PÉTER NYESTE

THE IMPACT OF THE PANDEMIC ON CRIMINAL INTELLIGENCE[1]

Abstract

The global pandemic, COVID 19 and its mutations have a significant impact on the structure of crime and law enforcement, and it will have a serious impact in the near future, on the branch of the criminal service. In my research, I examine the impact of a pandemic on global and domestic crime and how resilient law enforcement has been to respond to these challenges. I examine and present the changes in the structure of crime as a result of the pandemic, relying on international law enforcement professional sources. I established the trends and data on domestic crime on the basis of interviews and the analysis of statistical data.

In my research I have found that there have been changes in the qualitative and quantitative structure of crime due to the forced effects of the pandemic on society and I made suggestions for more effective law enforcement and intelligence activities.

Keywords: criminal intelligence, impact of pandemic, crime

The development and change of domestic criminal intelligence

Based on the professional history development of the Hungarian criminal service branch, already at the end of the 1880s the aim of the detectives' criminal intelligence activities was to monitoring, preventing and detecting crime. In order to monitor crime, effectively prevent, interrupt and detect crime, confidential intelligence procedures were carried out, such as surveillance, informants, covert methods of information gathering and various traps.

The confidentiality of criminal intelligence was justified by the nature of the assumed offenses (eg. crime without victim, political nature, identity of interest between the parties, organized crime, etc.) or by obtaining information with confidence way, informants or by an effectiveness of investigation.

Revolutionary events, periods of World War, new types of political crimes, which could have posed a threat to the whole society, social order, ruling regime, necessitated the detection of political crimes, primarily of a communist nature, and the development of an organizational system suitable for their prevention.

These extraordinary (revolutionary, war) circumstances necessiated the complex development of organizational systems suitable for obtaining information on a confidential basis (eg. police, gendarmerie, customs guard, army) in Hungary. Later,

[1] The publication was implemented with the support of the National Research Development and Innovation Fund TKP2020-NKA-09 project, in the financing of the Thematic Excellence Program 2020 application program

due to the prevention of parallel information and procedures of a state defense nature, an information center was established, but it ceased to function at the end of the Second World War.

In the losing domestic political situation of the Second World War, the social and political system of the country, based on centuries of civil traditions, gradually transformed. The new, dictatorial, Soviet-type, ideologically based social and political transformation changed the organization and goals of criminal intelligence.

The covert methods and procedures that have been preparing the judicial activity so far have been named secret operational activities and the state defense and state security units serving the ideological and political system have been set up on the Soviet model.

The secret operational activities did not have a preparatory role for the judiciary, and the prosecutor's office supervising the legality of the investigation could not have been aware of them. The use of confidential information gathering tools that severely restrict fundamental human rights took place without external scrutiny.

After the change of regime, following the so-called Danube-gate[2] scandal, the Parliament enacted Act X of 1990 on the temporary regulation of the licensing of special intelligence equipment and methods to regulate the secret information gathering activities of secret services and law enforcement agencies.

There was still no legal regulation on the use of internal authorized secret means and methods for law enforcement (and state security) purposes other than those subject to external licensing.

More than a hundred years have passed since the establishment of the Hungarian Detective Corps until the change of regime, and the nature and character of crime and criminal offenses have changed significantly, but the circumstances underpinning confidential information (eg victimlessness, organized crime) have not changed. These circumstancies continue to justify to collect information and record data without the knowledge of the party concerned, using appropriate external control.

After a long preparatory work, was born in 1994 The Act on the Police, which regulates the secret gathering of information for “criminal purposes” in a separate chapter (VII.), Which became a new, legal-level name for the activities called earlier ”covert confidental procedures” and later „secret operational tools and methods”. With this, the prevention, detection and proof of crime has gained new, available, legally regulated opportunities, with little external control.

The criminal intelligence system based on the internal, classified norms was similar of the procedures prior to the change of regime. The secret information gathering procedure was divided into two stages. The first phase was the control of

[2] In December 1989, the State Security Service of the Ministry of the Interior conducted secret means and methods of investigation against opposition parties and organizations, despite the fact that under the new constitution adopted on October 23, 1989, this was already illegal and even unconstitutional activity.

the primary information called secret control of information and the second phase was further verification of the information supporting the suspicion called secret investigation.

This continues to mean that the investigating authority independently, at its discretion, ordered and carried out a secret information gathering procedure at the aim of criminally relevant information check, at the aim of finding of suspicion and the existence of evidence without a substantive external audit.

In 2018, the time has come to transform the domestic criminal intelligence system and legal bases in order to ensure the continuity of supervision, investigations, the loss of information and the strengthening of the law.

The new Criminal Procedure Act, which entered into force on 1 July 2018, changed in system level the law enforcement model according to which the tasks of criminal intelligence remained in the Police Act, the National Tax and Customs Administration Act and the Prosecution Act. The covert methods for criminal investigation purpose are set out in the Criminal Procedure Act.

The established system of procedures ensures the possibility that proactive prior detection can be applied within a short period of time before ordering an investigation, but already within the framework of criminal proceedings.[3]

Current modern criminal intelligence[4]

First, domestic modern criminal intelligence needs to be defined on the basis of relevant legislation and literature, and then we take an international perspective.

In order to achieve the policing and law enforcement objectives (protection of public security, public order and state border, prevention and detection of criminal offenses) reflected in the Hungarian Basic Law the Hungarian modern criminal intelligence activity can be characterised as a proactive information gathering and analysis activity for the respect for family life, private residence and correspondence and its closely related information self-determination, the free flow of information and the protection of personal data[5].

Domestic criminal intelligence can basically have strategic, tactical or investigative support tasks.

The starting point of *strategic criminal intelligence*[6] is strategic criminal analysis, which provides criminal analysis methods and examines the extent, dynamics and structure of crime, as well as the long-term pattern and tendencies of the characteristics and prevalence of certain crimes.

---

3 NYESTE, Péter – SZENDREI, Ferenc: A bűnügyi hírszerzés kézikönyve; Dialog Campus, 2019.

4 NYESTE Péter: A bűnügyi hírszerzés; Magyar Rendészet 2012/4. pp. 25-32.

5 NYESTE, Péter – NAGY, Ivett: A bűnügyi hírszerzés az elméletben és a gyakorlatban; Rendőrségi Tanulmányok vol. 2021/1. pp. 1-2.

6 23/2018(VI.21.) ORFK Utasítás a Bűnügyi Elemzési Szabályzatról 2.§ n) pontja

The aim of strategic criminal intelligence is to satisfy current news needs formulated on the basis of continuous strategic analyzes and thus to establish strategic decision-making.

The purpose of *tactical intelligence* is to serve the immediate prevention, handling and solution of individual and specific criminal problems.

This includes intelligence activities that can be carried out in order to maintain the criminal intelligence infrastructure (eg protection of informant, covert investigator), but also protection of privileged persons and places based on risk analysis.

The starting point for *investigative criminal intelligence*[7] is investigative support analysis, which is the activity of examining data obtained through individual criminal proceedings and from the use of secret information gathering and from special investigative methods, which can assist in detecting an unknown perpetrator, planning investigative actions, to recognize the connections between the objects that can be connected to them, to detect organized criminal groups and their activities, to define the tasks of law enforcement work against the groups.

The task of criminal intelligence in support of an investigation is to provide information and result products (possible means of proof) to support further investigations based on the data containing individual and specific criminal offenses or elements referring to them.

In the European Union, instead of the concept of criminal intelligence, the term special investigative activities and special investigative tools can be found, and these indicate that the purpose of collecting confidential manner criminal information is to prepare and assist justice.

At the same time, criminal intelligence as crime monitoring, mapping of organized criminal groups, crime prevention, and the facilitation of other law enforcement tasks under police and other laws, are used yet with appropriate control outside of criminal proceedings.

In the European Union, by Special Investigative Means (SIM) we mean those special tools and methods, with the help of which evidence or information and analyzed information can be obtained in a covered way, without the knowledge of the person concerned. Their deployment will involve a breach of the right of private right, wich will have to be justyfied by those carrying out/ authorising the operation.[8]

The concept of special investigative tools is similarly defined in the European Union Recommendation:[9] “special investigation techniques” means techniques

---

7 23/2018(VI.21.) ORFK Utasítás a Bűnügyi Elemzési Szabályzatról 2.§ k) pontja

8 Council of Europe Office in Belgrade: Deployment of special investigative means. Belgrade, 2013. pp. 12-13.

9 Recommendation Rec (2005) 10 of the commitee of Ministers to member states on „special investigation techniques” in relation to serious crimes including acts of terrorism; https://www.legislationline.org/download/id/1732/file/46f9ab2c5ef4d150d845540a9b79.pdf (downloaded 22 September 2021)

applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons.

According to a report[10] prepared by the European Commission's Directorate-General for Migration and Home Affairs, the special investigative tools, technical, can be divided into two parts: one part is the so-called "Legal instruments" that belong to the area of justice (e.g., witness protection), the other is "investigative tools" as well as in law enforcement operations.

The report identified and examined eight special investigative tools:

– Interception of communication: interception of post, wiretapping, bugging, telecommunication data, location acquisition, telecommunication devices, computer remote searching, mobile and radio frequency identification devices, computers and Internet data file control devices are used to detection of serious crimes and usually for a maximum period of 6 months.

– Surveillance activity is not interpreted uniformly in the Member States. Some Member States distinguish between technical surveillance and non-technical surveillance (Austria, Belgium, Finland, France, Luxembourg), other Member States distinguish between short-term and long-term surveillance and distinguish between surveillance with or without a judicial authorization.

  The broader concept of observation can be the collection and examination of samples in a covered way, the replacement of goods in a covered way, the taking of videos, the taking of photographs in a covered way, hidden image recording, body-mounted hidden devices and tracing.

– Covert investigations refer to the following investigative activities in Europe: infiltration, pseudo or test purchase, participation in controlled deliveries[11].

  It is carried out by a trained member of the authority or by a civil person, who conceals his identity by means of cover documents. There are three types of use of undercover investigators: the first is the general, systematic collection of information to detect specific crimes, the second is the execution of short-term pseudo purchase type operations, and the third is long-term infiltration in a criminal organization.

– Controlled delivery is the technique of allowing illicit or suspect consignments to pass out of, through or into the territory of one or more States, with the knowledge and under the supervision of their competent authorities, with a view to the investigation of an offence and the identification of persons involved in the commission of the offence.

– Employment of Informants, as defined by Europol[12]

---

10 DI NICOLA, Andrea – GOUNEV, Philip – LEVI, Michael – RUBIN, Jennifer: Study on paving the way for future policy initiatives in the field of fight against organised crime: the effectiveness of specific criminal law measures targeting organised crime; Final report, February 2014, Brussel p.223.

11 Ibid. p. 266.

12 EUROPOL: Covert Human Intelligence Source Handling, European Union Manual on Common Criteria and Priciples, Europol, 2012. (Law enforcement only) p. 8.

Informant is a person who, in return for a guarantee of confidentiality, provides information, inside knowledge or assistance to the competent law enforcement agencies or intelligence services which facilitates the detection, investigation and detection of criminal offenses.

Two large groups of informants have emerged in the EU, which are often used in parallel in one Member State (eg Hungary). One group includes the employment of informants by a dedicated special unit (eg National Investigative Unit of Rapid Respond Police) developed and supported by Europol, the other model is the traditional one, in which any law enforcement investigator himself selects, studies and recruit their informants. In the latter case, the control and supervision of informants and contacts is only periodic.

– Joint investigation teams: a fixed-term group of judges, prosecutors, members of investigative bodies set up for the purpose of a specific investigation by written agreement to investigate criminal offenses involving two or more Member States.
– Witness protection includes the implementation of a witness protection program, which can be applied against protected "witnesses" who meet the requirements.
– "Hot pursuit" allows a person who has been convicted of a crime in one Member State to be prosecuted across borders for the purpose of apprehension.

According to the report, most often measures, that Member States are in place: interception of communications, followed by surveillance tools, followed by informants, followed by the use of a covert investigations, and controlled deliveries, witness protection, joint investigation teams and "hot pursuit".

In terms of the usefulness of the measures, it is first and foremost a very useful special investigative tool the interception of communications, followed by surveillance tools and informants, controlled deliveries, witness protection, and the line is closed by “hot pursuit” measures with case-by-case usefulness.[13]

Special covert investigative activities may be used in the European Union if:
– there is an available, public national legal mandate;
– there is an appropriate authorization and control procedure;
– its application is necessary and proportionate.[14]

The principles of application[15] are necessity, proportionality (with the gravity of the offense and the least possible restriction), and the last principle is the condition of application, "threshold", meaning the connection with a criminal offense. However, this does not preclude using covered measures for the prevention and countering of a public security emergencies (eg protected personal protection, crime prevention).

In the European Union, the need to develop intelligence and analysis-based law enforcement has gradually spread in the various strategic programs and action programs, particularly in order to combat organized crime, terrorism and serious crime

[13] Di Nicola – Gounev – Levi – Rubin (2014) op. cit. pp. 221-337.
[14] Council of Europe Office in Belgrade: Deployment of special investigative means. Belgrade, 2013. p. 13.
[15] Di Nicola – Gounev – Levi – Rubin (2014) op. cit. p. 243.

more effectively. The Hague Program, which is also based on information from strategic intelligence, drew attention to the need to apply a new strategic criminal intelligence methodology to changed crime. The so-called European Criminal Intelligence Model (ECIM) is based on the acquisition and analysis of operational-based quality information. The strategic goal is to reduce the legal, financial and human opprtunities of organized crime.

Based on the information of the criminal intelligence agencies, the data of other public administration control and licensing organizations, the analytical units are able to make a fairly accurate group and activity analysis of the structures identified as criminal organizations.

The legal fixation and application of the criminal intelligence model is mainly in the Anglo-Saxon area, but the EUROPOL Manual on the Use of Covered Human Intelligence sources[16] also discusses in detail the rules for the use of human resources in criminal intelligence as a recommendation to law enforcement.

In addition to the English National Intelligence Model[17], U.S. federal law also discusses in detail the principles of how criminal intelligence systems work. (Code of Federal Regulations, CFR Part 23 Criminal intelligence systems operating policies,).[18] Part 23 of the law describes in detail the rules of operation of law enforcement intelligence systems, which includes the objectives, applicability, operating principles, operational guidelines, system control and audit activities.

The impact of the pandemic on crime and criminal intelligence

The performance of law enforcement agencies has been and continues to be significantly affected by various local, regional or global challenges and emergencies. The COVID 19 virus falls into the latter category and thus has had a global impact and later versions of the pandemic are still affecting law enforcement agencies.

This global epidemic has been a challenge never seen before in modern societies.

Governments had to try at the same time to maintain the standard of services in modern societies, such as security or the operation of the economy, and to ensure stopping the spreads of pandemic and that health care systems were maintained.

Following the emergence of the pandemic in Europe, the primary tasks of law enforcement agencies were to apply quarantine measures, to reduce social contacts, and to apply lockdowns, border closures and border controls. These measures have fundamentally affected the normal performance of law enforcement.

---

16 EUROPOL: Covert Human Intelligence Source Handling, European Union Manual on Common Criteria and Priciples, Europol, 2012. (Law enforcement only)

17 ACPO: Guidance on the National Intelligence Modell; https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf (downloaded 09 September 2021)

18 Criminal intelligence systems operating policies; CFR Part 23, https://www.ecfr.gov/current/title-28/chapter-I/part-23 (downloaded 21 September 2021)

Ensuring the continuity of the work of health authorities and preserving the safety of society by introducing and maintaining various restrictive and control measures was the primary task of law enforcement agencies.

At the same time, after a brief halt, organized crime saw serious opportunities in the effects of the epidemic on society. There have been significant changes in crime and crime trends that have been quiet affected by the closures.

„More people are spending more time online throughout the day for work and leisure during the pandemic, which has greatly increased the attack vectors and surface to launch various types of cyber-attacks, fraud schemes and other activities targeting regular users. A lot of these goods are offered on online trade platforms, which have made it easier and cheaper for counterfeiters and other criminals to access a broad customer base. Creating virtual and obscuring real identities is easier online than in offline interactions, which greatly aids criminals using aliases and creating front companiees online."[19]

The majority of citizens were forced to stay in their homes and forms of crime that targeted people in their homes emerged or intensified. During the pandemic, the grew in fear, frustration, anxiety of citizens making them more vulnerable to crime and criminals responding flexibly to exploiting vulnerable people.

Crime, organized crime, has invented a number of forms of fraud that exploit the above effects of a pandemic. Organized criminals against property gained access into the elderly, vulnerable people's homes with various tricks, impersonation of representatives from public authoryties or medical stuff who providing saniterie products or perform a "Corona test" while stealing property from their homes.

Also a popular method of organised criminal groups to deceive vulnerable elderly people is the so-called "grandson frauds" also increased significantly during the pandemic. Fraudsters use essentially the same method to commit crimes. Elderly victims are called by a member of the organization and pretended to be a relative during the conversation. The caller most often claims to have caused an accident and needs money immediately to make good the damage. The fake relative, to avoid direct encounters, he convinces the victims that he cannot go for the money but sends an acquaintance for it.

A courier is then directed to the home of the elderly, who takes over the money, jewelry. There were also examples of criminals asking for a bank account to transfer money or dictating bank card details and using them to cause property damage through online transactions.

Due to "home office" and "home study", the children and juveniles were often at home without parental supervision and this opprutnities has not been left unused by criminals. Increase in activities related to the distribution of child abuse material online and the conversations of potential offenders around the increased accessibility

[19] Beyond the Pandemic – What will the criminal landscape look like after COVID-19? https://www.europol.europa.eu/newsroom/news/beyond-pandemic-what-will-criminal-landscape-look-after-covid-19 (downloaded 20 September 2021)

and vulnerability of children online due to isolation, less supervision. Online child sexual exploitation includes all acts of a sexually exploitative nature carried out against a child that have, at some stage, a connection to the online environment. There has been a continuous increase in activities related to online child sexual abuse over recent years.[20]

The use of encrypted communication channels, tools, programs, and Darknet forums facilitates the commission of this type of crime. The perpetrators use file-sharing networks and livestreaming platforms.

In both 2019 and 2020, several Darknet marketplaces were liquidated thanks to law enforcement cooperation. A coalition of law enforcement agencies across the world announced the results of a coordinated operation known as DisrupTor which targeted vendors and buyers of illicit goods on the dark web. This operation follows the takedown in May of 2019 of Wall Street Market, the world's then second largest illegal online market in the dark web.[21]

Interpol provides global assistance to law enforcement agencies around the world by continuously updating the International Child Sexual Exploitation database. Interpol's Child Sexual Exploitation database holds more than 2.7 million images and videos and has helped identify 23,564 victims worldwide.[22]

International Child Sexual Exploitation (ICSE) image and video database is an intelligence and investigative tool, which allows specialized investigators to share data on cases of child sexual abuse. Using image and video comparison software, investigators are instantly able to make connections between victims, abusers and places. The database avoids duplication of effort and saves precious time by letting investigators know whether a series of images has already been discovered or identified in another country, or whether it has similar features to other images.

It also allows specialized investigators from more than 64 countries to exchange information and share data with their colleagues across the world. The priority of Crimes Against Children unit of Interpol is to identify and rescue young victims of sexual abuse, block access to child sexual abuse material and prevent sex offenders from travelling abroad to abuse children or escape justice.

Europol established in 2017 the Stop Child Abuse – Trace An Object initiative. This initiative invites the public to identify objects and places in the hope that it can lead to the identification of victims down the line. Since then, Europol has received

---

20 European Union Serious and Threat Assesment 2021; https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment (downloaded 17 September 2021)

21 International sting against dark web vendors leads to 179 arrests; Press release, https://www.europol.europa.eu/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests (downloaded 17 September 2021)

22 International Child Sexual Exploitation Database; Interpol, https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database (downloaded 17 September 2021)

26.000 tips which have already led to the identification of ten children and the prosecution of three offenders.[23]

The rate of domestic violence and sexual abuse crimes among citizens forced into their homes due to the pandemic has also increased in the world.

According to official statistics of the Hungarian Ministry of the Interior[24], the number of crimes "endangering a minor" was 779 in 2019, while in 2020 it was already 964, which means an increase of almost 24%. By September 2021, 651 such crimes had occurred.

The number of „sexual violence" offenses was 240 in 2019 and 327 in 2020, an increase of 36%. By September 2021, 172 such crimes had occurred.

The number of „sexual coercion" crimes was 56 in 2019 and 95 in 2020, an increase of 17%. By September 2021, 42 such crimes had occurred. The number of „domestic violence" crimes was 392 in 2019 and 650 in 2020, an increase of nearly 66%! By September 2021, 410 such crimes had occurred, which is already in excess of the 2019 base year!

Looking at the base year 2019, it can be stated that in 2020, people who forced into their homes due to the pandemic, lockdowns, restrictions, other stressors, and psychological difficulties, caused to them a serious impact and there was a significant increase in deviant behaviors at home, violent, sexual violence within the family have increased significantly.

The numbers for 2021 are more encouraging, but for some types of crime they already exceed the base year, despite the extremely high latency for these crimes.

At the same time, due to the restriction of social interactions and lockdowns and increased law enforcement presence have led to a decline in street violence and property crimes, as well as human trafficking. As a result of supply disruptions, drug trafficking also came to a halt in the beginning. However, it was later stabilized or other supply routes emerged (Dutch, Belgian ports).

There has been an increase in the rate of social engineering attacks, mailware, phishing emails around the COVID 19, in which perpetrators mislead victims by referring to the coronavirus epidemic by selling fake cures or medicines against the coronavirus, or by other epidemic-related fakenews.

It identifies significantly more misleading or deceptive publications than before, so the National Investigation Bureau of the Rapid Response and Special Police Force of Police of Hungary has set up a special investigation team to prevent such crimes from being followed. Fake news or misleading content is experimented with on a daily

[23] Experts meet to identify victims of child sexual abuse; News Article, https://www.europol.europa.eu/newsroom/news/experts-meet-to-identify-victims-of-child-sexual-abuse (downloaded 18 September 2021)

[24] Criminal Statistic System; Ministry of Interior, https://bsr.bm.hu/ (downloaded 18 September 2021)

basis, and the commission of the crime is established, and proceedings are initiated immediately.

In the event of an emergency, new criminal code facts have also come into force, such as the crime of spreading false news suitable for disturbing the general public.

There has been a significant increase in cyber attacks with various extortionist viruses (etc.Wanna Cry, Emotet, NotPetya). It can be observed that the attacks are much more sophisticated, personalized.

In the course of committing a crime, they make contact with the victims and threaten them, which results in a very high latency for such crimes. Typically, they target smaller, less resilient targets with viruses. Users who are forced to go online due to a pandemic with little cyber security awareness can be attacked by installing various malware.

It can be a Bootnet that is an attack on networks, a Rootkit that is gaining administrator privileges, it can be a worm that infects without control, or it may be a Trojan that is embedded in other software, Backdoor which is obtaining remote access, Extortion Virus, Spyware, or Adware that is unsolicited advertising or Scareware which is a fake antivirus program

Today, not only individuals but also various organizations and health care institutions have become the targets of various cyber attacks. During the pandemic, targeted attacks hit hospitals and health care systems.[25]

Significantly increased and sophisticated a business e-mail compromise (BEC) The initial simple phishing and malicious attacks have become more personalised and complex. Ransomware to target particularly affected sectors such as healthcare and education.

The rate of investment fraud exploiting economic fears of the pandemic has also increased. There is an increase in the number of incidents related to bank and loan fraud, money laundering and corruption. The real estate and construction sectors become more attractive for money laundering

According to the official statistics of the Hungarian Ministry of the Interior, the number of money laundering crimes was 188 in 2019, while in 2020 it was already 308, which means an increase of 61%. By September 2021, 168 such crimes had occurred.

The number of „fraud crimes committed using the information system" was 2,624 in 2019, compared to 3,400 in 2020, an increase of nearly 30%. By September 2021, 1,438 such crimes had occurred.

---

[25] PALICZ Tamás – BENCSIK Balázs – SZÓCSKA Miklós: Kiberbiztonság a koronavírus idején – a COVID-19 nemzetbiztonsági aspektusai; Scientia et Securitas, 2021/1. p. 82. https://akjournals.com/view/journals/112/2/1/article-p78.xml (downloaded 08 October 2021)

The number of crimes against the information system or data was 587 in 2019, compared to 830 in 2020, an increase of more than 41%. By September 2021, 579 such crimes had occurred.

Statistics from cases in recent years show that some crimes have moved in online space independently of the pandemic, but forced home stays, lockdowns and increased use of online services during the pandemic have helped increase the number of crimes committed online.

During the pandemic, organized crime also exploited the huge demand for medical devices and hygienie products and sold counterfeit or poor quality medical devices such as masks, rubber gloves or medicines, disinfectants, some of which were actually sold, others only as part of financial fraud. Law enforcement officers identified more than 2 000 links to products related to COVID-19. A Member State's investigation focused on the transfer of €6.6 million from a company to another company in Singapore to purchase alcohol gels and FFP2 and FFP3 masks. The goods were never received. In another case reported by a Member State, a company attempted to purchase 3.85 million masks and lost €300 000. Similar supply scams of sought-after products have been reported by other Member States.[26]

Some business sector suffering negative economic pressures such as hospitality, catering, tourism are becoming more vulnerable to criminal infiltration.[27]

In Italy organised crime networks penetrated the healtcare system and able to divert investements originally aimed at providing financial rosources, equipment and influence procurement, commercial agreement within the healtcare system.[28]

Organized crime, taking advantage of the weakening of closures and supply chains, is vigorously present in the counterfeit and substandard foodstuff and beverage illegal market. During the first months of 2020 there was a decrease in organized crime involvement in food crime. The illicit livestock and meat products remain a threat for public health and potentially add additional risks in the context of the COVID-19 pandemic, and infection can spread rapidly amongst the workers of meat processing plants or in specialized markets. The pandemic created critical shortages of basic necessities (e.g. maize, wheat, dairy products, rice, sugar, tomatoes, vegetables). In lack of genuine raw material, whose cost raised a lot, dishonest producers used low quality or unsuitable ingredients. Consequence has been an increase of illegal, counterfeit and potentially unsafe food on the market.[29]

---

[26] Pandemic Profiteering: How criminals exploit COVID 19 crisis; Report, https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis (downloaded 16 September 2021)

[27] Enterprising criminals – Europe's fight against global networks of financial and economic crime; Report, https://www.europol.europa.eu/publications-documents/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime (downloaded 16 September 2021)

[28] Coronavirus: The impact on crime and criminal networks; Global Initiative Against Organised Crime, https://globalinitiative.net/analysis/crime-contagion-impact-covid-crime/ (downloaded 16 September 2021)

[29] Operation Opson IX. – Analysis Report; https://www.europol.europa.eu/publications-documents/operation-opson-ix-%E2%80%93-analysis-report (downloaded 27 September 2021)

The counterfeit and substandard foodstuff and beverage illegal market poses serious challenges for food safety authorities, who need to obtain up-to-date information in the field of organized crime in order to detect and prevent the placing on the market of food that is harmful to human or animal health.

Europol expects that the impact of the pandemic will unfold in three phases[30]:

- the current and immediate short-term outlook;
- a mid-term phase which will become apparent over the upcoming weeks and months;
- a long-term perspective

In the first phase the most notable immediate impact has been in the areas of cybercrime, the trade in counterfeit and substandard goods as well as different types of frauds and schemes linked to organised property crime. There has been limited impact of the pandemic on the level of terrorist threats to the EU. Another highly visible phenomenon has been the proliferation of scams promoting fake COVID-19 test kits and treatments.[31]

In the second phase (mid-term phase) cybercrime threats are likely to continue to be the dominant threats from serious and organised crime during the pandemic as continued lockdown and social distancing measures will only enhance the reliance on digital services to continue to work and interact.

Child sexual exploitation online will remain a significant threat as a result the lockdown and online education. The trade of counterfeit and substandard goods especially those related to healthcare such as pharmaceuticals and equipment remains very high, counterfeiters will continue to provide counterfeit and substandard versions of these goods.

In the third phase (long-term perspective) communities, especially vulnerable groups, tend to become more accessible to organised crime during times of crisis. Economic hardship makes communities more receptive to certain offers, such as cheaper counterfeit goods or recruitment to engage in criminal activity.

Some of the most threatening organised criminal groups (mafia-type) are likely to take advantage of a crisis and persistent economic hardship by recruiting vulnerable young people, engaging in loan-sharking, extortion and racketeering, among other criminal activities. Organised groups are able to exploit the global financial crisis with real estate investments, which allowe them to launder illicit profits.

Cybercrime activity is unlikely to diminish and new cyber threats that have emerged during the COVID-19 pandemic will continue to target victims even after

[30] Beyond the Pandemic – What will the criminal landscape look like after COVID-19? https://www.europol.europa.eu/newsroom/news/beyond-pandemic-what-will-criminal-landscape-look-after-covid-19 (downloaded 20 September 2021)

[31] European Union Serious and Threat Assesment 2021; https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment (downloaded 17 September 2021)

the end of the current crisis. A global recession as a result of the COVID-19 pandemic is likely to have a significant long-term impact on migration.

The long-term impact of the COVID-19 pandemic may be particularly significant in the area of economic and financial crime. Criminals will likely intensify their use of shell companies and companies based in off-shore jurisdictions with weak anti-money laundering policies.

Cashless payment options are likely to continue to become popular, which are key targets for cybercriminals

Europol's databases are updated by obligatory data uploads from Member States' authorities. Based on these, its ex-post and forward-looking analyzes are of paramount importance to the governments and law enforcement agencies of the European Member States.

Conclusions

Member States' criminal intelligence systems and procedures have been and continue to be affected by the pandemic. Mainly during the initial period of the pandemic, law enforcement agencies had to perform other tasks to reduce the health risks of the pandemic or to carry out control tasks at the state border instead of their usual tasks.

As a result, the investigations were delayed in time, and some procedural acts could only be carried out later. In several cases, the investigators were also infected with the coronavirus and after thus were able to perform their duties with a reduced number of staff. Of course, investigating and following up the legality of high-profile crimes was a priority even during this difficult period.

In addition to the aforementioned difficulties of investigations, the lockdowns and restrictions made difficult for the criminal staff of law enforcement agencies to handle covert informants. Certain covert measures were more difficult to enforce against criminals forced to stay longer in their homes. Effective action against new criminal trends requires closer cooperation between law enforcement agencies and national security services.

Law enforcement has greater emphasis must also be placed on monitoring, detecting new criminal trends, and preventing crime. Close co-operation is needed between police counter-terrorism units, given the link between organized crime and terrorist organizations. The latter are strongly present on online platforms.

The intensification of crime and organized crime online performance has entailed the importance of training investigators in cybercrime and strengthening the anti-cybercrime activities of organized crime units.

Responses to the current challenges of cybercrime include the operation of international cooperation channels 24/7, the development of virtual currency analyzes, the development of Big data, the use of Darknet operations, the use of covert investigators, covert informants, and ever closer cooperation with NGOs and continuous organization of awareness - raising campaigns (eg ENISA, Europol, National Investigation Bureau of the Rapid Response and Special Police Force of Police of Hungary).

Bibliography:

- 23/2018 (VI.21) ORFK Utasítás a Bűnügyi Elemzési Szabályzatról
- ACPO: Guidance on the National Intelligence Modell; https://whereismydata.files.wordpress.com/2009/01/national-intelligence-model-20051.pdf (downloaded 09 September 2021)
- Beyond the Pandemic – What will the criminal landscape look like after COVID-19? https://www.europol.europa.eu/newsroom/news/beyond-pandemic-what-will-criminal-landscape-look-after-covid-19 (downloaded 20 September 2021)
- Coronavirus: The impact on crime and criminal networks; Global Initiative Against Organised Crime, https://globalinitiative.net/analysis/crime-contagion-impact-covid-crime/ (downloaded 16 September 2021)
- Council of Europe Office in Belgrade: Deployment of special investigative means; Belgrade, 2013.
- Criminal intelligence systems operating policies; CFR Part 23, https://www.ecfr.gov/current/title-28/chapter-I/part-23 (downloaded 21 September 2021)
- Criminal Statistic System; Ministry of Interior, https://bsr.bm.hu/ (downloaded 18 September 2021)
- DI NICOLA, Andrea – GOUNEV, Philip – LEVI, Michael – RUBIN, Jennifer: Study on paving the way for future policy initiatives in the field of fight against organised crime: the effectiveness of specific criminal law measures targeting organised crime; Final report, February 2014, Brussel
- Enterprising criminals – Europe's fight against global networks of financial and economic crime; Report, https://www.europol.europa.eu/publications-documents/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime (downloaded 16 September 2021)
- European Union Serious and Threat Assesment 2021; https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment (downloaded 17 September 2021)

- EUROPOL: Covert Human Intelligence Source Handling; European Union Manual on Common Criteria and Priciples, Europol, 2012. (Law enforcement only)
- Experts meet to identify victims of child sexual abuse; News Article, https://www.europol.europa.eu/newsroom/news/experts-meet-to-identify-victims-of-child-sexual-abuse (downloaded 18 September 2021)
- International Child Sexual Exploitation Database; Interpol, https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database (downloaded 17 September 2021)
- International sting against dark web vendors leads to 179 arrests; Press release, https://www.europol.europa.eu/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests (downloaded 17 September 2021)
- NYESTE Péter: A bűnügyi hírszerzés; Magyar Rendészet 2012/4.
- NYESTE, Péter – NAGY, Ivett: A bűnügyi hírszerzés az elméletben és a gyakorlatban; Rendőrségi Tanulmányok vol. 2021/1.
- NYESTE, Péter – SZENDREI, Ferenc: A bűnügyi hírszerzés kézikönyve; Dialog Campus, 2019.
- Operation Opson IX. – Analysis Report; https://www.europol.europa.eu/publications-documents/operation-opson-ix-%E2%80%93-analysis-report (downloaded 27 September 2021)
- PALICZ Tamás – BENCSIK Balázs – SZÓCSKA Miklós: Kiberbiztonság a koronavírus idején – a COVID-19 nemzetbiztonsági aspektusai; Scientia et Securitas, 2021/1. https://akjournals.com/view/journals/112/2/1/article-p78.xml (downloaded 08 October 2021)
- Pandemic Profiteering: How criminals exploit COVID 19 crisis; Report, https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis (downloaded 16 September 2021)
- Recommendation Rec (2005) 10 of the commitee of Ministers to member states on „special investigation techniques" in relation to serious crimes including acts of terrorism; https://www.legislationline.org/download/id/1732/file/46f9ab2c5ef4d150d845540a9b79.pdf (downloaded 22 September 2021)