SecurityResearch
Community of Users

CoU Brief
Organised Crime

September 2019

Summary statement

Summary statement

- The trafficking of drugs constitutes the biggest crime market in the European Union, it is estimated to generate about 24 billion euros per year, thereby constituting a large part of the total proceeds of criminal activities in the European Union. The trade in these substances forms a priority for the European Union, especially since organised crime is generally involved.
- Another focal area is constituted by the darknet. Due to its anonymity, the darknet forms a challenge for law enforcement authorities and judicial actors across the European Union. Perpetrators are able to hide their identities in the anonymous platforms while national legislations do not always allow LEAs to start investigations when the identity of a perpetrator is unknown.
- The complex functioning of the online environment requires additional training for LEAs in order for them to be able to deal with such large amounts of information and data.
- Additional research in the domain of cybercrime, the darknet and blockchain technologies is welcomed in order to advance the abilities of LEA. In doing so, researchers are welcomed to interact with the practitioners intensively in order to develop solutions that meet their needs.

Introduction

This CoU brief summarises the topic Organised Crime and relevant EU-funded projects that participated in the 14th Meeting of the Community of Users (CoU) on Secure, Safe and Resilient Societies that took place 16 – 19 September 2019 at the BAO convention centre in Brussels. The Community of Users is a DG HOME initiative that aims to improve information transfer of research outputs and their usability by different categories of stakeholders. During the meetings and thematic workshops, policy updates and information about H2020 projects are provided and interactive discussions facilitated to ensure that solutions and tools resulting from research will reach users.

European Commission

Scope and relevance

Despite efforts on the national, European and international level, organised crime still prevails in the European Union. According to the 2017 Serious and Organised Threat Assessment (SOCTA) by Europol, there are over 5000 criminal groups active in the Union, compared to about 3600 in 2013.[1] These groups are increasingly poly-criminal and often consist of both EU-nationals as well as non-EU nationals. From the SOCTA 2019 mid-term review can be concluded that the top-level criminal groups are growing more and more complex and are increasingly active on the international level. The impact of such organised criminal groups has become more visible throughout the last couple of years as the amount of violence has inclined.

Proceeds of organised crime in the EU are currently (conservatively) estimated by Europol to be 110 billion euros annually. Generally, 2.2% of this amount is seized and 1% of the total value is annually being confiscated. This leaves ample of room for improvement from all involved actors.

Although the number of organised crime groups has increased over the year, the shares of the criminal activities have remained more or less constant with drugs trafficking, illegal immigration and fraud and swindling being the most common. The trafficking of drugs constitutes the biggest crime market in the European Union whereas illegal immigration has been on the rise in recent years.

Drugs

The drug market is estimated to generate about 24 billion euros per year, thereby constituting a large part of the total proceeds of criminal activities in the European Union. Organised criminal groups are heavily involved in this trade; over 35% of all groups are involved in the drug market. EU-based suppliers represent 44% of the annual global drug revenue, amounting to 69 million euros. This has more or less been consistent over the last years. In the European context, drugs most often originate from the United Kingdom, Germany and the Netherlands. More recently, the health threat of the drug trade has surged; worldwide the deaths as a result of overdoses have surged and the purity of substances has spiked, resulting in more health problems. Drug markets have also partially moved to the online domain, making use of the anonymity the darkweb offers.

The darknet

The darknet is a place on the internet that is designed in such a way that it is easy to conceal the identities of natural persons. This has attracted a multitude of criminal business. The darkmarkets are places where criminals trade weapons, illicit drugs, child abuse material, stolen credentials, and others.

The darknet itself poses a challenge for both law enforcement authorities (LEAs) and judicial actors in the European Union. On the one hand, the anonymity that such platforms offer hinder the ability of LEAs to trace potential perpetrators and collect evidence. On the other hand, national legislation does not always facilitate darknet investigations because often it is not clear (as a result of the granted anonymity) who the perpetrator is.

Although the web has not replaced the traditional supply methods, Europol observes an increase in the usage of the online platforms. While well-known markets such as Samsara, Empire market or Genesis remain popular. The European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) recently observed a shift from international online drug sales towards non-English local and regional online markets. The reasons for this development require further scrutiny, nevertheless, one explanation could point towards the erosion of trust in global markets as a result of recent take downs. Europol has recently increased its efforts in the domain of the darkweb by establishing a dedicated team which encourages increased coordination across the EU in terms of information sharing, joint actions, operational support, prevention and awareness raising, training, tool development and tactics). One of the focal areas of the intensified Europol efforts is the creation of distrust with the darkweb among the criminal community. Through joint LEA actions, the trust of criminals in the darkweb has been diminishing, however, the shift towards smaller (regional) markets forms a new challenge in this regard.

For both Interpol and Europol, cybercrime is one of their top priorities. The European Union has also been developing a strong legislative framework aiding the fight against organised crime on the EU-level. Examples of legislation in this domain include the EU Policy Cycle[2], the fifth EU Anti-Money Laundering Directive[3] and the EMCDDA's EU Drugs Strategy 2013 – 2020 (currently under evaluation). Besides facilitation on the legislative aspects, the European Commission also seeks to support the fight against organised crime through the funding of research. 2.2% of the total Horizon2020 budget was spent on research related to the fight against terrorism and organised crime. Specific focus has been paid towards the inclusion of practitioners in research projects, two LEA-oriented networks of practitioners have been established in this regard: I-LEAD[4] and ILEANET.[5] These projects can help other research initiatives in the domain of organised crime to better understand the needs

[1] European Union Serious and Organised Crime Threat Assessment 2017, Europol
[2] https://www.europol.europa.eu/empact
[3] COM(2018) 213 final
[4] https://cordis.europa.eu/project/rcn/210219/factsheet/en
[5] https://cordis.europa.eu/project/rcn/209954/factsheet/en

of practitioners, to picture the existing range of initiatives and to, ultimately, better align research outputs with the requirements of the end users.

Cryptocurrencies

Cryptocurrencies are an ever-increasing trend which continues to enhance due to more sophisticated encryption measures. The market is moving fast, even the social media platform Facebook and the messenger service Telegram are trying to launch cryptocurrencies. Bitcoins are becomingly increasingly relevant from a law enforcement perspective. Some very practical issues can arise when police officers are raiding homes and find bitcoins on seized computers, which are protected by a password. Without the password and without a so-called Bitcoin wallet account within the law enforcement organisation, the funds remains inaccessible and cannot be seized.

From a law enforcement perspective, the most important challenge are the skills, capacities and tools needed to analyse the phenomena and to catch and prosecute predators. EUROPOL has a couple of top level experts who are dealing with the topic, but the situation on EU Member State level is different. Most Member States are lacking sufficient knowledge and training of fraud in this field and cannot afford the high license fees for the few commercial IT solutions which exist on the market. To put it in perspective, one license costs approximately 10.000 EUR per year. Hence, there is a need for open-source solutions, but the 'low-cost' or 'no-cost' alternatives available on the market do not have the same technical features.

A big issue is the capacity. Apart from darknet or cryptocurrency data, the sheer amount of publicly available and self-generated content (e.g peer-to-peer chat, pics) confronts law enforcement with an enormous workload and is the reason for on-going capacity issues.

A panellist also highlighted the importance of providing more training measures for national law enforcement. Law enforcement practitioner receive very limited training in this relatively new field.

Blockchain

The topic blockchain in general poses a lot of legal question especially related to law enforcement investigation work. Can data on blockchain be considered as public or not? The working legal theory is that Blockchain is public data because of the fact that law enforcement is unable to only analyse a segment of the blockchain. Instead it has to analyse the entire blockchain which is why the question of proportionality is out of scope.

Current debates and stakeholder perspectives

This section provides an overview of the views on the fight against organised crime from a number of key stakeholders.

Policymakers

Government representatives play an important role in the fight against crime and terrorism; not only do they facilitate the combat on the national level through legislation and policies, they also play a crucial role in cross-border cooperation. Collaboration between different Member States (and beyond the European Union) is essential to effectively address organised crime as criminal groups increasingly started operating internationally.

The current European legal framework on the fight against the organised crime has grown over the past couple of years an currently involves the following key documents:

- Council Framework Decision on the fight against organised crime[6] which aims to ensure severe penalties for persons involved in criminal organisations (whether they commit offences or other acts such as setting up or directing an organisation, recruiting members or providing material or financial assistance).
- Directive on Combating money laundering by criminal law[7], published in 2018 and tob e implemented by the Member states on 3 December 2020 at the latest, introduces new criminal law provisions which will disrupt and block access by criminals to financial resources, including those used for terrorist activities. These new provisions include the establishment of minimum rules on the definitions of criminal offences and sanctions related to money laundering, the possibility of holding legal entities liable for certain money laundering activities which can face a range of sanctions and removing obstacles to cross-border judicial and police cooperation by setting common provisions to improve investigations.
- Directive laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences[8], also known as the 5th Money Laundering Directive seeks to enhance the powers of EU Financial Intelligence Units and facilitating their increasing transparency, to prevent risks associated with the use of virtual currencies for terrorist financing and limiting the use of pre-paid cards, to improve the safeguards for financial transactions to and from high-risk third countries, to enhance the access of Financial Intelligence Units to information,

[6] Council Framework Decision 2008/841/JHA
[7] Directive 2018/1673
[8] Directive 2018/0105 (COD)

including centralised bank account registers and to ensure centralised national bank and payment account registers or central data retrieval systems in all Member States.

- Council Decision concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime[9] encourages Member States to establish a national Asset Recovery Office, to facilitate the tracing and identification of proceeds of crime and other crime related property which may become the object of a freezing, seizure or confiscation order made by a competent judicial authority in the course of criminal or, as far as possible under the national law of the Member State concerned, civil proceedings
- Directive on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union[10] enables Member States to trace, freeze, manage and confiscate the proceeds of crime.
- EMPACT Policy Cycle 2018 - 2021[11] seeks to tackle the most prevalent threats posed by organised and serious international crime to the EU by improving and strengthening co-operation between the Member States, EU institutions and EU agencies as well as third countries and organisations, including the private sector where relevant.

Despite this advanced legal framework, challenges in this regard remain. As the Europol representative indicated, investigating the darkweb results in a variety of legal challenges. One of the most cumbersome ones being the fact that in many jurisdictions one is not allowed to open an investigation without a suspect, however, the anonymity granted by the darkweb often means that an investigation is needed to identify the suspect. Moving forward, this is an area that requires further thought.

Furthermore, policymakers can play a role in preventing people from resorting to crime and/or the use of substances. This can be done through education and various prevention campaigns, which would ideally be targeting both potential perpetrators as well as the consumers of the illegally traded substances such as drugs.

Research

With ever-changing modus operandi, the research community can play a pivotal role in strengthening the capacity and ability of LEAs to combat organised crime. As a Europol representative describes the interaction between LEAs and perpetrators as a 'cat and mouse game', researchers are invited to support the competent authorities to stay ahead of the game. Such innovations are welcomed in the shape of investigative tools as well as in relation to strategies to process vast amounts of data.

In addition, EMCDDA emphasised that more research is needed to better understand why people start using the darknet, how they get acquainted with the platform and why they stop using it. Such insights would help develop tailored strategies and policies to combat the usage of such online platforms.

Finally, researchers would benefit from being more aware of what is 'out there' already in terms of existing research initiatives in order to avoid duplication of work and resources.

Practitioners

Europol mentioned a number of successful joint actions which took place during the past couple of months. LEAs are encouraged to continue in this regard and to further enhance their international collaborations. With organised crime groups operating across borders, LEAs are required to do the same; both Interpol and Europol provide their support in this regard.

In addition, during the 14th CoU event it was highlighted that practitioners would benefit from an improved relationship with the research community. Whereas understanding the needs and wishes of the practitioners, one should also be aware of the current research landscape in order to create synergies with ongoing initiatives.

Ultimately, the need for better training of LEAs was voiced, in particularly with regards to the darknet and dealing with large amounts of data.

[9] Council Decision 2007/845/JHA
[10] Directive 2014/42/EU
[11] https://www.europol.europa.eu/empact

Europol mentioned a number of successful joint actions which took place during the past couple of months. LEAs are encouraged to continue in this regard and to further enhance their international collaborations. With organised crime groups operating across borders, LEAs are required to do the same; both Interpol and Europol provide their support in this regard.

In addition, during the 14th CoU event it was highlighted that practitioners would benefit from an improved relationship with the research community. Whereas understanding the needs and wishes of the practitioners, one should also be aware of the current research landscape in order to create synergies with ongoing initiatives.

Ultimately, the need for better training of LEAs was voiced, in particularly with regards to the darknet and dealing with large amounts of data.

Possible synergies

For an overview of CBRNE-related projects funded prior to 2018, see section 6 (Crime and Terrorism) of DG HOME, "Community of Users on Secure, Safe and Resilient Societies – Mapping Horizon 2020 and EU-funded Capacity-Building Projects under 2014-2017 Programmes". The projects referenced within this section of the aforementioned document are universally geared towards tackling similar subjects as those discussed in this brief, and thus have the potential of exhibiting synergies with them.

Lessons learnt and challenges

The general challenge when discussing the darknet, cryptocurrencies and blockchain is whether encryption should be somehow circumvented by innovative technologies because it hinders the work of law enforcement or supported because it protects the privacy of citizens.

Due to the nature of the organised criminal groups (some of them operating in a mafia-type structure), LEA struggle to get an accurate overview of the governance of such groups. In addition, as a result of the groups using encrypted communication means and the increased precaution they take when meeting physically, it is difficult for competent authorities to trace the group's activities. Furthermore, organised criminal groups tend to adapt their modus operandi easily, which thwarts LEAs to stay 'ahead of the game'. Staying one step ahead is challenging both in the real and virtual world. Investigative tools used by LEAs are often relatively old and require further development to allow them to effectively investigate the activities of organised criminal groups. Furthermore, it is encouraged for researchers to develop approaches for LEAs to deal effectively with the vast amount of data available.

Moreover, a key challenge in the domain of the fight against organised crime are the legal frameworks. With organised crime being cross-border by nature, the compatibility of different national legal frameworks can sometimes hinder the combat against crime. In addition, with the constant development of the modus operandi, the LEA community would benefit from a more advanced legal framework, in particularly with regards to the start of investigations without suspects (which would be particularly relevant for those working with the darkweb).

Darkweb, cryptocurrencies and blockchain

The shift of activities from the offline world towards online platforms on the darkweb poses an additional challenge for LEAs as such platform grant anonymity for its users, as do cryptocurrencies. It is essential to strike a balance between fighting criminals and to safeguard users who engage in legal transactions. During the 14th CoU event, the need for more access to data was voiced; LEAs indicated they would benefit from having more information on, for instance, shared bitcoin wallets and PGP keys. Having access to this type of information would also allow them to better protect those that make use of cryptocurrencies in a non-criminal way.

Generally, knowledge and understanding of the darkweb is lacking. Given its anonymous nature, it is even difficult to estimate the size of the user base of the darkweb. Therefore, more resources are needed to better grasp the size and activities of the darkweb.

Another issue is the incomplete picture of scientists when it comes to cybercrimes and cyber currencies. Due to the fact that the crime environments are moving so quickly, scientists often only get second or third handed information, while law enforcement has direct access of information on-going and past cases. To be able to be up-to-speed with the criminal inventions in the digital sphere, several researchers at the event called for more short-circle project funding and more access to information from the law enforcement. One participants called the current situation even an 'arms-race' of criminals against law enforcement and scientists. The best case scenario for scientists would be to get a lab environment within a law enforcement organisation so that scientists get first-hand and 'real' data on an international level. Bringing scientists closer to the real cases and being able to quickly adapt to changing environment would not only lead to an increase in innovation but would also help to make solutions more affordable. A positive example on the national level in this regard is the Dutch high-tech crime unit which operates such a lab. A Europol representative noted that Europol is willing to follow a transparent approach but that the EU Member States are still the owner of data which is why the agency has certain limitations and cannot just share the data with scientists. However, he stressed that the trust between the law enforcement communities and has rapidly improved within the last years which can be considered a step in the right direction. The convener of the event announced that the European Commission does have the ambition for the practitioners and scientists to be deeply involved in the whole cycle.

Drugs

A recent trend in the drug landscape is the usage of postal service for the delivery of substances in parcels and postal packages. Often, such substances are purchased on the darknet and, subsequently, transported using regular postal services. This provides a link between the offline and online world which creates opportunities for LEAs. Nevertheless, taking into account the vast amount of parcels and packages being shipped on a daily basis, this method would require further strategizing.

Way forward

To further advance the fight against organised crime, improved collaboration between the research community, practitioners and policymakers is encouraged. With much of the LEA capacities depending on the investigative tools they work with, researchers are invited to develop more innovative solutions in this regard. In doing so, researchers should start by identifying what is already 'out there' in terms of initiatives and projects to avoid duplication. Moreover, creating synergies with existing initiatives is encouraged just as bringing experts to the table from the very start of the research project. Such inclusive approach would help to improve the research uptake of project outputs.

Furthermore, the need for more coordination across Europe as well as with international partners was voiced. Organised crime groups operate across borders and with the online (darkweb) markets being accessible from each corner of the world, international cooperation is essential to effectively combat organised crime groups. In this regard, one should look at both sides of the coin: both the drug supply as well as the health problem feeding the demand for substances. In this regard, policymakers on the national and EU level can play a role in the shape of education and prevention campaigns.

When investigating the darkweb, LEAs are encouraged to not maintain a broad approach, taking into account the full chain. To advance the fight against organised crime, LEAs would benefit from understanding how and when to best intercept criminals on the darkweb and, therefore, monitoring the entire process is essential. In addition, the strategy to create distrust among criminals which Europol together with Member State competent authorities is currently creating seems to be effective and continuation of this approach is encouraged.

Key Contacts

http://www.securityresearch-cou.eu/

DG HOME

Nada Milisavljevic
Nada.Milisavljevic@ec.europa.eu

Philippe Quevauviller
Philippe.Quevauviller@ec.europa.eu

European Commission