IT expands the horizon for criminals who are looking for victims, accomplices, tools or clients. The internet allows criminals involved in banking malware, for example, to cast a very wide net in their search for potential victims. Furthermore, criminals looking for specific knowledge or tools can find them through criminal meeting places on the internet. In effect, IT leads to new forms of collaboration. Drug suppliers and consumers also find marketplaces on the dark web that in principle lack physical and social boundaries. Contacts in the offline world and close social relationships therefore seem less important, as it becomes easier to find people, expertise and resources. Trust in the capacities of such a person as an online drug provider is still essential, so people make use of the possibilities offered by the internet to check the reputation of resources (Holt et al., 2015; Decary-Hétu & Dupont, 2013; Soudijn & Monsma, 2012). Criminals also use the opportunities IT offers them to ‘safely’ communicate with each other. Technological developments have made encrypted communication accessible to everyone, including criminals who are active in traditional, offline forms of organised crime (see also Schuppers et al., 2016). Freely accessible hardware and software for shielded communications offer an important advantage for criminals who want to coordinate matters between themselves without the police being able to intercept them (as far as they can tell).

In addition, IT has led to new ways of working in more or less traditional activities such as drug smuggling as well, at least in a case where criminals hacked into a computer network to manipulate the collection of a container in which drugs were hidden.

Finally, IT-enabled features such as cryptocurrencies are also a major innovation. Cryptocurrencies offer a certain degree of anonymity and are the means of payment on dark web markets. Together with the TOR networks on which dark web markets operate, a currency such as bitcoin makes it possible for buyers and sellers of illegal goods and services to engage in more or less anonymous transactions.

In sum, IT is indeed used by organised crime groups, which changes their operations to some extent. However, traditional organised crime is in many ways still rather ‘traditional’, at least in our cases. For example, there are no indications of a
fundamental change in the way offline criminal networks develop. Nor does the logistical process of such criminal activities as drug smuggling seem to have changed significantly in our analysed cases, despite the innovative working method in one case. Furthermore, we only saw the use of cryptocurrencies in cases of cybercrime and online drug smuggling. In other words, this financial innovation was absent in the other cases. It is possible that many criminals simply do not need to drastically change or innovate their working methods.

However, what is more interesting – looking at cybercrime – is that cybercrime turns out to have a local dimension. Cybercriminals are to some extent locally embedded. This is interesting because, at least in theory, the internet allows you to defy physical borders. First, in our cybercrime cases, core members of criminal networks often knew each other in the offline world; they live in the same neighbourhood, for example, or meet each other in nightlife. Straw men such as money mules are often recruited in the vicinity of the main offenders as well. As a result, the resources of social capital used for participation in these cases of organised cybercrime consist to a large extent of offline interactions.

Second, in the dark web market that we studied, part of the transactions took place offline, particularly transactions concerning larger quantities of drugs. In addition, online transactions often concerned vendors sending packages of drugs to buyers living in nearby countries (see also Kruithof et al., 2016). Perhaps these drug traffickers considered the risks involved in sending items by post to be too high when it comes to larger shipments and distances.

Third, cybercrime offenders or offenders in cyber-related cases use local facilities. We saw bitcoin exchangers who rely on the Wi-Fi facilities of fast-food restaurants (among other places), where they physically meet up with customers who want to change euros for bitcoins.

Perhaps one of the most striking similarities between cybercrime and traditional crime is the preference of offenders for cash. Malware and phishing offenders in our cases as well as online drug traffickers change their digital currencies for cash, at least in part. This process is probably also one of the most important bottlenecks in these types of criminal operations, because changing digital currencies for cash in many cases produces some sort of trace or paper trail.

Policy implications

Regulation of cryptocurrency and related services?

The occurrence and investigation of new criminal working methods could raise the question of whether existing laws and regulations are properly equipped to deal with the new situation. This fact applies to the criminal use of cryptocurrency, for instance. Bitcoins and other variants are largely unregulated at the current time. This report, and previous publications, describe how offenders use such innovation. It is not only the cryptocurrency itself, but also related services that largely bypass financial regulation and supervision at this time. As a result, bitcoin exchangers are not subject to a reporting obligation within the framework of the Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme, Wwft), for example.

Regulation and supervision could provide tools to combat money laundering through cryptocurrency. For instance, Dutch online exchange offices such as the bitcoin exchangers could be brought under the scope of the Dutch supervisory bodies. This process can reduce the opportunities to launder money through cryptocurrency. Regulation, however, could also have disadvantages from an anti-money-laundering perspective. Cryptocurrency is currently not very widely accepted in the mainstream
Regulation could contribute to the ‘normalisation’ of cryptocurrency and a higher degree of acceptance of cryptocurrency as a means of payment. This, in turn, could increase the opportunities by which cryptocurrency obtained through criminal activities might be ‘laundered’, or transferred to the mainstream economy (see Oerlemans et al., 2016).

Criminal investigation

Inherently vulnerable technology

The shielding possibilities offered to criminals by IT and the international aspect of cybercrime make the fight against organised crime more difficult. However, even cybercriminals and perpetrators who use IT to carry out their criminal activities leave traces and/or are vulnerable to countermeasures in another way (see also Odinot et al., 2017; Oerlemans et al., 2016).

First, anonymity on the internet has its own limitations. For example, internet traffic is often registered in one way or another, even though the registrations are not always directly accessible to third parties. Even the transaction history of bitcoins is recorded. An obstacle to detection is that the people behind specific bitcoin addresses are often using pseudonyms. By analysing transaction data and linking it to other sources, and because of the suboptimal behaviour of users, certain transactions can still be traced back to individuals (Meiklejohn et al., 2013; Ron & Shami, 2013; Oerlemans et al., 2016). In short, a lack of anonymity is sometimes ingrained in the technology used.

Second, even technology which is presumed to be ‘watertight’ does not guarantee that offenders are shielded from the police. This fact is apparent from the investigation into Ennetcom, for instance. Ennetcom was a key provider of encrypted communication which, at least according to the Public Prosecution Service (Openbaar Ministerie, OM), was widely used by criminals. In 2016, the Public Prosecution Service gained access to enormous amounts of data from the server used by Ennetcom. Ennetcom customers used modified smartphones (Blackberries) which had encryption software (Pretty Good Privacy) installed. This software allowed users of these smartphones to ‘safely’ communicate with each other. The police, however, managed to come by the ‘key’ to the messages that were sent through Ennetcom. During the criminal investigation a copy was made of the server, among other things. According to the police, the decrypted information from the server gave them access to millions of messages, which up until then had been hidden from police investigations. The information obtained in this way would prove to be useful in a large number of investigations into serious crimes.

Third, the same characteristics that make a technology attractive to criminals can in some cases provide the police with tools to tackle those same criminals as well. An example is the level of anonymity offered on dark web markets, which makes these marketplaces attractive to providers of prohibited goods, but also provides a good cover for investigating officers (see also EMCDDA, 2016). As a result, criminals operating online are vulnerable to detection methods originally developed for the offline world, such as undercover operations. Our own case material provides an example of a successful undercover operation against criminals who were active on a dark web market. There are more examples, including the police intervention against Hansa Market. Such undercover operations damage the mutual trust between buyers and sellers that is essential for the functioning of dark web markets (see also Kruithof et al., 2016).

Online-offline interfaces
IT is a crucial part of contemporary society. Moreover, IT plays at least a minor role in many types of organised crime as well, even if only because offenders use modern communications technology. To this end, knowledge of IT and IT-related investigation tools are important for investigating both traditional and cybercrime. However, the interface between the online and offline worlds works both ways. As our study of cases shows, the modus operandi of cybercriminals has a significant local dimension. In the cases of cybercrime and other types of IT-related crime we studied, it turned out that one or more essential links in the criminal operations took place in the physical, offline world. For instance, we saw key players who shared the same social and local origins, offenders who recruited frontmen from their local environment, bitcoin exchangers who serviced their customers from Wi-Fi-enabled public places, and online drug dealers who relied on regular postal delivery. Because of this local dimension, new manifestations of crime not only require new powers or specific technical investigation tools, but they also provide many leads for more classical methods.

Financial investigation
Since the last decades, organised crime control policies have become supplemented with a financial approach, i.e. financial investigation, the prevention of and fight against money laundering, and the confiscation of criminal earnings (see also Krúsbergen, 2017). This approach is fruitful in the case of IT-related crime as well. First, criminals who operate online are usually motivated by financial gain as well. Second, particularly the cashing in or exchanging of proceeds in various forms of IT-related crime, is a stage in the criminal business process at which criminals are vulnerable, because they come into direct or indirect contact with the offline world. This fact applies to offenders in phishing and banking malware cases, for example, who want to exchange their digital euros for cash. It also applies to drug traffickers who want to exchange their cryptocurrency, which they earned on the dark web, for cash euros. Third, a financial approach can offer a new perspective on certain aspects of cybercrime groups. For example, investigating money flows can lead to new suspects, while information on the distribution of criminal proceeds can reveal which criminals provide crucial services in criminal networks. A financial perspective, therefore, can teach us a lot, particularly in view of the fact that relatively little is known about money flows in cybercrime cases.

The situational approach: putting up barriers
The monitor reports that have been published to date all demonstrate how closely organised crime is interwoven with its social environment. The situational approach to organized crime, instead of focusing on offenders, focuses on the environmental factors that make the occurrence of crime possible. In the various IT-related forms of organised crime that are discussed in this report, offenders also use people or facilities in their surroundings, such as banks. For instance, the perpetrators of phishing or banking malware attacks find their victims among the account holders at ordinary banks. For this reason, banks play a vital role in preventing and combating various types of crime. Banks are aware of this role and participate in the Electronic Crimes Task Force (ECTF), which is a collaboration between banks, the police and the Public Prosecution Service. Figures published for fraud committed through Internet banking and skimming have fallen significantly in recent years, probably due in part to banks initiating measures and campaigns to detect and prevent these crimes. The banks also play an important role in combating money laundering. Bank accounts are used to transfer and cash in criminal earnings or to convert cryptocurrency into regular currency. Banks can report transactions from specific accounts
which could indicate banking fraud or money laundering. As can be seen from our case study material, these reports are beneficial to tackling these criminal activities. The importance of the action taken by the banks is evidenced by the significant reduction in the amount lost through Internet banking fraud and by the investigations into money laundering initiated after a report of a bank. Given the central position of the banks and the dynamics in the modi operandi of the offenders, banks continue to play an important role in preventing and combating organised crime.

Banks, money mules (and other ways of channelling money), and cryptocurrency exchange services are crucial to certain forms of crime. The latter two services may exist because many offenders prefer cash even in the world of digital crime. In this regard, the approach to IT-related crime can profit from general measures against cash money flows within organised crime. The case study material gives rise to assume that a significant proportion of the money earned by illegal means is still finding its way into regular economy in the form of cash. Offenders spending their money are facilitated, intentionally or unintentionally, by providers allowing expensive goods or services to be paid for in cash (‘concealed consumption’). Because of the dominant role played by cash in offline and online crime, making this concealed consumption more difficult could be an effective contribution to combating criminal money flows.

Other examples of services and service providers that play an intentional or unintentional role in the offenders ‘working methods are postal companies’, ‘mixing services’ for cryptocurrency, providers of equipment and software for shielded communications, and online meeting places where technical expertise need for specific crimes can be found. Identifying these and other services vital to the offenders is not only important for the prevention of organised crime. It is also important for the investigation of organised crime. Usually, the number of potential suspects in investigations into IT-related crime is larger than available capacity allows for (just as with traditional organised crime). As a result, choices have to be made. Targeted investigation of facilitators can temporarily or permanently disrupt criminal processes. Moreover, it sends a message to those who provide similar services and who profess ignorance of their clients’ intentions, certainly when it involves relatively new types of services.

Our analyses of criminal investigations show that even IT-related crime has important interfaces with the offline world and is partly reliant on the mainstream environment just as traditional organised crime. On the one hand, this conclusion implies that the distinction between cybercrime and traditional organised crime is not as clear-cut as some might assume. On the other hand, it indicates that more traditional investigation methods and a situational approach provide useful opportunities in the approach to IT-related crime in addition to technical tools.

References


