THE EFFECTIVENESS OF INTERNATIONAL CRIMINAL AND JUDICIAL COOPERATION IN THE CONTEXT OF CYBERSPACE TOOLS[1]

Ivett Csontos-Nagy, MA

Ludovika University of Public Service
Doctoral School of Law Enforcement
PhD student
Hungary

Keywords: cyberspace, international cooperation, migration, organised crime

DOI: https://doi.org/10.15158/8s98-j844

[1] SUPPORTED BY THE ÚNKP-23-3-II-NKE-107 NEW NATIONAL EXCELLENCE PROGRAM OF THE MINISTRY FOR CULTURE AND INNOVATION FROM THE SOURCE OF THE NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION FUND.

ABSTRACT

The effectiveness of international criminal and judicial cooperation is becoming increasingly important in today's digital world. Crimes committed in cyberspace are becoming more frequent and complex, and it is, therefore, essential to think across borders and to take into account the fact that other organised crimes may also take place on an international scale. One of the most important factors to take into consideration is time, as the aim is to exchange information and evidence as quickly as possible.

This paper describes the international cooperation tools currently available to investigating authorities and prosecutors in a European Union member state to ensure effective prosecution in terms of the collection of information or evidence. It explains what *organised cybercrime* is, how migration, migrant smuggling, human trafficking and cyberspace are interlinked in typical organised crimes, and how this poses serious security challenges.

The research methods used to conduct the study detailed in this paper were an analysis of relevant literature and structured interviews with investigators and prosecutors in Hungary.

The paper describes the range of possible cooperation tools with the aim that they will be used in the future by investigators and prosecutors in EU member states. To help achieve that aim, it provides insights into the Hungarian context that can help other countries better understand the cooperation tools that are, if less known, available in their own countries and can be used to address the security challenges posed by organised crime.

INTRODUCTION

Today, there is hardly a crime that does not involve at least one electronic device, such as a phone, a laptop, a computer or the Internet. A wide range of devices are available to offenders to commit crimes with as few traces as possible. However, while offenders try to take advantage of this anonymity, this does not always work because, at some point, all people make mistakes. It is this propensity for error that investigating authorities and prosecutors rely on when it comes to fighting cybercrime.

Research into certain categories of organised crime, such as migrant smuggling, human trafficking, drug offences and money laundering, has shown that most of these categories involve activity in cyberspace, suggesting that a complex vision is needed for this work to bear meaningful results.

The dangers of cyberspace are due not only to the wide range of possible crimes but also to the fact that criminals' motivations, such as passion, revenge, profit or ideology, can vary greatly (Leukfeldt, Lavorgna & Kleemans, 2016). An offender can target several victims at once, commit crimes more quickly and at a distance, and is not hindered by geographical location, all of which increase the risks posed by such crimes.

However, not all cases have a victim. For instance, in categories of organised crime such as migrant smuggling or drug trafficking, the groups involved provide services to each other without harm (material or moral) being done to either party. Thus, while the latency of such crimes is already high (as there is no victim), the advent of cyberspace has increased it, along with generating new security challenges. Law enforcement authorities can no longer begin their investigations by tackling offline offences alone; instead, they must adopt a completely different way of thinking. The fall in the cost of technology has made it even cheaper for offenders to commit a crime (Wall, 2015, p. 74).

The definition of *organised cybercrime* remains a divisive issue among researchers internationally. Nonetheless, in recent years, it has become increasingly accepted that cybercrime cannot be said to be less serious and dangerous than organised crime, and correspondingly, better methods for analysing the risks, harms and threats that it poses are being

proposed (Whelan, Bright & Martin, 2024). An essential element of such investigations is how to implement proper data protection on any electronic evidence obtained in their course, for instance, to meet GDPR requirements – an issue that remains difficult to legislate for and has raised concerns among the judiciary in several countries (Samdani & Malik, 2023).

One initiative to address this problem is the Second Additional Protocol to the Convention on Cybercrime developed by the European Union, which takes into account the changes that have taken place in the field over the last 20 years. The Second Additional Protocol introduces several innovations regarding, for instance, requests for domain name registration information, the disclosure of subscriber information and the procedures pertaining to emergency mutual assistance or video conferencing (Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, 2022).

The Serious and Organised Crime Threat Assessment (SOCTA), published in 2021, shows that there has been a visible increase in the number of cybercrimes under investigation. However, due to the fact that most criminals commit their crimes individually, it does not establish whether there has been a corresponding increase in the number of criminal networks (Europol, 2021). What makes it so difficult to determine exactly how many criminal networks there are in cyberspace is the high degree of latency, for example, as with human trafficking networks or migrant smuggling, where the latency is increased by the lack of confessions from its victims.

When raising the issue of organised crime, the consequences of migration should also be addressed. While the protection of the state and its citizens is the main concern of any country, there are also security challenges that arise from globalisation (Milovanovic, 2023). Correspondingly, investigative authorities and justice officials must think of the specific security challenges of migration in global terms and take into consideration that aspects of organised crime are changing as a consequence and that this interconnection will pose an even greater threat in the future.

It is important to underline that both organised crime and cyberspace are transnational; hence, it is imperative that countries cooperate both

within and outside the European Union. In addition, it is important to recognise that, given that the European Union is a preferred destination for many migrants, cooperation is one of the best tools for countering emerging security threats, such as migrant smugglers and human trafficking organisations, and will remain so in the future.

The primary aim of this research is to provide justification for the use of electronic data obtained through effective international criminal and judicial cooperation against transnational cybercrime as evidence in the prosecution phase. The second aim is to provide justification for extending such cooperation to cyberspace, which serves as a kind of intersectional space between organised crime.

Accordingly, this work's research question is how to achieve these goals more effectively. The motivation for focusing on this problem is that the processes by which law enforcement authorities might obtain data stored in the cloud under the criminal jurisdiction of unknown countries are subject to jurisdictional, territorial and many other obstacles. In view of this, very few of these crimes are brought to court; thus, the majority of their victims are left without recourse for reprisal.

The scientific problem is, therefore, closely linked to the subject of the research, which also stems from the fact that, in addition to the differences in legislation between countries, cooperation is less effective due to a lack of awareness of the tools available to quickly and efficiently obtain and share reliable evidence among members of the investigating authorities and prosecutors. The main emphasis of the research is on the importance of international cooperation just because, if such cooperation is not effective enough, it is almost impossible to fight serious and organised crime.

The first part of the paper explains why effective international cooperation is essential, the threats that need to be addressed at both criminal and judicial levels, and the importance of understanding current patterns of offending in order to ensure such effective cooperation across borders. Through analysis of the relevant literature, this section clearly identifies the links between organised crime and cyberspace and the risk and threat factors associated with that. The remaining sections of the paper focus on current practice, drawing on the earlier literature review

and interviews to elucidate this. In that light, the discussion focuses on how professionals respond to the current situation, how difficult they feel it is to fight organised crime, and what the current instruments of criminal and judicial cooperation are.

1. ORGANISED CRIME IN THE MODERN ERA

Already one of the most complex and serious problems facing societies across the world, organised crime in the modern era is undergoing a clear transformation, a process that is far from complete. Now, authorities are no longer looking to uncover the classic mafia-style organisations but are focusing instead on a new kind of criminal organisation that combines several categories of crime and is open to trading in multiple products and smuggling both people and drugs at the same time. Despite the differences in the scope of their criminal activities, the aim of these new criminal entities has not changed from those preceding them – to achieve the highest possible profit – and they remain highly organised, even while the members of the organisation do not always know each other (Gyaraki, 2019).

The central characteristics of organised crime are the use of legal economic structures, the pursuit of extra profit, the creation of monopolies and the hierarchical structure of the relevant groups (Nyeste, 2023, p. 111). Organised crime represents a direct threat to the security of both society and individuals and destabilises the legal order and state power. Therefore, law enforcement authorities mobilise considerable resources in pursuit of criminal organisations, in relation to which it is important to achieve statistically well-exposed results (Vári, 2014b).

According to the website of the European Council, the priority crimes most frequently committed in the European Union are migrant smuggling, cybercrime, drug trafficking, human trafficking and excise fraud. To tackle these activities and help member states in their fight against organised crime, the European Union has introduced and is continuing to introduce an increasing range of measures and legislation (European Council, 2024).

Statistics from a 2024 Europol report on criminal networks well illustrate the seriousness of the situation. The report found that there are currently 821 criminal networks active in the European Union and third countries, with more than 25,000 people and 112 nationalities involved in those networks. 34% of the most dangerous criminal networks have been active for more than 10 years, even though some of their members or leaders have been arrested. 76% of all the organisations identified are active in at least two and up to seven countries. And 6% are involved in migrant smuggling, which means 295 people (Europol, 2024). Given these figures, it is crucial that all member states reflect on the extent to which they think globally and how open they are to cooperation with other countries when a criminal prosecution crosses international lines.

Today, migrant smuggling is one of the most common forms of organised crime with increasing significance for citizens, law enforcement authorities and the heads of state of some European Union member states – particularly since the European migrant crisis in 2015. Countries of transit and countries of destination face different problems. Migrants hope to reach their destination country as quickly as possible, whether through legal or illegal means. For example, they may seek help from organised criminal groups if they encounter obstacles at the state border (Milovanovic, 2023, p. 325). Yet, while such activity occurs in the physical world, communication takes place digitally; hence, it is still linked to cyberspace.

Given the above, it can be concluded that cyberspace has had an important part in the transformation and modernisation of contemporary organised crime groups, and it is fitting to say that such groups now operate without borders. Correspondingly, law enforcement agencies and institutions must recognise the need to work with other countries to be effective.

In investigating crimes of the kind described so far, it is important to consider how many countries may be primarily involved, whether or not the country or countries concerned are EU member states, and whether or not there are any personal connections between investigators or prosecutors in the relevant countries. Once these factors have been taken into account, further consideration of what information and evidence is needed and whether time is a factor can follow. International

organisations also have an important role to play, and it is especially worth considering leveraging the support of Europol or Eurojust, both of which can provide a material, technical and physical presence to help in the dismantling of all types of criminal organisations, whether migrant-smuggling, human-trafficking or any other kind which is an objective for Europol and Eurojust as much as it is for a given country. Reflecting this, it is therefore crucial that such international organisations not only increase the amount of statistical data they keep but also share that information with countries when necessary.

In most cases, investigating criminal activity in cyberspace requires specialist knowledge and a deep understanding of the processes involved in such activity, the ability to think like the criminal, and recognition that at least one aspect of the crime will have an international dimension.

The following section describes in more detail the various tools for cooperation that can facilitate the detection of certain organised crimes that are currently used in practice. It should be noted that most cooperation tools can also be used when investigating crimes without a cyberspace dimension, where electronic evidence is not required, and, thus, where the 24/7 data preservation request typically used when electronic evidence is required is not a factor.

2. THE LINK BETWEEN ORGANISED CRIME AND CYBERCRIME

As formerly traditional organised crime groups have realised that the chance of their being caught is much lower and their potential profits much higher if they exploit all the opportunities offered by digitalisation, they have started to seek out cyberspace experts or, increasingly, train themselves to take advantage of that.

The actual perpetrators of cybercrimes may be operating individually, working in an organisation, or they may offer their services to criminal organisations but outside of the hierarchy that is associated with the traditional form of organised criminal groups. They are characterised by

having flexible networks and expertise and using non-violent means to control the dominant market (Mezei, 2019, p. 135).

As a consequence of the above, a new concept of the *organised cybercriminal group* has emerged. This is defined as a structured group of three or more members whose aim is to commit one or more serious cybercrimes for financial gain using information systems and the Internet (Malas, 2017, p. 365). To pursue such groups, it is not only the investigating authorities and prosecutors who need to have up-to-date expertise in the digital methods they employ and, therefore, develop effective tools to fight cybercriminals and emerging organised crime networks, but also national leaders, international organisations and the European Union.

International cooperation and information exchange are key to the fight against criminal organisations and cybercrime, including in policing and at a judicial level. Therefore, cooperation is an important part of the fight against such criminal groups. To ensure effective prosecutions, the many tools of international cooperation must be used.

3. MIGRATION IN THE SHADOW OF ORGANISED CRIME NETWORKS AND CYBERSPACE

The following section expounds upon the examples of migration, migrant smuggling and human trafficking to show how cyberspace has become indispensable to the criminal organisations operating in these areas, despite the fact that these activities all occur in physical space and are, indeed, not imaginable as cybercrimes.

First of all, migration – whether driven by internal armed conflict, climate change, civil uprising, poverty, or other factors – inevitably makes migrants vulnerable during their journey. It is precisely because of this that there is a link between migration and human trafficking. From the point of view of the psychology of human trafficking, it is interesting that the people who are forced to migrate and so become the potential victims of exploitation by criminal organisations may be recruited in the spirit of cooperation and the offer of better material and living conditions, even

while they are still vulnerable to cooperation being replaced by coercion (Szuhai, 2017a, p. 75).

However, in the flood of migrants to Europe since 2015, it is very difficult to identify who the victims of trafficking are, as in many cases, they do not report to the police, and so there is a high degree of latency in the statistics. Victims of trafficking are mainly girls, adult women and children who are trafficked for sexual exploitation, while men and young boys are mostly victims of labour exploitation (Szuhai, 2017b, p. 81).

In terms of cyberspace, traffickers also take advantage of the opportunities offered by digital technology, with processes such as recruitment and exploitation, as well as control, playing a major role. New forms of offending have also emerged with the advent of social media, such as the so-called "lover boy method", and traffickers are keen to employ these (L'Hoiry, Moretti & Antonopoulos, 2024, p. 2). The main focus of these activities is on the Internet – especially the deep web – and involves recruitment and, in some cases, the provision of services. Since the victims also use the Internet and social media on a daily basis, it is not difficult for the perpetrators to target them.

While there are elements of trafficking that must be physically carried out to be completed, such as the transport of people, there is the potential for even greater profit when operations are extended to the digital space. Today, it can be said that the Internet is involved in all the different forms of human trafficking, including trafficking for the illicit use of the human body, sexual exploitation or trafficking for labour exploitation (Ripszám, 2020).

Migration and migrant smuggling have become so intertwined in recent years that they have developed a cause-and-effect relationship. Migrant smuggling is perhaps one of the most organised criminal activities and exemplifies the concept of criminal organisation involving the most people in any area of criminal activity, even though those people are aware that the risk of being caught is greater than in other areas. According to Luigi Achilli (2016, p. 102), smuggling networks tend to organise the transport of nationals who do not have enough money to move by other means, but when any ethnic connections with the migrants are broken, the main objective becomes exploitation. These groups not only recruit

in person, but they also make use of online spaces and social media platforms. Organised crime group members not only choose to recruit in person, but also take advantage of the online space and social media platforms.

Both human trafficking and human smuggling involve security risks, though these differ depending on whether the country of destination or transit is the country of origin. Among the risks for the country of destination, for example, is illegal employment – carried out in the hidden economy or possibly involving terrorist acts – which raises the question of integration. Transit countries are also at great risk from other crimes, such as trafficking in human beings, arms and drugs. But if there is effective international cooperation between countries, more prosecutions can be pursued more effectively.

Migration to Europe is dangerous not only because it is illegal but also because it is massive, uncontrollable and unmanageable (Fábián, 2020). One consequence of this may be that other organised crimes are also committed. One possible way of avoiding this is for transit countries and destination countries to cooperate in order to at least reduce the risk of the acts described above. With combined human resources and tools, it is possible to carry out permanent monitoring activities in the online space and continuous surveillance along the borders.

4. RESEARCH OBJECTIVES, HYPOTHESES AND METHODS

4.1. RESEARCH OBJECTIVES AND HYPOTHESES

The aim of the study is to raise awareness of how international criminal and judicial cooperation within the European Union can be made even more effective, thereby reducing the threat and security challenges posed by criminal organisations.

The study is based on two hypotheses, which it aims to confirm or refute:

Hypothesis 1.

The entry into force of the Second Additional Protocol to the Convention on Cybercrime will make international cooperation in the field of cybercrime easier because it aims to establish a number of different international cooperation tools, such as the transfer of subscriber data.

Hypothesis 2.

Though the activities of organised criminal groups in cyberspace are becoming more dynamic, the capacities of law enforcement institutions and judiciaries to detect and investigate the proof of crimes already detected will be more efficient if they cooperate through joint investigation teams because any evidence collected by such groups would bridge the divergent laws between member states and so be immediately usable.

4.2. METHODS

The research on which the study was based covered a 12-month period. This was preceded by basic research on the European Investigation Order and the joint investigation team as proactive international cooperation tools. The results of the basic research showed that there are still a number of tools that could be explored and put into practice that would help member states, especially in the fight against organised crime where cyberspace is involved.

As the current study falls under the purview of social science, it employed structured interviewing as its primary research method. The aim of this was to obtain as much information as possible and to compare the answers to the questions in the draft interview. The interviews were all conducted online via Microsoft Teams with the camera on, with 50 minutes allocated for each interview.

The interviews involved five Hungarian investigators and five Hungarian prosecutors, who were homogeneous in terms of interviews, the main criteria being completeness and the need to show how the research results currently compare with the jurisprudence of the member states at an international level. The main criterion for the selection of the interviewees was that each of them should work and cooperate on a daily basis with members of the investigating authority or prosecutors of another member state in cases with international implications, i.e. in certain categories of organised crime, in particular in cyberspace.

The study compared the results of the interviews on three dimensions: (i) the differences and similarities between investigators' responses, (ii) the differences and similarities between prosecutors' responses, and (iii) the differences and similarities between the responses of investigators and prosecutors.

Both groups were asked broadly similar questions; however, there were several different answers. The questions dealt with specific aspects of cyberspace, as the results of the literature analysis pointed to cyberspace as a point of intersection between criminal organisations' various forms of offending activity.

4.3. RESULTS

In line with the assumptions, research questions and objectives outlined at the beginning of this paper, the results of the study "The Effectiveness of International Criminal and Judicial Cooperation in the Context of Cyberspace Tools" were as follows:

> **Question:** In your experience, how difficult is it to detect cybercrime, and what detection and evidence obstacles have you encountered in your work? (On a scale of 1 to 5)

The investigators' scores for this question were all 4 or 5, and, in their short explanatory memoranda, all stressed that the difficulties were caused by the professionalism of the perpetrators, the transnational nature of the crimes and the lack of technical conditions.

> **Investigator 2:** *"…4, because all clues can be hidden in the commission of a cybercrime, if someone knows what they are doing, they have the advantage, but we also have the advantage that if they make a mistake, the perpetrator leaves a clue…"*

Among the prosecutors, the scores were split between 3, 4 and 5. One respondent, who gave a score of 3, commented that the difficulty is a function of how prepared the offender is and how well they can hide any clues left in cyberspace. The scores from the other prosecutors were split between 4 and 5, with the respondents listing several factors that made it difficult for them to detect cybercrime, including the barriers to prosecution between countries, the type of crime (such as overload attacks), and technical barriers, organisational workload and lack of professional skills.

> **Prosecutor 3:** *"…significantly fewer such crimes are detected and proven, especially if the perpetrator knows how to conceal his identity…"*

Talking about the difficulties with detection and evidence, one of the investigators said that "all the clues can be hidden on the Internet, and there is a lot of evidence; it is just difficult to get it". The investigators also listed the lack of appropriate software (for financial reasons), the lack of new technologies and the lack of experts as obstacles. Prosecutors said that hidden IP addresses involving intermediary service providers are very difficult to identify. Problems also include data retention time, a lack of cooperation between service providers, the unavailability of cryptocurrency providers and defensive techniques used in the judicial phase (e.g. by arguing that other people had used the same device or that data had been insufficiently backed up).

> **Question:** How much of a problem is it to investigate and prove cybercrimes involving other country/countries? (On a scale of 1 to 5)

The responses of both investigators and prosecutors to this question were almost identical, and all gave scores between 4 and 5. In most cases, the respondents explained, it is necessary to go to a foreign provider, but the attitude of providers is improving. It was also mentioned that while cooperation within the European Union and contacting an EU member state is smooth, cooperation with third countries is much more difficult.

For example, neither Singapore nor Vietnam responded to requests for mutual legal assistance. Evidence has been very difficult and time-consuming to obtain from China, or there has been no response at all. While contact with Ukraine is no easier, Ukraine has become more active and cooperative in the fight against organised crime since the outbreak of the Russian-Ukrainian war and its expression of the desire to join the European Union.

The United States was mentioned by several interviewees, as most of the service providers are American companies, but the prosecutors said that when it becomes necessary to issue a request for mutual legal assistance to the United States, they take a long time to respond, up to a year and a half, by when the response is no longer relevant. Common to all the responses was that time is a major factor as it is important to carry out investigative actions as quickly as possible, which is important for data retention, and to collect evidence as quickly as possible so that the perpetrator can be brought to justice before they cover their tracks in cyberspace.

> **Prosecutor 4:** "*…it is not so much the cooperation but the time factor that is difficult, the problem of data retention, contacting third countries and asset insurance, usually the money is not there anymore…*"

> **Investigator 1:** "*…if it is a state party to the Budapest Convention, it is easy to prove with a European Investigation Order; if not, then only legal assistance…*"

> **Question:** How well do you think countries can cooperate internationally to fight cybercrime? (On a scale of 1 to 5)

The police investigators' scores for this question were all either 4 or 5. They reported that, in their experience, countries can cooperate well, but this has mostly been within the European Union and is dependent on a lot of direct, personal contact. When there is no personal point of contact, a request sent via SIENA (Secure Information Exchange Network Application) may take several months to receive a response (depending on the country). For any cooperation, the question is always about how long it will take to get a response. For example, how soon can the investigating authority of the other country contact the service provider?

Among prosecutors, the picture was more nuanced. All gave a rating of 3 because they found that they do not follow the other country's mutual legal assistance, do not comply with the requesting country's rules of criminal procedure, and prioritise their own procedures. They had had some positive experiences but said that time is of the essence, and the time it takes to receive a response to a European Investigation Order or mutual legal assistance is not always the same. They also said that they try to rely on personal contacts and will ask Eurojust to help them connect with the country they are looking to cooperate with.

> **Prosecutor 1:** *"…3, there are good examples, and there are bad examples, sometimes countries cooperate quickly and helpfully, sometimes not; in mutual legal assistance, I see the fault in the fact that the other country does not deal with what is in mutual legal assistance, their own country comes first, it is best to go directly to the request, and unfortunately often they do it badly, not according to the procedural rules…"*
>
> **Question:** What can you tell us about the practices of the member states within the European Union?

In their responses to this question, investigating authorities said that similar tools are available in the field of criminal cooperation in all EU member states, but the question is which technology and software is available in which state (an example was given of an efficient blockchain analysis software used in Germany). One prosecutor pointed out that Romania is surprisingly at the forefront in the fight against cybercrime, as are Poland and Estonia, where a specialist unit has been set up, and continuous monitoring and risk analysis are carried out. Prosecutors were also most concerned about the differences in legislation (criminal procedure law). However, as has been said several times, the respondents unanimously answered that the fact that data is stored for different periods in each country is a major obstacle.

> **Investigator 3:** *"…about everyone is at the same level, non-EU countries are harder to cooperate with. Ukraine is like that, but since the war, they are very much together, trying to be cooperative. With Turks, it's hard; they don't necessarily respond…"*

> **Prosecutor 3:** *"…the Estonians have a cybercrime unit that monitors all crimes committed in the online space and also carries out continuous monitoring and risk analysis…"*

> **Question:** How do you think international criminal and judicial cooperation on cybercrime has changed in recent years?

According to the interviewees, within the European Union, cooperation between member states has improved a lot in recent years, facilitated by the activities of Europol and Eurojust and the development of practices and networks between law enforcement authorities and prosecutors. The willingness to cooperate is hampered by the different legal systems in the countries, which, in practice, are circumvented by alternative solutions, such as leveraging personal contact capital. In almost all cases, it was stressed that good cooperation makes it easier to obtain evidence.

> **Prosecutor 4:** *"…there is progress in this, the tools are there, people just don't know about it and don't use it…"*

> **Investigator 5:** *"…moving forward in a positive direction, bilateral relations are also getting closer…"*

To prove or disprove the first hypothesis, the following questions were asked:

- Are you familiar with the innovations contained in the Second Additional Protocol?
- What are your views on them?
- In your opinion, in what direction will the entry into force of the Second Additional Protocol advance the work of cybercrime investigators in the future?

The Second Additional Protocol is not yet in force but is now available. Interviewees unanimously agreed that there could be a number of positive aspects to this cooperation, especially regarding service providers, who will be obliged to respond more quickly and the information obtained from whom will be considered as evidence. This, they said, for

example, will facilitate cooperation with countries that are not members of the European Union but have signed the Convention on Cybercrime (Budapest Convention), meaning that no mutual legal assistance will have to be sent to these countries to obtain evidence following the information received. Reflecting this, they that the European Union has noticed the shortcomings and has, therefore, reacted to them.

> **Investigator 2:** *"…good, because there will be direct data acquisition, more and more countries will sign the protocol…"*

> **Prosecutor 1:** *"…it can be used in the judiciary; it will have to react faster, it will speed it up, it is not yet in law…"*

Given the results of the interviews, the study confirms the first hypothesis, namely that the entry into force of the Second Additional Protocol to the Convention on Cybercrime will facilitate international cooperation in the field of cybercrime.

To prove or disprove the second hypothesis, the following question was asked:

- How effective and efficient do you think a joint investigation team is when it comes to cybercrime?

One interesting finding of the research was that opinions on this question were divided into two groups. Those interviewees who had not worked in a joint investigation team before claimed that it is a lengthy and bureaucratic process, "too many people have to say yes to it", as one respondent said. The other camp, who have had worked in joint investigation teams, had almost exclusively positive things to say about the experience, saying that it speeds up the exchange of evidence, it is faster, you don't have to wait months for a response, it is supported financially and technically by Europol and Eurojust, and even prosecutors are involved, which helps to think together and make investigations more effective. This was the same among both the prosecutors and the police investigators.

> **Prosecutor 4:** *"…a question of openness, lack of knowledge, fear of the unknown…" / "…it would be very good, no need to send legal advice on who should do what, simple exchange of evidence.."*

The second hypothesis was partly supported by the research results, i.e. cooperation in a joint investigation team would make the investigation and proof of cybercrime more efficient. Efficiency in this regard means that the authorities have quick access to evidence of sufficient quality and that the investigative phase can be conducted in a relatively short time (Vári, 2014a).

Overall, the research results show that there are factors that depend on the individual and their qualifications, openness and mindset, as well as external influences, such as the time factor, that need to be addressed to conduct effective investigations.

5. THE AVAILABLE INTERNATIONAL COOPERATION TOOLS

For any crime, the existence of evidence is crucial, and without it, criminal proceedings will not even reach the judiciary. Obtaining or exchanging evidence – in this case, electronic evidence – becomes even more difficult and problematic, and care must be taken to ensure that the information received is converted into evidence before charges are made.

In Hungary, the tools to obtain electronic evidence and information most often used by the police and prosecutors offices are, in order: direct requests for data, data preservation requests, the European Investigation Order, and mutual legal assistance. The first two instruments are criminal cooperation instruments (providing the possibility to obtain information); the third and fourth are judicial cooperation instruments (providing the possibility to obtain evidence).

The available international cooperation instruments were examined during the interviews, with the most frequently mentioned instruments presented below.

During the interview, a separate section was devoted to the acquisition of electronic evidence from another country and asked the question:

- What tools do you use to obtain electronic evidence if the crime involves another country?

The zero-one that investigators use on a daily basis is OSINT (Open Source Intelligence), and they primarily try to obtain as much information as possible on their own, within their country's borders. The most important sources of information are social networking, grey literature, open repositories, registries, traditional media and Internet news (Nyeste & Szendrei, 2019, pp. 56–57). It is also important to take the first investigative acts towards the other country at the same time in order to reduce the loss of evidence. A complex vision is always needed to recognise and react to the characteristics of a crime.

Following OSINT, there are several tools that can be used in parallel, depending on the nature of the crime. Firstly, Europol:

Europol is perhaps one of the bodies that can most help member states investigations, both financially and professionally. The SIENA channel[1] set up by Europol is already a tool that can be used on a daily basis by investigative interviewers. It allows the investigating authorities of the member states to request information from each other or from Europol. It also enables them to ascertain whether a member state is pursuing a similar case, which is a good starting point in case of a positive response, but only information can be obtained this way.

The SIRIUS project,[2] set up by Europol and highly appreciated by investigators and prosecutors, also provides significant benefits for those familiar with the platform. All useful documents and information are available via SIRIUS, which can speed up work, and it provides a forum that makes it possible to consult with investigators and prosecutors from other member states. It also offers several sample requests and guidelines for service providers.

In the field of cybercrime, one of the tools most commonly used by investigating authorities is the direct request for data from service providers.

[1] The SIENA channel is a platform created by Europol to enable the rapid exchange of operational and strategic information. Available at https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena

[2] Available at https://www.europol.europa.eu/operations-services-innovation/sirius-project

This is said to be the quickest way to obtain information that can point the way forward. In addition this, some providers – such as Google, Paypal, Binance and Coinbase – provide a "law enforcement portal" where you can upload a request with a short factual statement and where they will respond. This saves investigators time if they are familiar with and use these platforms where, as noted, time is especially of the essence in the field of cybercrime. Some providers also support the authorities by providing an "emergency" email address via which they will respond to requests almost immediately – though this is only information and not evidence.

To obtain electronic data, investigators use the data preservation request, in practice referred to as 24/7, sometimes in parallel with a direct data request. This tool is based on Articles 29 and 30 of the Budapest Convention on Cybercrime.[3] Thus, any country that has signed and ratified this Convention can send and receive data preservation requests to any other country that has also signed it. Incidentally, the data thus received is also considered as information. The great advantage of the Budapest Convention is that it has been signed by more countries than there are members of the European Union, 69 in total, including African and South American countries.

The secure exchange of documents and protocols between countries was discussed in terms of the ELF (Exchange of Large Files)[4] platform for members of investigating authorities.

There are two very important tools used by prosecutors to cooperate with investigators. The first is the European Investigation Order (which can only be issued between EU member states); the second is mutual legal assistance. The digitisation of the European Investigation Order has been a great help for the prosecution service since it is faster and less costly than it was beforehand (e.g. in terms of translation and postage), so they are happy to use it where possible and if the other member state requested has digitised it. Evidence is obtained by both means.

[3] Council of Europe (2001). Convention on Cybercrime, Budapest. Articles 29 and 30.

[4] Available at https://elf.sourceforge.net/

The work of the prosecution service is also supported by Eurojust,[5] where prosecutors from the member states are available to facilitate communication and judicial cooperation between prosecutors.

The use of a joint investigation team as a cooperation tool has already been mentioned, but it is important to stress that it is also available as an option where there is no loss of time and investigators and prosecutors are able to work together effectively.

One possible tool for cooperation with third countries is to contact Interpol as well as liaison officers and embassies.

Interviewees said that there were several cases involving cyberspace where proceedings were terminated or suspended because evidence was no longer available and where time was a factor once again, whether because of slow international cooperation, a lack of knowledge of the possible means of cooperation, or different retention times between countries.

CONCLUSIONS AND RECOMMENDATIONS FOR THE FUTURE

The conclusions of this research can be considered from the perspective of a European Union member state, how Hungarian professionals see the situation in the European Union and what their experiences with the practices of the other member states are, how other countries cooperate and what tools those countries have.

One key point that the research made clear is that the financial situation of a country is one of the most important factors influencing how much a government can fund and support the fight against organised crime. Hence, it can be seen that there are more developed and less developed countries in this field.

[5] Available at https://www.eurojust.europa.eu/

Another finding was that the retention of data varies from country to country: some countries retain data for a year (see our country), others for 8–10 days or not at all. Consequently, all the cooperation tools can be rendered useless if, for instance, evidence such as a call log or IP address is no longer available.

Finally, the research showed that some member states need to cooperate more often, others less, but it is crucial that the principle of reciprocity is respected by all. Therefore, countries should not prioritise their own prosecutions or avoid answering requests from other countries.

Any agreement to create a joint investigation team is a matter of leadership, both from the police and the prosecution. It depends on how the leader in question feels about cases with an international dimension and how well versed they are personally in international cooperation. If more than two countries are linked by a case, then countries should certainly consider setting up a joint investigation team.

It is clear that the European Union is doing its utmost to make cooperation easier and is constantly monitoring what measures and legislation are needed in the fight against organised crime. Nonetheless, it would be worthwhile to initiate measures and standardise data retention as well.

In the case of the member state presented, Hungary, it is important to provide as much training as possible in the field of cybercrime, to participate in professional forums, to raise the level of professional knowledge (which varies from one country to another) to near equal to other countries, to ensure that the awareness of existing cooperation channels is as wide as possible, and to make greater use of those same channels.

Based on some of the phenomena discussed in the literature, it can be said that if countries recognise the link between cyberspace, migration and organised crime, they should definitely consider the tools presented here. At the same time, migration in itself can lead to a range of further threats, including social, terrorist and economic ones. Organised crime, such as migrant smuggling, can also take advantage of migration, though the phenomenon of migration does not automatically follow from the presence of organised crime. The dangers of the link between globalisation and migration should also be underlined, although it should also be

remembered that local, in-country management is a priority and that it is also worthwhile to cooperate at an international level.

The current research contributes to the field by identifying the obstacles to cooperation in the investigation of the offences described in the literature. By examining how the available cooperation tools could be used to make international investigations even more effective, it highlights the need to address the scientific aspects of making the fight against organised crime more effective.

The research results highlight problems that need solutions. However, they also point to new directions, making it essential that further studies on this topic are carried out in the future, including in other member states, thus helping international cooperation in theory.

SUMMARY

To sum up, in the member states discussed here, neither criminal nor judicial cooperation currently functions sufficiently smoothly (in many cases due to error on the part of those involved in the cooperation, in others due to external causes – as discussed in the research findings). The reasons for this are that the people working at the end-points are no longer informed about the current changes and that the majority are unmotivated and afraid of new opportunities because the force of habit can easily prevail if one's eyes are not open. That is why it is sometimes worthwhile to be self-critical.

While it is clear that there are organisational initiatives in the Hungarian police and the Hungarian prosecution service, they would perhaps be more effective if they were centralised under the purview of one body. Although financial support would contribute greatly to the fight against organised crime, in most areas, there is still room for independent development, which should first be developed within the country and then expanded to the international sphere. As crimes against life, limb and health are slowly becoming the only crimes that do not involve the digital sphere, there is an imperative need for a change in how cyberspace is

approached by law enforcement authorities. This places a heavy burden on professionals, but we must try to keep up with the offenders.

In international terms, Hungary's situation with regard to the fight against organised crime can be considered typical within the European Union. Nonetheless, as explained above, there are countries where, among other things, major organisational changes have already been made to cyberspace to make investigations and prosecutions more effective. In these countries, it was determined that just as the fight against organised crime is always a major challenge, when it is combined with cybercrime, even more time, energy and money need to be invested.

As far as migration and cybercrime are concerned, it is necessary to have the capacity to assess which countries are at risk, which are the destination countries, which are the transit countries and what the statistics show and to strive for maximum efficiency through continuous risk analysis, because "the pursuit of security is a basic and elementary human need" (Kondorosi, 2009, p. 112). Therefore, it is valuable to examine the practices of other countries to get a picture of the country itself and to see where there is room for improvement.

There are three things to focus on when it comes to international cooperation to increase efficiency and reduce security challenges: first, always keep the task in mind; second, good communication; and third, good relations. It is also important to focus on awareness-raising, which should start early in the professional's career.

Finally, the paper concludes with a quote calling for everyone to keep an open mind and to think broadly and globally.

> *One of the main cyber-risks is to think they don't exist. The other is to try to treat all potential risks.*
>
> Stephane Nappo

Contacts:

Ivett Csontos-Nagy, MA

Email: ivett364@gmail.com

Ludovika University of Public Service

REFERENCES AND SOURCES

Achilli, L. (2016). Irregular Migration to the EU and Human Smuggling in the Mediterranean: The Nexus between Organized Crime and Irregular Migration. *IEMed Mediterranean Yearbook*. Barcelona: IEMed.

Council of Europe (2022). Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, Strasbourg.

Council of Europe (2001). Convention on Cybercrime, Budapest.

European Council (2024). The EU's fight against organised crime. [www] https://www.consilium.europa.eu/en/policies/eu-fight-against-crime/#how [Viewed on 22.04.2024].

Europol (2024). Decoding the EU's most threatening criminal networks. Luxembourg, Publications Office of the European Union.

Fábián, P. (2020). A migrációról. Ügyészek Lapja, Vol. 6. [www]. https://ugyeszeklapja.hu/?p=3061#easy-footnote-bottom-49-3061 [Viewed on 29.04.2024].

Gyaraki, R. (2019). A kiberbűncselekmények megjelenése és helyzete napjainkban, A bűnügyi tudományok és az informatika, Pécsi Tudományegyetem Állam- és Jogtudományi Kar; MTA Társadalomtudományi Kutatóközpont, Pécs, Budapest, p. 85. [www] https://real.mtak.hu/108477/ [Viewed on 29.04.2024].

Kondorosi, F. (2009). *Válság és veszélyek a nemzetközi kapcsolatokban*. Budapest: Urbis Kiadó.

Malas, M.-H. (2017). Cybercriminology, Oxford University Press, New York, p. 365.

Mezei, K. (2019). A bűnügyi tudományok és az informatika, Pécs, Magyarország, Budapest, Magyarország: Pécsi Tudományegyetem Állam- és Jogtudományi Kar (PTE ÁJK), MTA Társadalomtudományi Kutatóközpont, p. 135.

Milovanovic, D. (2023). Illegal migration as a form of organized crime and security risk, 96th International Scientific Conference on Economic and Social Development - Era of Global Crises – Belgrade, 18-19 May 2023, pp. 323-325.

L'Hoiry, X.; Moretti, A. and Antonopoulos, G. A. (2024). Human trafficking, sexual exploitation and digital technologies, Trends in Organized Crime. pp. 1–9.

Leukfeldt, E., R.; Lavorgna, A. and Kleemans, R., E. (2016). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the

Conceptualisation of Financial Cybercrime as Organised Crime, European Journal on Criminal Policy and Research, Vol. 2. pp. 287-300.

Nyeste, P. (2013). A nemzetbiztonsági célú stratégiai felderítés/elhárítás és a bűnügyi célú stratégiai hírszerzés összehasonlítása, kiemelten a szervezett bűnözés elleni fellépés területén, Felderítő szemle, Vol. 12, No. 1. p. 111.

Nyeste, P.; Szendrei, F. (2019). Nyílt forrású információgyűjtés a bűnüldözésben, Nemzetbiztonsági szemle Vol. 7, No. 2. pp. 50–67.

Szuhai, I. (2017). Migráció és emberkereskedelem válság idején – A szíriai konfliktus és a kiszolgáltatottság kapcsolatának dinamikája, Magyar Rendészet, Vol. 17, No. 3. pp. 75-81.

Ripszám, D. (2020). Emberkereskedelem az interneten [www] https://www.kre-dit.hu/tanulmanyok/ripszam-dora-emberkereskedelem-az-interneten/ [Viewed on 3.05.2024].

Samdani, S.; Dr. Malik, A., A. (2023). Understanding the role of data privacy in the investigation and prosecution of digital crimes and real crimes, Conference on Digital Forensics.

Vári, V. (2014a). Hatékonyság a nyomozásban. In: Schaub, Anita; Szabó, István (szerk.) III. Interdiszciplináris doktorandusz konferencia 2014 = 3rd Interdisciplinary Doctoral Conference, Pécs, Magyarország: Pécsi Tudományegyetem Doktorandusz Önkormányzat (2015) 1,070 p. pp. 177-195., 19 p.

Vári, V. (2014b). Hatékony vagy eredményes bűnüldözés = Efficient or effective the criminal investigation. MAGYAR RENDÉSZET, 14 (1). pp. 87-97.

Wall, D. (2015). Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime, The European Review of Organised Crime, Vol. 2(2), p. 74.

Whelan, C., Bright, D., Martin, J. (2024). Reconceptualising organised (cyber) crime: The case of ransomware, Journal of Criminology, Vol. 57, Issue 1.