Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 17(66) Special Issue – 2024
https://doi.org/10.31926/but.ssl.2024.17.66.3.9

CYBER THREATS IN THE EUROPEAN SPACE. SECURITY MEASURES AT THE LEVEL OF THE EUROPEAN UNION

Carmina TOLBARU[1]

Abstract: *Cybercrime is taking on new global dimensions, with more and more criminals turning to technological services and tools both to plan and to commit crimes. Electronic evidence is becoming vital to crime fighting, both in tracking and convicting criminals. Such digital data that is used for the investigation and prosecution of crimes can be used to identify a person or to obtain more information about his activities. In light of the fact that evidence of any crime is increasingly stored in electronic form, there is a need to protect society and individuals against crime not only offline, but also online, including through effective investigations and prosecutions.*

Key words: *cybercrime, electronic evidence, investigation, prosecution of crimes, crime fighting.*

1. Introduction

The widely use of the computer and of the internet represented over time the foundation of cybercrime. Thus, at present, computer is used to promote illegal goals, such as committing frauds, traffic of child pornography and intellectual property, theft of identities or violation of private life. Therefore, cybercrime, especially by means of internet, has developed rapidly, becoming a real octopus whose tentacles are deeply rooted in all areas of economic and social life.

The evolution of technology created new criminal opportunities, without understanding by this that new offences have occurred. The offences could have been committed even before the occurrence of internet, as a criminal does not necessarily need a computer to commit frauds, traffic of child pornography or intellectual property, theft of identities or violation of somebody`s private life. Practically, cybercrime by means of internet is an extension of the criminal behaviour as part of some new illegal activities.

Similar to the offences committed in the physical environment, when the criminals leave physical traces, the same happens in the digital environment, the cybercriminals

[1] National University of Science and Technology Politehnica Bucharest, Pitești University Centre, Romania, carmina.tolbaru@upb.ro.

leave clues regarding their identity and location, even though the internet provides criminals a certain anonymity and they have the possibility to hide better than in real world. In this regard, the problem is especially in the context of pursuing such criminals beyond the borders, considering the non-local character of cybercrime. Illegal actions can involve separate jurisdictions which can create serious problems with regard to the enforcement of the law. That is why, international cooperation in criminal matter is essential in preventing and fighting this type of crime.

At the level of the European Union, when considering the rapid growth of the cyberthreats, including against the background of regional conflicts which continue to be an important aspect regarding cybersecurity, efforts are being made to issue new regulations to increase the access to the digital data used in criminal investigation and prosecution of offences, regardless of their location.

2. The Cyberspace and its Challenges. Preliminary Issues

At present, the whole world is connected to the electronic technology and this interconnectivity of the global society allows criminals to operate in different jurisdictions, elements of their crimes being widely spread around the world in time and space (Herrera-Flanigan & Ghosh, 2011, 265-308).

The interaction with cyberspace has put us in front of some new security challenges, as many of the economic, commercial, cultural, social and governmental activities and interactions are carried out in this area, which makes that data protection against cyberattacks be a difficult problem (Aghajani & Ghadimi, 2018, 218-225).

Cybercrime includes a wide spectrum of crime-related activities and this can be seen in the different manifestations that could take place (Dennis, 2024, 203-218):

- offences involving *fundamental breaches of private or corporate confidentiality*, such as attacks on the integrity of digital information and the use of such information to harass, hurt or blackmail a company or a person; the theft of identity is also included in this area;
- offences *based on transactions*, such as fraud, traffic of child pornography, digital piracy, money laundry and counterfeiting; some victims are targeted. Sometimes, there are involved individuals within corporations or governmental bureaucracies in order to obtain profit or for political goals.
- offences involving attempts to disrupt the real functioning of internet. They vary from spam, hacking and denial of service attacks against some websites, to acts of cyber terrorism.

Therefore, cyber crimes includes computer viruses, data violations, denial of service attacks (DDoS), and also other attack vectors, whose actors can be both trusted users and unknown persons, situated in remote locations. Anonymity, uncertainty of the threatening geographic area, dramatic impact and lack of public transparency are likely to facilitate the pathway to the most serious threats: cyber war, cybercrime, cyber terrorism and cyber intelligence (Niraja and Srinivasa Rao, 2021).

The problem is massive, Europol offering a thorough analysis of the most recent threats of cybercrime affecting the European Union (EU). Thus, pursuant to the latest

Internet Organised Crime Threat Assessment (IOCTA), cybercrime becomes more and more aggressive and confrontational regarding the volume, intensity and potentially harming (IOCTA, 2024, 6).

3. Types of Cyberthreats

Cyberthreats or cyber security threats are malicious intentioned acts towards digital life in general, whose goal is getting non-authorised access, disturbing, disrupting or data theft, respectively the theft of an asset of technology of information, computer network, intellectual property or any other form of sensitive data.

Cybercrime can have different forms, many common offences being cyber-facilitated. Taking advantage of internet addiction in the daily life of individuals, criminals use this "technological innovation" for communication and collection of information, which facilitates a series of traditional criminal activities. Broadly, illegal activities included in this area can target:

- getting the control over the private devices with the help of malware applications;
- theft or compromising personal data and intellectual property in order to commit online frauds;
- use of internet and of social media platforms in order to share illegal contents;
- use of "darknet" in order to sell illegal goods and hacking services.

The area of cyberattacks includes a wide spectrum of illegal activities that become more and more complex and hard to track, which put the law enforcement authorities in difficulty, they already facing a lack of capacity and of proper resources to treat such types of manifestations (Widhaningroem and Widowaty, 2024, 287-300). The factual reality shows us that these increased rapidly starting with the latter half of year 2023 and continuing with the former half of year 2024. The European Union Agency for cybersecurity (ENISA), responsible with reaching a high common level of cybersecurity in the entire Europe, identified seven main threats to cybersecurity.

First, there are the threats to availability, followed by ransomware and threats to data. Phishing is considered as the most common initial vector of such attacks. These threats can be broadly classified in several types, each of them with unique features and methodologies (ENISA, 2024, 6-8):

- Ransomware – is one of the main threats to cyber security, consisting in encrypting the victim`s data and requesting payment for decrypting codes; malware attacks contain computer viruses or worms, trojans and are likely to infect the systems in different ways, most often through ill-intentioned links or by email (Gupta, 2013).
- Malware – is a malicious code and malicious logic, is used to describe any software or firmware intended to perform an unauthorised process that will have a negative impact on the confidentiality, integrity or availability of a system.
- Social Engineering – refers to a series of activities of manipulation by which they are trying to exploit the human error or the human behaviour, in order to get access to sensitive or secret information or services: phishing, spear-phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps

and scareware; among them, phishing is one of the most common forms of tricks by means of which users disclose sensitive data.

- Threats against data – can target both data breaches, and data leaks. Data breaching is a deliberate cyberattack in order to get unauthorised access and to issue sensitive, confidential and protected data; therefore, in order to steal data. Data leaking involves the loss or unintentional exposure of some sensitive and confidential objects or protected data, as a result of a wrong configuration, of a vulnerability or even of a human error.
- Threats against availability: Denial of Service – targets the availability of the system or of the data by compromising their functioning. The attacks occur when the system or service users cannot access data, services or other relevant resources, by running out the service or its resources or by overloading the components of the network infrastructure.
- Information manipulation and interference – is a form of cyberattack which does not steal data, but proposes to change the data to impede the functioning of an organisation. Such an activity has a manipulative character, carried out in an intentional and coordinated manner.
- Supply chain attacks – as a result of digital and electronic technologies in the supply chain, in each aspect of its end-to-end process, the use of such technologies also significantly opened different security threats and risks, which widened the surface of attack in the whole end-to-end supply chain (Hammi et. al, 2023, 1-40). The supply chain attacks compromise the software and the hardware before reaching the consumer, by exploiting the relationship of trust.

4. The Importance of Electronic Evidence in Matters of Prosecution and Conviction of Criminals

Considering the fact that more and more criminals use technology to plan and commit a wide range of offences, electronic evidence is vital for authorities in the judicial procedures regarding the prosecution and conviction of criminals. By their nature, these devices allow leaving traces associated with crime, as they store, transmit or process a lot of data on users, data that are integrated to email accounts, cloud-based services, social media platforms and synchronised desktop applications (Blažič & Klobučar, 2019, 66-81).

Getting electronic evidence by means of judicial cooperation channels often needs a long period of time, which makes some clues to disappear, considering the volatile character of electronic evidence. There are many obstacles in the efficient fight against cybercrime due to inconsistent understanding regarding the cross-border search of electronic evidence, the legality of the data sought and the rules of cooperation with communication service providers (Blažič & Klobučar, 2019, 66-81).

By electronic evidence or e-evidence, we understand those digital data that are used for the criminal investigation and prosecution of criminals, i.e.: emails, text messages or contents from messenger applications, audio-visual contents, information on the online account of a user.

Tere are two types of electronic evidence:

- data stored in computer systems or devices;
- information transmitted electronically through communication networks.

Such data can be used to identify a person or to get more information about his/her activity, having 85% relevance in all criminal EU investigations. IP addresses, for example, as well as the related access numbers and information, can be an essential starting point for criminal investigations where the identity of a suspect is not known, thus serving to establishing his/her profile.

In order to carry out a specific criminal investigation, the law enforcement authorities might need to request an IP address, as well as access numbers and related information, in order to identify the user or to get more intrusive information on his/her private life, such as contact data and the location of the user.

The cross-border character of computer networks and the fact that network services can be provided from anywhere and do not require a physical infrastructure, raise serious jurisdictional issues regarding the access to electronic evidence (Arnell & Faturoti, 2023, 29-51). Most of the times, the relevant problems are found stored on servers located in another state than the one in which the offence was committed or where the investigation is carried out. That is why collection of such electronic evidence by authorities can be difficult and the process itself can be complex and long. Against this background, it is necessary to provide specific regulations regarding the cross-border judicial cooperation to preserve and disclose the electronic evidence, regulations that should approach the specific nature of electronic evidence.

As more than half of the criminal investigations include a cross-border request to access the electronic evidence, even since 2018 there has been requests on behalf of the European Council and of the Council, to the European Commission, i.e. to make the access of authorities to electronic evidence more efficient, regardless of their location, and that is why the Commission proposed new rules in this regard. Therefore, this allowed the judicial authorities from an EU country to request direct access to electronic evidence to any service provider who offers services within the European Union and is established or represented in another Member State.

The lack of a harmonized framework of cooperation with the service providers determined the need for regulation through two legislative acts subject to evaluation at present, to be enforced starting with 18 August 2026 (Regulation) and 18 February 2026 (Directive):

- a Regulation on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (Regulation (EU) 2023/1543); thus, the national judicial authorities involved in criminal procedures will have the possibility to order the service providers offering services within the European Union (EU) to produce and preserve electronic evidence anywhere the data is; also, the regulation aims at facilitating even more rapidly the cross-border access to electronic evidence and to prevent their erasure, at the same time ensuring judicial guarantees for the persons whose data is searched.
- a directive laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of

gathering electronic evidence in criminal proceedings (Directive (EU) 2023/1544). Thus, the Directive imposes to some service providers offering services within the EU to have designated establishments or designated legal representatives in the EU, so that they can receive and obey orders from the national authorities in order to gather electronic evidence within the criminal procedures.

In this regard, the new regulations concretely target:

- creation of an *European disclosure order* that should allow a judicial authority from a Member State to get electronic evidence directly from a service provider or its legal representative into another Member State (such as emails, text messages or messages in applications, as well as data to identify an offender); it will have the obligation to answer within 10 days or, in case of emergency, for example an imminent threat to life, physical integrity or safety of a person, within 8 hours. An European disclosure order for electronic evidence should be necessary and proportionate for the purpose of the procedures mentioned in article 2 para.3 of the Regulation.

- creation of an *European preservation order* that should allow a judicial authority from a Member State to request that a service provider or its legal representative from another Member State to preserve specific data for a subsequent request to produce such data in the mutual judicial assistance base, an Investigation order or an European production order.

For the criminal procedures, the European disclosure order of electronic evidence and the European preservation order of electronic evidence, should be issued only within some specific criminal procedures regarding an actual offence that has already taken place, following an individual evaluation of the need and proportionality of such orders in each case, considering the suspect`s or the defendant`s rights. Also, within the provisions of this regulation, there are also the procedures initiated by an issuing authority for the localisation of a convicted person that escaped justice, in order to execute a prison sentence or a detention measure as a result of some criminal procedures.

- ensure some *strong guarantees* of the fundamental human rights and liberties, regarding getting such data – we especially mention the right to personal data protection, as, from all the categories of data mentioned in the Regulation, - data relating to subscribers, traffic data and contents data – they contain personal data that should benefit from full protection pursuant to the European Union acquis. The persons whose data are searched will benefit from different guarantees and will also have the right to an appeal. We also mention rights and principles, such as the right to freedom and to safety, respect for the private and family life, the right to an effective way of appeal and to a fair trial, presumption of innocence and right to defence, the principles of lawfulness and proportionality, as well as the right not to be judged or convicted twice for the same offence. The respect for private and family life, and protection of physical persons regarding personal data processing, are fundamental human rights. In accordance with article 7 and article 8 para.1 from the Charter, any person has the right to respect for his private and family life, his home and his communication, and to protection of personal data regarding such person. In order to stand guarantee for the full respect of the human rights, the evidentiary value of the evidence obtained in the application of this regulation should be evaluated within the trial by the competent judicial authority, pursuant to the domestic law and to the respect of the right to a fair trial and the right to defence (Regulation (EU) 1543, Official Journal of the European Union, L 191, 2023, 120*).*

By electronic evidence pursuant to the Regulation, we should understand "data relating to subscribers, traffic data or contents data stored by a service provider or in his name, in electronic form". Thus:

- "data relating to subscribers" means any data owned by a service provider related to the subscription to his services; data relating to subscribers and IP addresses, access numbers and related information, when the data is requested exclusively to identify the user, can offer the first clues regarding the identity of a suspect within an investigation;
- "data requested exclusively to identify the user" means IP addresses and, if any, the source ports and the relevant temporal mark, i.e. date and time or the technical equivalents of the respective identifiers and the related information;
- "traffic data" means the data related to the provision of a service, such as the origin and destination of a message or of any other type of interaction, the position of the device, date, time, duration, size, route, format, and also other metadata regarding the electronic communications and data related to the beginning and end of an access session of the user, such as date and time of usage, connection to service and disconnection from it;
- "contents data" mans any digital data, such as written messages, vocal messages, video recordings, images and sounds, other than the data regarding the subscribers or traffic data.

Their relevance in the criminal investigations is unquestionable, but the data related to traffic and to contents are the most relevant.

5. Conclusions

Cyberattacks, of all kinds, are constantly growing, which requires the need for an effective plan of cyber security. So, there is a need for active security measures, to be included in sound and sustainable strategies with specific IT tools. Authorities should rely more and more on electronic evidence in order to identify offenders and to convict them, and in this regard the detection, investigation and disturbance are the main activities that should be carried out within the context of the current offence-related manifestations and of the future challenges to be seen in the cybercrime environment. Bigger efforts are necessary to increase the capacity of law enforcement and also a direct cooperation between authorities and e-commerce platforms, remaining to be seen to what extent the new regulations contained in the European legislative framework offer an effective answer to the crisis of social reality.

References

Aghajani, G. & Ghadimi, N. (2018). Multi-objective energy management in a micro-grid*. Energy Reports,* 4, 218-225*.* https://doi.org/10.1016/j.egyr.2017.10.002.

Arnell, P. & Faturoti, B. (2023). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology*, 37(1), 29–51. https://doi.org/10.1080/ 13600869.2022.2061888.

Dennis, M.A. (2024)*.* Cybercrime. *Encyclopedia Britannica,* 203-218. Retrieved from *TOCTA Report 2010_low res.pdf (unodc.org).*

Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. *Official Journal of the European Union, L 191/28.7.2023*, 181-190.

European Union Agency for Cybersecurity. (2024). *ENISA Threat Landscape 2024*. DOI: 10.2824/0710888. Retrieved from ENISA Threat Landscape 2024 — ENISA (europa.eu).

European Union Agency for Law Enforcement Cooperation. (2024). Internet Organised Crime Threat Assessment (IOCTA). doi:10.2813/442713. Retrieved from Internet Organised Crime Threat Assessment IOCTA 2024.pdf (europa.eu).

Gupta, S. (2013). Types of malware and its analysis. *International Journal of Scientific & Engineering Research,* 4(1). Retrieved from Types-of-Malware-and-its-Analysis.pdf (ijser.org).

Hammi, B., Zeadalli, S. & Nebhen, J. (2023). Security Threats, Countermeasures and Challenges of Digital Supply Chains. *ACM Computing Surveys,* 55(14s), 1-40. https://doi.org/10.1145/3588999.

Herrera-Flanigan, J.R. & Ghosh, S. (2011). Criminal Regulations. In: Ghosh, S., Turrini, E. (eds)., *Cybercrimes: A Multidisciplinary Analysis*, (pp. 204-211). Heidelberg: Springer.

Niraja, K.S. & Srinivasa Rao, S. (2021). *A hybrid algorithm design for near real time detection cyberattacks from compromised devices to enhance IoT security.* Science Direct. https://doi.org/10.1016/j.matpr.2021.01.751.

Regulation (EU) 2023/1543 on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. *Official Journal of the European Union, L 191/ 28.7.2023*, 118-180. Retrieved from http://data.europa.eu/eli/reg/2023/1543/oj.

Widhaningroem, S. & Widowaty, Y. (2024). Digital Evidence Tracing in the Investigation of Identity Theft inthe E-Commerce Era. *Formosa Journal of Social Sciences (FJSS),* 3(2), 287-300. doi*: 10.55927/fjss.v3i2.9797.*

Other information may be obtained from the address: carmina.tolbaru@upb.ro