DR HAB. AGNIESZKA GRYSZCZYŃSKA, PROF. UKSW
Cardinal Stefan Wyszyński University in Warsaw | DOI: 10.32041/9788367149761/0

Preface

We present a monograph summarising the research conducted in 2023 by an international Polish-Hungarian research team on the new trends, challenges and solutions in combating cybercrime. The team was established as part of the Polish-Hungarian Research Platform project organised by the Institute of Justice in Warsaw. The team was composed of Piotr Burczaniuk, Judit Jacsò, Agnieszka Gryszczyńska, Erika Róth, Ferenc Sántha and Rafał Wielki.

The rapid development of digital technology has caused an evolution in criminal behaviour, as it creates opportunities for previously unknown forms of crime. The term "cybercrime" is nowadays widely used, especially in the Council of Europe's Cybercrime Convention, international and national literature, incident reports, scientific publications and the mass media. However, it remains unclear what exactly the terminology means and difficulties in understanding cybercrime also arise from the diversity of terminology and the inconsistency of legislation on cybercrime in different countries.

Meanwhile, analysis of reports on the security of networks and information systems indicates an increasing number of incidents. Certain incidents described in the reports also constitute offences – cybercrimes. Additionally added to the problems associated with defining cybercrime, it is also necessary to overlay the terminology

associated with incidents and particular types of attacks in order to better understand the phenomenon of cybercrime.

The modus operandi of perpetrators of cybercrimes is characterised by a high degree of adaptability to the current economic, geopolitical, and social situation. Perpetrators exploit loopholes in the law, adapting the modus operandi to regulatory changes on an ongoing basis. They make use of modern technological solutions (ICT, AI/ML) that allow them to remain anonymous, communicate efficiently and transfer the proceeds of cybercrime.

In order to conceal their own identity, they create a new identity or use the data of other individuals, use services and technical tools that make it difficult or impossible to analyse network traffic (TOR), determine the IP address assigned to them by the telecommunication network providers (VPN, PROXY), encrypt data and their carriers and use anti-forensics techniques. Crimes are committed by them individually as well as within highly specialised and organised criminal syndicates. The attribution of the attack and the identification of the perpetrators is hampered by the cross-border nature of cybercrime – manifested, among other things, by the need to collect evidence in different jurisdictions.

Considering the increasing number of incidents and cybercrimes and their consequences, research is required to identify solutions that would facilitate the detection of offenders and increase the effectiveness of criminal proceedings.

In view of these identified problems, the main research hypothesis that is being tested in this monograph is the hypothesis that the effectiveness of countering of cybercrime is determined not only by the scope of criminalisation and substantive criminal and procedural law, but additionally there is a need for an ecosystem of criminal, administrative and civil regulations, both at the national and international levels.

To verify this hypothesis, the individual chapters of the monograph address the verification of the following researched questions:

- Is there a generally accepted definition of cybercrime, and is it possible to develop a new classification of cybercrimes that takes into account the latest trends of this form of criminality?

- Does the scope of criminalisation of cybercrime need to be expanded due to the continuous development of tactics, techniques and procedures used by cybercriminals?
- Is there a need to define new forms or methods of money laundering?
- Are current measures in the European Union adequate to combat money laundering?
- Are traditional jurisdictional principles in national and international criminal law able to meet the challenges of cybercrime, in particular positive jurisdictional conflicts?
- Are the responsibilities and international cooperation of cyber security actors and law enforcement agencies carrying out reconnaissance activities sufficient, given the nature of the current types of cybercrime, and what are the most significant challenges in this area that require legislative activity?
- What are the effective coercive measures in cybercrime cases?
- What are the specificities of electronic evidence and how should the rules for their preservation be regulated?
- Should new cybersecurity responsibilities be imposed on digital service providers, and should efforts be made to enhance end-user cyber awareness?
- Is the key to effectively countering cybercrime to correlate the scope of the services' operational and investigative powers with the level of technological development of ICT systems, software and services?

In order to verify main research hypothesis, the first step was to examine the definitions and systematisation of cybercrime. The research conducted by Ferenc Sántha in Chapter 1 indicates that the definition of cybercrime and the categorisation of criminal offences are of great importance for a number of reasons. From a legal perspective, a unified definition of cybercrimes can facilitate the harmonisation of national cybercrime legislation. Presently, there are notable discrepancies between European countries with regard to the categorisation of illicit acts perpetrated in cyberspace as criminal offences. Moreover, international cooperation in criminal matters and efforts to combat cybercrime may be more effective if national legislation governing cybercrime is based on

the same principles and if the designation and statutory definition of the crimes can be aligned and harmonised to the greatest extent possible. In conclusion, a unified definition of cybercrimes and the associated statistical methods and metrics will facilitate a more comprehensive understanding of the true scope of cyber-criminality and enable a more precise measurement of the crimes.

The main conclusion of the review of international, Hungarian (Ferenc Sántha) and Polish (Agnieszka Gryszczyńska) literature, is that there is no universally accepted definition of cybercrime. This fact has led to various definitions put forward by researchers and international organisations. The two-factor approach (dividing cybercrime into "cyber-dependent" and "cyber-enabled") is dominant in the academic literature. This may be because that this definition makes a simple but clear distinction between types of cybercrime. As Ferenc Sántha pointed out, the most popular definitions of cybercrime are those that refer to broader categorisations of cybercrime, namely typologies and taxonomies. Considering the scope, a taxonomy of cybercrimes based on the Budapest Convention and its First Additional Protocol is presented more broadly. The classification system of the Budapest Convention (and its First Additional Protocol) contains 13 different cybercrimes in five categories. The first category is *offences against the confidentiality, integrity and availability of computer data and systems*, including illegal access (Article 2), illegal interception (Article 3), data interference (Article 4), system interference (Article 5) and misuse of devices (Article 6). The second group is *computer-related offences*, which include computer-related forgery (Article 7) and computer-related fraud (Article 8); the third is *content-related offences* which in the Convention are offences related to child pornography (Article 9); the fourth is *offences related to infringements of copyright and related rights* (Article 10). Finally, under the Additional Protocol, the fifth category covers *acts of a racist and xenophobic nature committed through computer systems*, which include the dissemination of racist and xenophobic material through computer systems (Article 3), racism- and xenophobia-motivated threat (Article 4), racism- and xenophobia-motivated insult (Article 5), denial, gross minimisation, approval or justification of genocide

or crimes against humanity (Article 6). The Budapest Convention was also the basis for an analysis of the scope of criminalisation of cybercrime in Poland (Agnieszka Gryszczyńska) and Hungary (Ferenc Sántha).

The research presented in Chapter 2 on the scope of criminalisation of cybercrime in Poland indicates that in Poland, there is no legal definition of cybercrime or a statutory catalogue of acts deemed to be cybercrimes, while the criminal conducts that may be deemed cybercrimes is dispersed and, in addition to the Criminal Code, also includes administrative law regulations containing articles introducing criminal liability and defining the elements of the offences. With regard to the scope of criminalisation of cybercrime in Poland, Agnieszka Gryszczyńska points out that the work of the Council of Europe (Budapest Convention) and the EU (Directive 2013/40/EU) has had the greatest influence on the shape of criminal regulations in Poland. The criticised slowness of changes to criminal code provisions relating to cybercrime is in stark contrast to the speed of extra-code provisions resulting from ad hoc measures related to the increase in specific attacks or the exploration of gaps and vulnerabilities (e.g., CLI spoofing and smishing). In order to ensure regulatory consistency, it is advisable to limit the placement of criminal law provisions outside the Criminal Code.

The empirical research on the number of incidents and cybercrimes analysed in Chapter 2 shows a significant increase in the number of incidents and a growing number of cybercrime cases. A problem with the empirical research and the mapping of incidents onto a cybercrime taxonomy is the lack of a uniform classification for CSIRT teams and law enforcement agencies. The lack of a uniform and acceptable classification also hinders the cross-border exchange of information between CSIRT teams and law enforcement authorities as well as the research and analysis of the most serious threats. In order to increase knowledge on current threats, reliable data from multiple entities is necessary. Quantitative studies show that prosecutors are most likely to pursue cases involving fraud committed online. The grounds for criminalisation included in cyber-dependent crimes are not common grounds for registering cases at the prosecutor's office.

Apart from the critical remarks concerning the correct and consistent with the Convention on Cybercrime characterisation of the elements of individual cybercrimes in Poland, after the introduction of criminal liability for abuse of electronic communication, currently the scope of criminalisation of cybercrime in Poland does not need to be expanded. Definitely greater deficiencies are diagnosed in the procedural provisions. However, it should be mentioned that the scope of criminalisation of cybercrime in Poland may be influenced by the ongoing work of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes.

Finally, Agnieszka Gryszczyńska points out that the development of cybercrime leads to the need for constant evaluation and improvement of existing legal regulations, as changes in the threat landscape must be followed by changes in substantive and procedural law. Undoubtedly, another trigger for change will be the need to include criminal liability related to the use or abuse of disruptive technologies.

Research conducted in the area of money laundering by Judit Jacsó (Chapters 3 and 4) indicates that the development of the digital technologies had opened the door to new types and methods of criminal activity, which is true for the laundering of money as well. It is the reason that cybercrime and money laundering is one of the biggest challenges of our time. It should be stressed that money laundering is a constantly changing phenomenon. Hence, the combat against money laundering is a continuously developing area, which can be seen in the international, the EU and the domestic regulation as well. Cyber-laundering is a term that combines cybercrime and money laundering, representing the convergence of these two illicit activities, that is why the combat against it is a special challenge. However, the purpose of cyber-laundering is no different from the traditional form of money laundering, i.e., it aims to make it impossible to identify the origin of illegally acquired money derived from a crime.

New technologies create new methods for the commission of money laundering, which requires the legislators and the law

enforcement bodies to create and use new measures. Offenders increasingly use innovative technologies to launder criminal assets. The COVID-19 epidemic, the expansion of the new payment technologies and innovative payment system has given new power to the spread of cybercrime in parallel of money laundering. It is difficult to estimate the scale of money laundering, given the high latency rate for legalised amounts. The same can be established with regard to cyber-laundering.

One of the most important questions in connection with money laundering is the scope of the predicate offence. The fight against money laundering was initially similar to the fight against organised crime (including drug trafficking). But today the so-called all-crime approach became significant, which means that all criminal activity could be a predicate offence of money laundering. It means that the crimes in the field of cybercrime can also be a predicate offence of money laundering, if it results in financial advantage or assets.

Crypto assets should be given special attention as an object of money laundering. Crypto (currency) assets have expanded into practically every country and sector in the last decades. Cryptocurrency is being abused to commit new forms of crime and to launder the proceeds of crimes, however, the unique characteristics of blockchain-based technologies offer an unprecedented opportunity to investigate organised crime and money laundering networks and to recover the illicit asset. It is essential that crypto assets be treated as any other asset for the purposes of AML/CFT supervision and enforcement; likewise, it is important to bring the crypto assets (and service providers) into existing AML/CFT frameworks, and such laws should be broad enough to cover crypto assets and have the capacity to anticipate future evolutions in the crypto industry. In addition, the need for training, adequate communication and increased cooperation between public and private actors in the AML regime was also stated.

The cross-border nature of money laundering and of the cyber-laundering cases is also a significant factor that makes it difficult to combat these crimes and to identify perpetrators. In the fight against money laundering, the cooperation of several institutions is very important, both at the national and at the international

level. The dynamic change in money laundering methods requires regulatory authorities, including those in the European Union (EU), to constantly modify their regulations to effectively combat these illicit activities. It must be highlighted that the majority of cases in money laundering involve cross-border money-mule operations, where both the predicate offence and the transfer of proceeds occur in distant jurisdictions. International cooperation is crucial for these cases, but finding a legal basis for reaching countries on the other side of the globe can be challenging. This is where the multilateral conventions of the United Nations and the Council of Europe play a very important role by providing a legal framework for dialogue and mutual assistance in global money laundering cases.

Since 1991, the European Union has tried to create an effective and coherent framework against money laundering, which include five anti-money laundering directives that require Member States to prescribe the service providers many obligations, the most important of which are the identification of their customers (Know Your Customer, (KYC) and the Suspicious Transaction Reports (STRs)). It is important to emphasise that from the beginning, when formulating the obligations, the European Union regulation has been taking international standards into account, especially the Forty Recommendation of the Financial Action Task Force (FATF) and international conventions of United Nation and the Council of Europe. Several reports of international organisations and scientific studies pointed to the danger that the anti-money laundering (AML) regime, which was created to fight the traditional forms of money laundering, was not adequate against money laundering using virtual methods, thus it became necessary to modify them and extend their scope to virtual assets (VAs) and virtual assets providers (VASPs). An important and necessary first step in the necessary action against cyber-laundering was the creation of a regulatory framework in connection with crypto assets.

Research carried out by Judit Jacsó in the area of money laundering leads to the conclusion that it is essential for the national legislator, also for the Polish legislator, to continuously align domestic legislation with international and EU legislation, which is one of the keys for the effective action against money laundering.

Furthermore, another essential component of Poland's AML/CFT system is international co-operation, which is even more essential in cyber laundering cases. The inclusion of crypto-asset service providers in the system of preventive tools against money laundering helps to fight against money laundering (cyber-laundering). The legal framework for this must also be created by the Polish legislator by amending the relevant national regulation. With the new EU legal framework, every cryptocurrency-related business will adhere to the same AML/KYC rules as other financial service providers. In the digital age, the traditional strategy of "follow the money" could be supplemented by "follow the virtual asset" or "follow the crypto asset", which could contribute to the effective fight against the new form of money laundering: cyber-laundering.

Determining jurisdiction in cybercrime cases and instruments of international cooperation are essential for law enforcement and the judiciary. As Ferenc Sántha points out, until the mid-20th century, crime was largely a local matter, and the principles governing the exercise of criminal jurisdiction were based on the axiom that a crime was a phenomenon tied to a specific geographic area. Cybercrime has fundamentally changed the nature of crime, making it transnational and borderless. As Ferenc Sántha outlines in Chapter 5, traditional jurisdictional principles in domestic and international criminal law are unable to respond to the challenges posed by cybercrime, in particular positive jurisdictional conflicts. One potential solution to the aforementioned challenges is the creation of a global international treaty that would regulate jurisdictional issues and establish a framework for addressing conflicts of jurisdiction. In addition, it should be emphasised that the successful determination of the state that has de facto jurisdiction over the case is only the first step towards holding the offender accountable, as jurisdiction can only be effectively exercised and proceedings conducted if the offender is accessible to the authorities of the state that has jurisdiction. Otherwise, the institution of international or European mutual legal assistance in criminal matters should be used.

In Chapter 6, Piotr Burczaniuk examines the pre-trial activities directed at acquiring information, relevant from the perspective of criminal law enforcement agencies, to carry out activities

in identifying and detecting cybercrimes and prosecuting their perpetrators. These considerations focus on two key types of these activities: first, security activities related to the functioning of the European and national cybersecurity system, and second, operational and reconnaissance activities authorised by national services in the context of the possibility and scope of their use to combat cybercrime. A complementary element of these considerations was the analysis of international cooperation in the two areas indicated. The main objective of the research presented in Chapter 6 was to answer the question of whether the scope of action and international cooperation of entities responsible for cyber-security and law enforcement agencies conducting reconnaissance activities is sufficient, given the nature of current types of cyber-crimes, and to identify the most significant challenges in this area requiring legislative activity.

Referring to the first of the analysed areas, Piotr Burczaniuk pointed out that the cybersecurity system, based on prevention, detection and response to various types of cyber threats, plays a key role in the combat against cybercrime. This role is outlined in two key aspects: first, when the cybersecurity system supports the process of identifying and prosecuting cyber criminals and second, when it neutralises opportunities for perpetrators by eliminating system vulnerabilities previously identified in specific criminal activities. The directions of cyber security policy changes indicated in the chapter, focusing on the role and importance of the user of an ITC system, and thus also on the potential victim or perpetrator of a crime, lead to the conclusion of an even greater need for rapprochement between cybersecurity and countering cybercrime. However, it should be kept in mind that this rapprochement may face significant legal and practical problems. The most significant of these seem to be related to the different outlook of both regulators and the main participants in both aspects on privacy and data protection issues. The second aspect is the concern about the use of various modern technologies, such as facial recognition systems, the monitoring of online behaviour, and artificial intelligence algorithms, among others, which, on the one hand, may have a high level of effectiveness in the fight against cybercriminals, but on the other hand, the mechanism of their operation is based on the collection

and aggregation of large amounts of personal data. Also worth noting is the challenge of the lack of consistency and harmonisation between different countries and regions in the regulation of both cybersecurity and fighting cybercrime. Many companies operate globally, in multiple markets, and face the need to comply with different standards and regulations, which can lead to complex and costly compliance processes and often, in situations of apparent contradiction, lack of implementation.

Summarising the second of the analysed areas in Chapter 6, it should be pointed out that undoubtedly the most important and effective tool in the hands of law enforcement agencies remains operational control, particularly in the scope involving the so-called electronic surveillance. This is because the detection and prosecution of many types of cybercrimes is only possible thanks to the ability of authorised services to conduct monitoring of the means of electronic communication, of content delivered electronically or, finally, electronic data itself. These activities may include various levels of "depth" of interference in civil rights and freedoms, including in particular the secrecy of correspondence, ranging from the analysis of instant messaging, messages transmitted by e-mail, or in Internet chats, to the study of user activity on social media platforms or information on websites visited by the user. However, it should be added that the effective application of this activity, mainly due to technological developments, faces numerous difficulties. It should be noted, however, that a fundamental political and legal debate is currently underway around this activity, specifically the scope of telecommunications data collected by providers, at both the European Union and national levels. Moreover, retention obligations are at this date not imposed on electronic services providers (e.g., providers of e-mail and instant messaging services), which creates a significant information gap in this regard. Changes in this regard were proposed by the Polish legislator in the draft Law on Electronic Communications, which met with a negative opinion from both public administration bodies and publicists and representatives of social organisations.

Research on international cooperation between services indicates an overabundance of organisations responsible for cyber-security

and countering cybercrime. This leads to both information chaos and coordination deficiencies, both at the level of the organisations themselves and at the level of individual member states. In addition, these organisations are still equipped only with soft tools, both in terms of information acquisition and threat response, which ultimately translates into their often insufficient effectiveness. Research presented in Chapter 6 leads to the conclusion of the need for consolidation at both the legislative and operational level. At the level of European and national legislation, a kind of demarcation is noticeable, separating prevention activities (the domain of cybersecurity) from activities directed at combating threats, and from procedural activities strictly related to the combat against cybercrime. This boundary translates directly into the tasks and powers granted in each area to the services and entities responsible for them. In turn, with respect to them, there is a distinct lack of clearly defined coordination rules and cooperation mechanisms. The comprehensive outlook should be adopted by both European and national legislators, in the numerous currently underway normative acts aimed at raising the level of cybersecurity.

In Chapter 7, Erika Róth undertakes an analysis of the application of coercive measures in cybercrime cases. She points out that a delicate balance need prevail in criminal proceedings. On one side of the scale is the interest in the effectiveness of criminal proceedings, while on the other side are the rights of the participants in the proceedings. And while the principles of coercive measures in Hungarian law do not differ depending on whether they are applied in cybercrime cases or in other criminal cases, several features specific to cybercrime can be identified in the case of coercive measures affecting property, in particular with regard to the search, seizure and rendering of electronic data temporarily inaccessible. An interesting legislative solution in Hungary, analysed by Erika Róth, is the rendering of electronic data temporarily inaccessible which may be ordered where a proceeding is conducted regarding a criminal offence subject to public prosecution, and in connection with which the rendering of electronic data permanently inaccessible may be ordered when so doing is necessary to interrupt the criminal offence. Rendering electronic data temporarily inaccessible restricts

the right to dispose of data published via an electronic communications network. It may be ordered in the form of temporarily removing the electronic data concerned, or temporarily preventing access to the electronic data concerned. The enforcement of this coercive measure is organised and controlled by the National Media and Communications Authority. In addition, the Hungarian legislator also created the possibility for the prosecutor or the investigating authority to call on the service provider capable of preventing access to electronic data to voluntarily remove electronic data, provided that this doesn't harm the interests of the criminal proceeding. The purpose of this provision is to ensure that the content that violates criminal law is only available for the shortest possible time. The Hungarian regulation also regulates searches (including of the information system) and seizures of electronic data more broadly and in greater detail. It indicates in particular the methods by which electronic data, including electronic data used for payments, may be seized. The seizure of electronic data used for payment can also be carried out by performing an operation on the electronic data that prevents the person concerned from disposing of material (property) value expressed by the electronic data. According to the current rules of criminal procedure in Hungary, the Bitcoin to be seized is transferred from the owners address to the address of the authority.

In conclusion, Erika Róth pointed out that although certain coercive measures affecting assets (e.g., search, seizure) are of paramount importance in the case of cybercrimes, it should not be forgotten that other coercive measures can also play a role in ensuring the effectiveness of evidence or preventing re-offending (e.g., pre-trial detention, criminal supervision or restraining order).

In Chapter 8, Erika Róth analyses the principles of electronic evidence preservation. The rules resulting from the Hungarian Code of Criminal Procedure seem to be more detailed and comprehensive. In Poland, there are no special rules governing the preservation of electronic evidence, and the application to it by analogy of the rules relating to physical evidence is sometimes questionable. The HCCP provides a list of the means of evidence and evidentiary acts. Electronic data was also recognised as one of the means of evidence

in Hungary. As Erika Róth points out in her summary of the research, lack of regulation or insufficient regulation of the preservation of electronic evidence may even result in inadmissibility of evidence. In order to avoid such law enforcement actions that result in inadmissibility of evidence and consequently render prosecution ineffective, the legislator must monitor law enforcement practice and respond to problems that can be solved by legislation. The legislature should also be sensitive to amendment proposals formulated by the scientific community that recognise regulatory deficiencies or loopholes. Moreover, the legislator should pay attention to international expectations, which means more than compliance with EU requirements only.

In Chapter 9, "Data Retention and Legal Problems of Investigating Cybercrime", Rafał Wielki draws attention to the problem of storing and processing data held by operators of ICT services. While there used to be EU regulations that facilitated a uniform understanding of the problems (Directive 2006/24/EC of the European Parliament and the Council), their legality has been challenged by the Court of Justice of the European Union, with the result that today there is no legal act that defines what type of data can be processed by ISPs, how long it can be stored, and on what basis law enforcement agencies can use it. By failing to cooperate with law enforcement agencies in sharing traffic data on suspected users, online platforms are essentially making it easier for cybercriminals to go unpunished. Despite the introduction of a number of laws that indirectly address the retention of telecommunications data, email data, etc., there is still a lack of legislation that regulates this issue directly. The regulations in force in individual EU countries are not uniform, which does not serve to promote the exchange of information crucial in the fight against cross-border cybercrime. It seems high time to raise the need for renewed discussions among member states on creating a piece of legislation that would frame and address civil liberties on the one hand, and the needs of investigators who need access to data on the other.

An analysis of the perpetrators' modus operandi carried out by Rafał Wielki allows conclusions to be drawn regarding effective methods of fighting cybercrime that use information analysis tools (Chapter 10). By understanding the characteristics of cybercrimes, it is possible to understand the motivations of the perpetrators, their

modus operandi, and the tools used to commit criminal acts. Among the *de lege ferenda* proposals, it is suggested that international cooperation in the prosecution of cybercrimes be tightened in general, and that as many procedures as possible be regulated in a similar manner, so that laws are not mutually exclusive in different countries. Nowadays, criminals are turning more often to instant messaging to communicate with each other, while at the same time the tools of classic communication via telephone network (SMS, voice calls) are gradually being consigned to oblivion. This fact poses a very serious challenge in the form of the lack of access to network traffic data of suspected users, as currently the retention of data collected by social media and instant messaging is regulated neither by national law nor by international law. This demonstrates the need for uniform regulations to facilitate cooperation with social media operators as processors of personal data and user activity information. Among the legal and technical challenges, attention should also be paid to the impact of disruptive technologies, i.e., the impact of quantum computing on encryption methods and the use of artificial intelligence by perpetrators of crime. Given the increasing technical advancement of the perpetrators using encryption tools, anonymisation of network traffic and sophisticated money laundering methods, it is of fundamental importance that law enforcement agencies are also equipped with tools allowing them to effectively conduct criminal proceedings. As indicated in many chapters of the monograph, the rapid acquisition and analysis of electronic data and the preservation of evidence are important for the effectiveness of criminal proceedings in cybercrime cases. This process is significantly influenced by the availability of modern technology and work-supporting IT systems in the police and in the prosecutor's office.

We believe that the monograph will have a positive impact on setting the direction of legislative work aimed at countering cybercrime and protecting users of digital services from cybercriminals. Since cybercrime issues are a very popular research topic, the introduction to the Polish and Hungarian legal background and law enforcement practice will provide an essential source for researchers as well.

Agnieszka Gryszczyńska