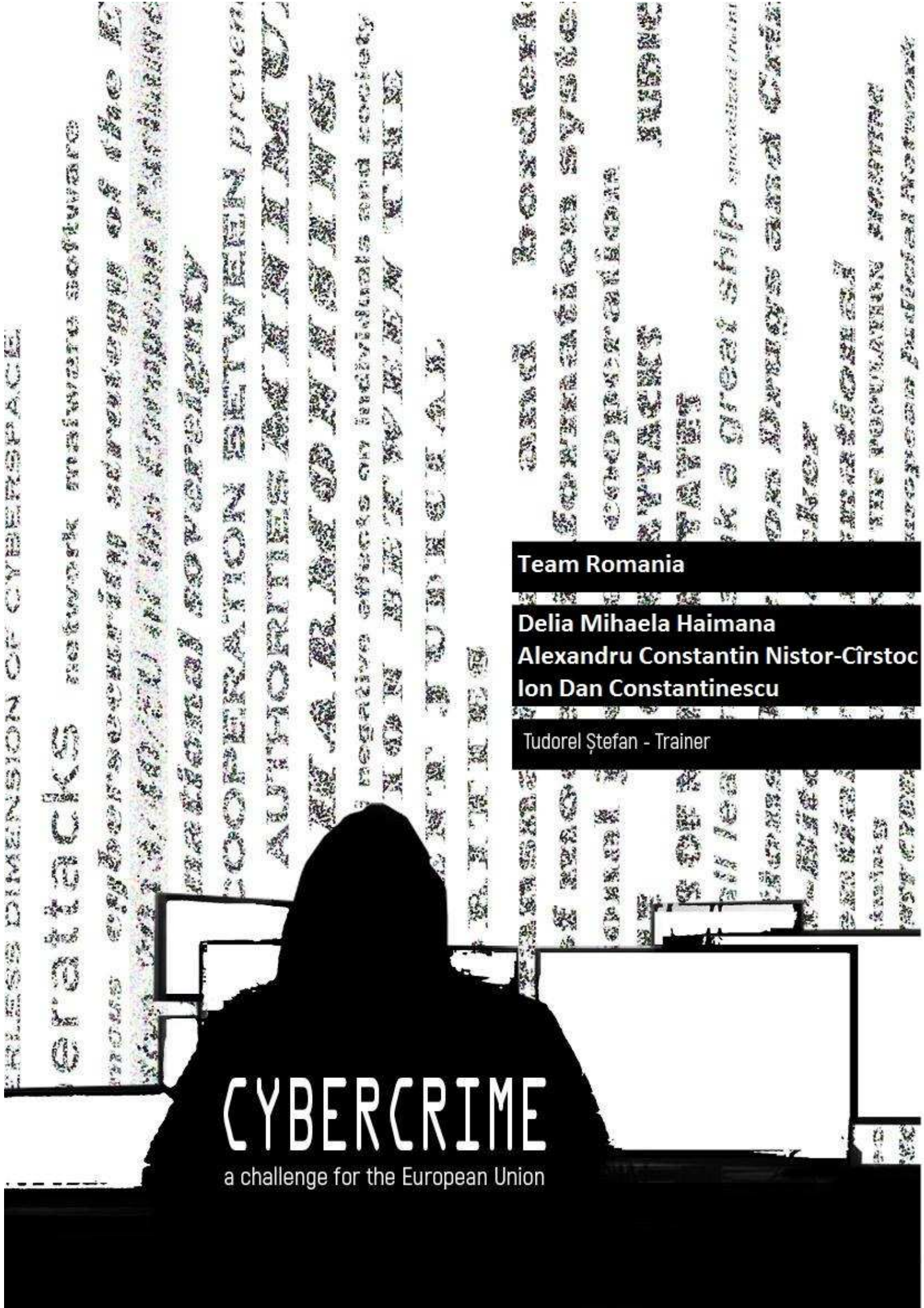

CYBERCRIME

a challenge for the European Union

Team Romania

Delia Mihaela Haimana
Alexandru Constantin Nistor-Cîrstoc
Ion Dan Constantinescu

Tudorel Ștefan - Trainer

Cybercrime: a challenge for the European Union

1. Introduction

As we move towards a digitalized world, the European Union (EU) recognized that this huge leap for humanity needs the same attention as the internal single market that has been the main focus of the EU for more than half a century[1]. With that in mind, one has to realize that new challenges will arise, not only regarding the judicial regulation of the cyberspace, but also in assuring the safety of individuals and any other user on the internet.

Cybercrime, or computer-oriented crime, is a crime that involves a computer and a data network either as a primary tool or as a primary target. Although there is no single universal definition of cybercrime, law enforcement generally makes a distinction between two main types of internet-related crime: on the one hand there is advanced cybercrime (or high-tech crime) representing sophisticated attacks against computer hardware and software (e.g. attacks against information systems, denial of service and malware) and on the other hand there is cyber-enabled crime representing many traditional crimes which have taken a new turn with the advent of the internet, such as crimes against children, financial crimes and even terrorism[2].

Cyberattacks can take many forms, and they are evolving and developing day by day, making us think that it is almost impossible to keep up and to upgrade our security measures at the same rate. Some of the most frequent types of attacks are related to DDoS, ransomware and malware.

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.

Malware represents a software which is specifically designed to disrupt, damage, or gain authorized access to a computer system[3].

---

[1] "The EU will prioritise international security issues in cyberspace in its international engagements, while also ensuring that cybersecurity does not become a pretext for market protection and the limitation of fundamental rights and freedoms, including the freedom of expression and access to information. A comprehensive approach to cybersecurity requires respect for human rights, and the EU will continue to uphold its core values globally, building on the EU's Human Rights Guidelines on online freedom. In that regard the EU emphasises the importance of all stakeholders' involvement in the governance of the internet." http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450, accessed on 19.03.2018.

[2] https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime, accessed on 24.03.2018.

[3] A malware software was recently used by Russian hackers in order to get access to 32 ATMs of a Romanian bank and to steal 860,000 Euros in just a few seconds, https://malwaretips.com/threads/russian-

The importance of cyber-security has been underlined by the EU in recent times[4], and in light of some recent events one could say that it is not just a problem that affects ordinary citizens, but it can also happen to the best of us[5].

A simple look at the recent activity of the EU regarding the cyberspace, can easily show that this has been a major concern in the last half a decade; in 2013, there was released a joint communication about the cybersecurity strategy of the EU, which established the intentions that the Union has in this area, and also the principles for cybersecurity[6].

In the next chapter we will analyse the Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems (Directive 2013/40). The main reason why we chose this particular piece of legislation is the fact that it offers a general view to the problem of cybercrime and it is an important step taken by the EU towards creating security in cyberspace.

2. The Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems

According to Article 83 Paragraph 1 of the Treaty on the Functioning of the EU[7], the EU has shared competence with Member States in the area of criminal cooperation.

Thus, the objective of the EU cybercrime Directive 2013/40 is to counter cybercrime and to promote information security through stronger national laws, more severe criminal penalties and greater cooperation between relevant authorities[8].

---

hackers-stole-860-000-euros-from-32-atms-belonging-to-the-raiffeisen-romania-in-just-one-nig.80595/, accessed on 24 March 2018.

[4] COM (2017) 354 final, Brussels, 29.6.2017, C (2017) 6100 final, Bruxelles, 13.9.2017, JOIN (2017) 450 final, Bruxelles, 13.9.2017.

[5] https://www.securityweek.com/czech-leader-says-computer-hacked-child-porn, accessed on 18.03.2018.

[6] "For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace. Our freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace. Governments have several tasks: to safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading role." http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001, accessed on 08.03.2018.

[7] "The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime."

The Directive 2013/40 comprises minimum rules harmonising the definition of criminal offences and sanctions related to the field of attacks against information systems. On the other hand, the Directive 2013/40 focuses on prevention, through strategies and measures aiming to reduce the risk of committing such criminal offences and also to attenuate the potential negative effects on individuals and society.

This European legal instrument provides the approximation of criminal law systems between the Member States and the development of the cooperation between the competent judicial authorities, with respect to the following criminal acts: illegal access to information systems, illegal system interference, illegal data interference and illegal interception.

Directive 2013/40 does not impose criminal liability when the objective criteria of the criminal offences provided by this legal instrument are fulfilled and the perpetrator did not have any criminal intent to commit the incriminated act. Such situations may occur, for example, when a person does not know that the access was unauthorised or when a company mandates a person to test the strength of its security system.

In order to effectively combat these criminal offences, it is necessary to ensure that the same offences are criminalised in all Member States.

Another key point in fighting cybercrime is the international judicial cooperation, including operational national points of contact. The EU cybercrime directive underlines the importance of networks, such as the G7 or the Council of Europe's network of points of contact available on a 24 hour, seven-day-a-week basis. Consequently, the Directive 2013/40 establishes the obligation of the Member States to have such contact points, even if some of these States are not part in the above-mentioned networks. The points of contact should be equipped to provide assistance and should have the capacity to communicate with the points of contact from other Member States promptly, with the support, *inter alia*, of trained personnel.

It is also recommended that the requested points of contact should provide an answer to the urgent requests of another Member State within eight hours of receiving of the request.

The EU dedication to cooperation in this matter is highlighted by the first article of the Directive 2013/40 which provides that it aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities.

[8] http://eur-lex.europa.eu/summary/EN/l33193, accessed on 07.03.2018.

As far as the terms contained by the Directive 2013/40 are concerned, they are defined in Article 2 thereof, the first two ("information system" and "computer data" respectively) having very technical definitions.

Articles 3 to 8 of the Directive 2013/40 identify dangerous conduct as far as information systems are concerned against which Member States should take action. With regard to these dangerous behaviours, it should be pointed out that this directive not only does it name those criminal offences that Member States should criminalize but also defines those offences, showing what specific behaviour should be incriminated by the Member States.

The directive then sets minimum limits on the penalties that should sanction attacks against information systems as well as the situations in which the conducts referred to in Articles 3 to 8 become very serious and therefore should be penalized more severely.

Another important provision of the Directive 2013/40, taken from Framework Decision 2005/222/JHA on attacks against information systems[9], is that referring to legal persons.

A legal person will be held accountable for any of the offences provided by Articles 3 to 8 as long as it has been committed for its benefit by a natural person having a leading position within it as well as the power to represent that legal person. The Directive 2013/40 also penalizes legal persons if a natural person under their control has committed a crime against information systems if the offence has been committed because of the lack of control of the legal person.

However, the liability of the legal person will not exclude the liability of the natural person who is guilty of an attack against an information system.

With regard to the sanctions that may be imposed on a legal person, they start from the interdiction to receive public funds and may go as far as capital punishment for a legal person, that of judicial winding-up.

Pursuant to judicial cooperation between Member States, we must point out that, a Member State is competent with respect to an offence against an information system if the offence has been committed at least in part on their territory or by one of their nationals.

When several countries have jurisdiction over an offence, they must cooperate to decide which one will conduct proceedings against the author of said offence.

[9] OJ L 69, 16.3.2005.

So, we can observe that the Directive 2013/40 places great emphasis on cooperation between Member States, the cross-border dimension of crime against information systems being carefully analysed at EU level.

3. Cooperation is the key or we may have all come on different ships, but we're in the same boat now

Cybercrime is developing all the time, causing costs running to billions of dollars[10]. In the past, computer related crimes were perpetrated mostly by individuals or small groups. In our days, we remark highly complex cybercriminal networks, incorporating individuals and groups of persons from across the globe.

In order to have a prompt and efficient response to these attacks, countries must cooperate with each other, and this kind of cooperation is one that could not satisfactorily be accomplished individually.

3.1. The international perspective or how a small leak may sink a great ship

The recent years have shown us that cybercriminals are always creative in terms of methods they choose perpetrate cyber offences. Although the case files may sound interesting from a theoretical approach, they offer new perspectives on how the international approaches regarding the prevention of the cybercrime phenomenon have failed and how cooperation can fix such issues.

One of those fascinating case files is known as Operation "Exposure/Unmask". This case file represented an international cybercrime investigation that was performed in Europe and South America, which led to the arrest of 25 alleged members of the international hacking network Anonymous. Tens of the arrested persons were Argentinean, Chilean and Colombian citizens and four were Spanish citizens[11].

The case is relevant for two reasons: first of all, it highlights the transnational dimension of cyberattacks, that can defy the distance between the perpetrator and the victims and, secondly, it proves that proper cooperation may lead to the removal of boundaries, even between states that are located in different continents.

It is known that Anonymous most commonly attacks the information systems through distributed denial-of-service (DDoS), web defacements and information disclosure.

[10] https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime, accessed on 26.03.2018.

[11] https://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/esp/operation_exposure.html?lng=en&tmpl=sherloc, accessed on 14.03.2018.

According to the United Nations Office on Drugs and Crime (UNODC), the elusive and transnational nature of the Anonymous network made it extremely difficult to identify the individuals responsible for the cyberattacks. Interpol and Europol played a crucial role in supporting law enforcement agencies in different countries. They facilitated international cooperation among national authorities and provided high-degree technical knowledge. Europol also provided on-the-spot support to law enforcement authorities in Spain and Bulgaria[12].

In this case file, the defendants were accused of "illegal interference", "breach of privacy" and "disclosure of confidential information". Concretely, according to Interpol, the suspects were charged with releasing personal data of police officers and bodyguards protecting Spain's royal family and the prime minister. Also, Colombia's Ministry of Defence and presidential websites, as well as the electricity company Endesa from Chile were victims of the cybercriminals[13].

The head of this operation was known as "Thunder" or "Pacotron" and was allegedly responsible for managing Anonymous' communication channels in Spain and South America[14].

Interpol and Europol played a major role. Particularly, the Europol Cyber Crime Centre allowed the preservation of data contained in servers located in Bulgaria and Czech Republic, while the Europol agents supported law enforcement in Spain and Bulgaria in arrests, searches and server disruptions[15].

3.2. The European perspective or all the flowers of all the tomorrows are in the seeds of today

In November 2014, Europol and several law enforcement and judicial authorities carried out an investigation, including house searches, against citizens from different Member States (Estonia, France, Romania, Latvia, Italy, United Kingdom). Following this action, 15 individuals were arrested. Most of the suspects were teenagers and young adults and they

[12] hhttps://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/esp/operation_exposure.html?lng=en&tmpl=sherloc, accessed on 20.03.2018.

[13] https://www.interpol.int/News-and-media/News/2012/PR014, accessed on 20.03.2018.

[14] https://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/esp/operation_exposure.html?lng=en&tmpl=sherloc, accessed on 20.03.2018.

[15] *Ibidem.*

were prosecuted for using remote access Trojans[16] (RATs) in order to perpetrate computer related crimes, such as theft of personal information, DDoS attacks and extortion.

The operation was initiated by France and had the support of Europol's Cybercrime Centre, which helped the countries involved in this investigation by hosting two operational coordination meetings, collating intelligence and providing analytical support[17].

Although this case may appear, at first sight, as an ordinary, typical cyberattack, probably the most interesting aspect of it, which caught our attention, is the age of the suspects and their attitude as regards their criminal conduct.

Thus, given that most of the persons involved were teenagers and young adults, they did not seem to understand, from a psychological perspective, the danger and the consequences of their actions.

In this respect, even the European Cybercrime Centre of Europol expressed its concern about the particularity of this operation, stating that crimes committed online are sometimes perceived to be "less serious" by these young offenders as they cannot physically see the victim or the effects of their crimes. Of course, this is simply not the case and their criminal activities will not be tolerated in cyberspace[18]. Thus, the need to discourage the young individuals from pursuing this criminal path plays a key role in the manner in which we build our cyber future and this can only be achieved by education.

3.3. The Romanian perspective or all roads lead to Roma…nia

In the past years, numerous Romanian citizens, most of them originated from Râmnicu Vâlcea, a small, but cybercrime concentrated city in the South-West of Romania, also known as "Hackerville", have been involved in computer crime offences.

In this section we will analyse a case in which two Romanian citizens were involved and we will describe how the cooperation between the Romanian authorities and their corresponding authorities from the other State was carried out.

In August 2016, the National Prosecutor's Office in Rotterdam, Netherlands, sent a letter of request to the Romanian authorities, requesting the legal assistance of the Romanian prosecutors, in order to identify two persons and to provide specific information about them.

[16] Remote access Trojans are malware that are used to spy on victims' computers (to access personal information, record on-screen activity, record webcam and microphone activity, collect passwords or credit card information).

[17] https://www.europol.europa.eu/newsroom/news/users-of-remote-access-trojans-arrested-in-eu-cybercrime-operation, accessed on 21.03.2018.

[18] *Ibidem*.

These persons were suspected by the Dutch authorities for recurrently committing ransomware attacks during the 18 months previous to sending the letter of request. In specific terms, the investigation performed in Netherlands revealed that two persons hacked many computers of Dutch citizens, by attacking them with a virus called Curve-Tor-Bitcoin Locker (CTB-locker). The suspects used e-mail addresses that were very similar to those of some existing companies and sent such e-mails to their victims to which they attached some PDF or ZIP files.

Given the appearance of the e-mails and their similarity to those that were usually sent by the trusted companies, the victims opened the files attached to them. In that moment, their computers became encrypted and a message appeared on the screen, requesting that the users should pay a certain amount of money, in order to unlock their computers.

The Dutch authorities started an investigation and managed to identify the server that was used to send these e-mails, with the aid of the National Centre of Cyber Security from Netherlands. The prosecutors corroborated the data existing on that server and reached the conclusion that there was a reasonable suspicion that two Romanian citizens owned the e-mail address that might have been behind those ransomware attacks.

The Romanian authorities received the letter of request and started its execution. The requested assistance included the following actions: the name and other identification details of these persons, the IP addressed they used from their homes, information about their studies and backgrounds, financial data, such as the transfers they performed during the last two years and other information provided by the fiscal authority regarding the incomes of these persons during the same period of time.

The Romanian prosecutors had the support of local police officers, who started to gather this information. Concretely, the police officers specialized in the investigation of cybercrimes did an exhaustive research, starting from the details provided by the Dutch authorities. Thus, they made connections between the existing data they had about these persons and succeeded in identifying them as being Mr. X and Mr. Y.

This identification was possible due to the fact that the suspects used the same e-mail address when logging in social media networks, such as Facebook and Skype, as well as other Romanian dating websites and sale-purchase websites. Thus, the authorities found their complete names and their addresses, so the identifying process became easier.

Subsequently, based on the identification of Mr. X and Mr. Y, the police officers and the prosecutors started to gather the other requested information. In this respect, they

requested the authorization of the judges to obtain data from the local fiscal authorities as regard their incomes, as well as from their personal bank accounts.

The judges authorized these operations and, based on their mandate, the prosecutors were given access to this information. They gather all information in a case file and sent it to the authorities from Netherlands, thus fully executing the letter of request.

3.4. The importance of Directive 2013/40 in the context of European judicial cooperation – the early bird catches the worm

As noted in the second chapter, probably the most significant provisions of the Directive 2013/40 are those related to the information exchange between the Member States. Therefore, the challenge of combating cybercrime in all of its dimensions demands multiple approaches, including both voluntary and mandatory cooperation.

Article 13 of the Directive 2013/40 provides that the Member States should implement the necessary procedures, in order to give an answer to the urgent requests within a maximum of eight hours as of the receiving of the request.

Generally, the requested cooperation involves many activities, so the time limit of eight hours may be feasible only for incomplete responses. Although the celerity of the actions performed in relation to such requests is crucial, there are few chances – objectively speaking – that the requested State executes the request and provides full, complete responses within the eight hours. However, such responses "shall at least indicate whether and in what form the request for help will be answered and when". Consequently, substantive responses are not necessarily required in this initial response[19].

Furthermore, many Member States expressed some reservations as regards this time limit and considered that a more realistic time frame would be around twenty-four hours[20].

On the other hand, taking into consideration the specific nature of computer crimes and their international dimension, the time aspect is crucial. Thus, fighting against these crimes – especially when the international judicial cooperation is required – involves the need to rely on fast communication channels. In this respect, the effectiveness of contact points is decisive in the success of cooperation between Member States.

As described in the second chapter of this paper, the main purpose of the Directive 2013/40 is to harmonize the legislation of the Member States. This aspect is also essential

[19] The Directive on attacks against information systems - A Good Practice Collection for CERTs on the Directive on attacks against information systems, ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013, p. 31.

[20] *Ibidem.*

from the point of view of international cooperation, such that the perpetrators of computer related offences could not use in their favour the potential lacks of inadequate national laws from less developed Member States in order to avoid prosecution or greatly complicate investigations[21].

The transposition of the Directive 2013/40 in the national law of Member States should eliminate such lacks of criminalization, by creating an overall cohesion and increased cooperation between the Member States. It is generally known that cyber criminals do not hesitate to exploit the weaknesses in the laws and practices of the states, so the speed and the complexity of cyber activities require predetermined, consented procedures for cooperation in investigating and combating their attacks.

4. Tension between human rights and prosecuting cybercrimes or run with the hare and hunt with the hounds

When applying the provisions of the Directive 2013/40, it should be taken into consideration to ensure the balance between human rights and state security. The guarantees offered by Article 8 of the European Convention on Human Rights (ECHR) and Article 7 of the Charter of Fundamental Rights of the European Union (CFREU) are the most likely to be breached when investigating cybercrimes.

Even if the ECHR has yet to catch up with the digital reality and its case-law is scarce in this area, there are two judgements that may be of interest in our approach.

4.1. Čalovskis v. Latvia

In the case of Čalovskis v. Latvia[22], the applicant, Mr. Deniss Čalovskis, was indicted by a grand jury sitting in the United States on five counts of conspiracy to violate the criminal laws of the United States. The accusation was based on the fact that the applicant together with other members of a criminal enterprise had created and distributed malware software known as the "Gozi Virus".

After the indictment, a warrant was issued for the arrest of the applicant, who at that time, was living in Latvia. Pursuant to the 2005 US-Latvia Extradition Treaty, a request was made by the United States for the applicant extradition. Following the request, the Latvian authorities arrested the applicant.

[21] Abraham D. Sofaer, Seymour E. Goodman, A Proposal for an International Convention on Cyber Crime and Terrorism, Hoover Institution Press, August 2000, p. 7.

[22] Čalovskis v. Latvia, no. 22205/13, 24 July 2014.

A few days after his detention, he was brought before the Riga City Centre District Court for a detention hearing. During this hearing, the applicant claimed that he was put in a dock with metal bars and that he was instructed by the police to pull the hood of his jacket over his head.

We chose this case because we think it underlines a great misconception about cybercrimes, specifically, the way an attack against an information system is viewed by the public[23].

The public associates cybercrime, no matter of its form, with some kind of act of terrorism, or a violent crime. Even though cyber terrorism is a crime in its own rights, and it should be placed in the category of terror attacks, one could not possibly say that cyber terrorism has the same implications or the same level of danger as accessing someone's email without their permission.

In the case that we have presented above, even the ECHR has come to the conclusion that "although, in contrast with the cases referred to by the Government, the applicant had not been handcuffed and special security forces were not present, the Court considers that given their cumulative effect, the security arrangements in the courtroom were, in the circumstances, excessive and could have been reasonably perceived by the applicant and the public as humiliating"[24].

In our opinion, the Directive 2013/40 solved this problem. Article 9 of the Directive 2013/40 begins by stating a principle regarding the sanctions that the Member States have to enact in relation to the offences provided for by this legal instrument. Thereby the penalties should be "effective", "proportionate" and "dissuasive". The key word is "proportionate".

What defines the distinction between cyberattacks is Paragraph 4 of Article 9, which establishes aggravating circumstances. So, if they are committed within the framework of a criminal organization, as defined in Framework Decision 2008/841/JHA[25], irrespective of the

[23] Even the CJEU has stated in one of its cases that computer crimes have a determinant level of danger that can justify the expulsion of a person and constitute an exception to the principle of freedom of movement.

"Article 28(3)(a) of Directive 2004/38 must be interpreted as meaning that it is open to the Member States to regard criminal offences such as those referred to in the second subparagraph of Article 83(1) TFEU as constituting a particularly serious threat to one of the fundamental interests of society, which might pose a direct threat to the calm and physical security of the population and thus be covered by the concept of 'imperative grounds of public security', capable of justifying an expulsion measure under Article 28(3), as long as the manner in which such offences were committed discloses particularly serious characteristics, which is a matter for the referring court to determine on the basis of an individual examination of the specific case before it." Judgement of 22 May 2012, P. I. v Oberbürgermeisterin der Stadt Remscheid, C-348/09, EU:C:2012:300, par. 33.

[24] Čalovskis v. Latvia, no. 22205/13, 24 July 2014, par. 107.

[25] Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime, OJ L 300, 11.11.2008.

penalty provided for therein, if they cause serious damage, or if they are committed against a critical infrastructure information system, the crimes ought to be punishable by a maximum term of imprisonment of at least five years.

One final statement that the Court made in this case which we believe is to be kept in mind while discussing measure against cybercrime is that "inherent in the whole of the Convention is the search for a fair balance between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights. As movement about the world becomes easier and crime takes on a larger international dimension, it is increasingly in the interest of all nations that suspected offenders […] should be brought to justice"[26].

Being aware of the rapidity with which technology is evolving, we can say that this "speed" is probably the greatest enemy of the legislative process. To always have a legal text that incriminates all the ways of committing a cybercrime, it would require an overwhelming effort on the part of the legislators and given the length of the legislative process that must always ensure compliance of all democratic guarantees, this would probably produce more damages and instability than an actual solution.

Although it is in the interest of the entire international society that all those committing crimes should be held accountable and that the states cooperate in this matter, not even this should justify a treatment contrary to the convention, and the Directive 2013/40 should be a sufficient instrument to both prosecute the suspects and respect their rights.

4.2. Nagla v. Latvia

Another relevant case, this time regarding Article 8 and 10 of ECHR, that displayed a problem which should be taken into consideration is the case of Nagla v. Latvia[27].

Ilze Nagla (the applicant) was a journalist living in Latvia, at the time of the events. One day, she received an e-mail from an unknown person, going by the name "Neo", who claimed that he had found some security flaws in a database of the state. Exploiting these flaws, he had accessed the system and he had stolen some data; to support his allegations, he showed the applicant some examples of the data, whose veracity could be confirmed by the applicant. So, after she concluded that what Neo showed her was real and that it might be the case of a security breach, she proceeded to inform the authorities.

[26] Čalovskis v. Latvia, no. 22205/13, 24 July 2014, par. 129.
[27] Nagla v. Latvia, no. 73469/10, 16 July 2013.

A few days after the first e-mail, the applicant went on and made public the news that there was a data leak from a database of the state. After this broadcast, Neo started to publish data on his own, through his Twitter account.

As soon as the authorities started to investigate the leak, they asked the applicant to turn over her e-mails, which she refused, saying that it is her right to refuse to disclose the identity of her sources or information that might lead to its disclosure as stated by the Law on Press and Other Mass-Media.

A few months later, the police conducted a search at the applicant's home based on a search warrant which was only authorized by the public prosecutor, being approved by a judge a day after the warrant had been put in practice. As a result of the search, there were confiscated a laptop, an HDD and some memory sticks containing work related information among other things.

First of all, what we have observed in this case is that in order to prosecute the persons guilty of a cyberattack, the state authorities were willing to apply a procedure that did not fully respect the fundamental rights of the citizens as provided by the Convention.

The applicant has stated before the ECHR that "the Latvian legal system did not provide her with adequate legal safeguards to allow an independent assessment of whether the interests of the criminal investigation overrode the public interest in the protection of journalistic sources"[28]. Moreover, given the fact that the Court said that there has been a violation of Article 10, only goes to show the need to establish a common procedure for investigating cybercrimes.

And this brings us to our point: in order to secure an investigation that is effective, but also respects the fundamental rights of the citizens, this common procedure should be regulated at a higher, supra-state level; if the EU has decided to establish guiding principles for defining cybercrime, even more it would be appropriate to determine a set of rules to help identify and properly investigate these offences.

5. Proposals or the future is already here, it's just not evenly distributed

Is there a mechanism to ensure both the proper investigation of cybercrime and the prevention of these types of crimes, if not entirely, at least to ensure a proper damage control response?

[28]Nagla v. Latvia, no. 73469/10, 16 July 2013, par. 53.

As mentioned before, cyber-attacks happen in matters of seconds and they could spread to almost an entire country in hours. Hence, would the supervision of all networks and computers, not just those in public institutions but also those of citizens could be a solution to stopping these attacks? Could the Big Brother keep us all safe and be a guardian of the digital market?

The advantages and disadvantages of this idea have put us in a position of scepticism about its implementation. Even if there is an institution that has the abovementioned attributions, an institution that functions at the level of the EU, an institution which in its turn is monitored by the Commission, the Parliament and the Council in all its aspects, such an institution would not present all the guarantees of independence and impartiality in the eyes of every citizen.

A case could be made for the sovereignty of states. Such an institution, even though it would be under indirect control by the member states, would nevertheless be an institution of the EU, which is a distinct entity. Thus, a question could arise whether such an authority, which would have access to the digital privacy of every citizen and even organs of the state, would not violate the sovereignty of states. People agreed to give part of their freedom in order to be better protected and that led to the formation of states and democracy as we know them today. But to have someone looking over your shoulder as you browse the web, knowing your desires, and keeping a tab on every click you make is a choice that should be made by the people who represent us, or by every citizen himself?

Seeing as the previous proposal is controversial and the debate on whether it is a benefit or a burden could go on beyond the principles, further we'll analyse ideas that could be put to practice in order to reach the same goal, specifically, to improve the EU's response to cybercrime and to establish a strong collaboration that will constitute a "Union firewall".

As shown above, cross-border cooperation between the authorities involved in the fight against cybercrime has become crucial in any investigation, since there is almost no investigation that does not involve an extraneous element.

Among the most important aspects that should be improved regarding the Member States of the EU, there is a corresponding, preferably unitary, transposition of the Directive 2013/40, in order to avoid any discrepancies that may make cooperation difficult, a stronger regulation of electronic evidence which is vital to ensure an effective cybercrime investigation, better public-private cooperation on information exchange in the case of cyber-attacks, a specialized training of prosecutors in the field of cybercrime, with specialized

sections within prosecution offices for investigating these crimes and education of the population in cyber security and personal data protection.

5.1. Proper implementation – specific is terrific

With regard to the proper and uniform transposition of the Directive 2013/40, the Commission published on the 13th of September 2017 a Report addressed to the European Parliament and the Council on the degree of implementation of the Directive.

Even though there is significant progress made by EU-wide uniform regulation of cybercrime, and cross-border cooperation has greatly improved, there are still inconsistencies in the application of the Directive's provisions, so the proper implementation of the Directive comes like natural step in the future for the Member States, in order to co-operate in the annihilation of cybercrime.

The first and most important of these is the transposition of Article 2 of the Directive on definitions of the terms "information system", "computer data", "legal person" and "without right", these terms having an effect on the application field of the Directive.

For example, there are Member States that have not included the phrase "a program that allows a computer system to perform a function in the definition of the term computer data"[29], act that may lead to a cooperation problem if in one of the Member States a certain behaviour is an offence, and in another Member State exactly the same behaviour is not considered an offence.

Another issue linked to a unitary transposition, on which Member States should focus, is the lack of unity in the inclusion of all possibilities that define actions in relation to offences. There are Member States that have not explicitly stipulated that illegal access to a part of a computer system is considered a criminal offence, criminalizing only illegal access to a computer system as a whole[30]. Even if for someone outside the IT domain, this omission may appear to be legally irrelevant, it is quite important because the Directive provides the definition of a computer system, a simple part of a computer system not being included in the definition given by the Directive, and so, illegal access to a part of a computer system will remain unpunished.

[29] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, p. 7.

[30] *Idem*, p. 8.

There are also issues of transposition of the terms "deterioration" and "making inaccessible" in the cases of "illegal system interference" and "illegal data interference", as well as incrimination of the "illegal interception of electromagnetic emissions" or "acquisition for the use of equipment to commit cybercrime"[31].

Also, there is a slip regarding the definition of the term "minor cases". "Minor cases" are an essential element of this Directive when qualifying an offence. For reasons of legal certainty, EU therefore has to give a definition of this term, so we appreciate that Article 2 of the Directive should contain this definition.

One of the good things that can be distinguished by looking at how the Directive is implemented by Member States is that the rules on competence for the investigation of cybercrime have been fully transposed, facilitating possible cross-border cooperation at EU level.

Another element of collaboration at international level, perhaps the most important one, is the network of contact points. As it has been said, each Member State is required to establish a 24 hour a day, 7 days a week contact point, to ensure communication with other Member States in relation to the offences established by the Directive.

Again, it is gratifying that all Member States have established such contact points (some of them using the contact points of G7 network or of the Council of Europe's Budapest Convention on Cybercrime). However, Romania[32] and Ireland have these contact points available only within a certain timeframe. Therefore, it is necessary to establish such contact points available 24 hours a day, 7 days a week (in Ireland and Romania), but more important than this is to provide a legal framework in which these contact points can collaborate with the judicial authorities from other Member States.

Also, it is important that, while the rapid exchange of information and mutual help is an essential tool of fighting jointly the cross-border cyberattacks, these rules must not affect the admissibility of evidence in possible subsequent criminal procedures.

Most of the time, these requests for information submitted by the judicial authorities of a Member State to a contact point in another Member State concern the identification of

[31] *Ibidem.*

[32] Even if Romania has informed the Commission that these contact points are only available within a certain timeframe, following discussions with the Chief Prosecutor of the Cybercrime Investigation Section of the Direction for the Investigation of Organized Crime and Terrorism, which is also a contact point, we found that he is available 24 hours a day, 7 days a week to assist the judicial authorities in the Member States.

IPs that private companies providing Internet services may or may not provide, according to national legislation[33].

So, these issues lead us to a second proposal, which is a stronger regulation of electronic evidence.

5.2. Electronic evidence

It is obvious that cybercrime leaves digital traces that the judicial authorities can collect and exploit in an investigation. However, at the EU level, there is no effective mechanism regulating the collaboration in obtaining this evidence.

Collecting real time electronic evidence from the Member States of the EU and ensuring their admissibility in court is very important.

Until now, the principle of territoriality has applied to direct cross-border access to stored electronic data in the framework of criminal proceedings, just as it does to other cross-border sovereign measures. Pursuant thereto, in advance of any access, mutual legal assistance measures must be used to obtain the consent of the State on whose territory the data are physically stored. In practice, this legal situation leads to problems primarily because that State often (as in the case of cloud computing) cannot be ascertained with reasonable technical effort, and the level of speed required, above all in carrying out open measures, does not allow prior proceedings for the granting of mutual legal assistance, especially in the prosecution of cybercrimes.

Our proposal is to create an effective instrument for states consisting of a mere notification in order to intercept telecommunications across borders without the necessity of technical assistance from the other State, but with the opportunity for the State in case to object to such operations[34].

Also, we must point out again that different standards on the admissibility of evidence must not constitute an impediment to the fight against cybercrime. The EU should take a step further and make sure that such an exchange of information shall not be affected by Member States' national ruling the use of evidence in criminal proceedings.

[33] For example, in Romania, companies providing Internet services are not required to provide information about a given IP at the request of the contact point, but there are situations when they make it from courtesy to the judicial authorities and to fulfil their civic duty to help sanction criminal behaviour.

[34] This solution could be modelled on Article 31 of the Directive 2014/41/EU regarding the European Investigation Order in criminal matters.

The European Commission is working on a legislative solution that hopefully will answer all these issues[35].

5.3. Collaboration between the public and private sectors or it takes two to Tango

Collaboration between the public and private sectors on the exchange of information in the cases of cyber-attacks is certainly an area that needs to be improved. Article 13 Paragraph 3 of the Directive requires Member States to take the necessary measures to ensure that adequate channels are available to facilitate the prompt notification of cybercrimes to the competent national authorities. Given the cross-border nature of these crimes, and in the spirit of loyal cooperation in ensuring the security of the EU, Member States should ensure that national authorities don't cooperate only with the judicial authorities of other Member States and the private entities of their own State, but also have channels through which they can collaborate with private entities in other Member States[36].

So, besides the cooperation between the authorities, it is vital to increase the cooperation between the private sector and public authorities in order to effectively fight against cyberattacks and increase the resilience of both public and private networks.

Cooperation with the private sector is of critical importance, with public-private partnerships to structure a common effort to fight online crime. The response to cybercrime (phishing) must involve the entire chain: from Europol's European Cybercrime Centre, Computer Emergency Response Teams in the Member States concerned by the attack, to internet service providers that can warn end-users and provide technical protection[37].

Governments and public authorities are reluctant to share information on cyber security because of the risk of compromising national security or competitiveness. Private businesses are reluctant to exchange information about their cyber vulnerabilities and resulting losses, for fear of compromising sensitive business information, risking their reputation, or risking breaching data protection rules.

---

[35] At the Justice and Home Affairs Council on 8 June 2017, Ministers asked the Commission to proceed with the implementation of the set of practical measures and to come forward with concrete legislative proposals regarding the electronic evidence. Commissioner Jourová announced her intention to put forward legislative measures for adoption by the Commission in early 2018.

[36] For example, a legal person in Austria should be able to report a cyber-attack on its servers directly to the Romanian judicial authorities if it has information that these judicial authorities are in a position to effectively conduct an investigation into the accountability of the perpetrators by that computer attack.

[37] EUROPEAN COMMISSION - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - The European Agenda on Security, Strasbourg, 28.4.2015, p. 20.

From our point of view, trust in public-private partnerships needs to be strengthened in order to support wider cooperation and exchange of information between a larger number of sectors through campaigns which draw attention of the private sector that collaboration with law enforcement authorities responsible for the investigation of cybercrime can help them in the long run. Also, public authorities should provide insurance that such collaboration will not affect the reputation of a private company and will not cause it to violate the legal provisions protecting personal data.

Lex ferenda, the adoption of a directive harmonizing the provisions protecting personal data as regards relations between judicial authorities fighting cybercrime and legal persons could address many of these issues.

This directive should assure that public and private sectors should share more information related to cyber threats, vulnerability and consequences work to create new platforms, strengthen existing platforms, and coordinate these platforms to increase information-sharing and improve investigations and prosecutions. Also, public and private sectors should cooperate to encourage and advance wider adoption of the Directive 2013/40, or, of the principles it promotes and should build trust and discuss contentious topics related to cybercrime, such as encryption, cloud servers, data access and protection of privacy, to find appropriate solutions.

5.4 Education and training – education, education, education

Regarding the specialized training of prosecutors in the field of cybercrime and education of the population in cyber security and protection of personal data, we believe that the whole society should take a stand.

Adequate training of the actors concerned with prosecuting cyber criminals is vital in the fight against cybercrime. Further, at EU level there are instruments to enhance this cooperation and training. This is all the more important as police and judicial bodies are faced with legal systems that qualify and define offences differently. Mutual understanding is hence pivotal.

Improved cooperation between law enforcement bodies and between judicial authorities across the Union is essential in fighting effectively against cybercrime. In this context, the EU and the Member States should step up their efforts, as regards adequate training of law enforcement bodies and judicial authorities, in order to raise the understanding of cybercrime and its impact, and foster cooperation and exchange of best practices, for

example through the European Judicial Network, with the assistance of Europol, Eurojust and the European Network and Information Security Agency.

Even though there are training programs for prosecutors and other authorities competent in the investigation of cybercrime[38], the same cannot be said about the rest of the population.

Given that, according to studies, more than 95% of computer incidents are reported to have occurred because of a human error[39], we believe that prevention courses on cybercrime need to be introduced in schools. It is only by instructing new generations to be aware of the danger this crime represents that we can really counteract the phenomenon.

Education is the most powerful weapon that EU citizens have in fighting cybercrime. We are talking about education in terms of prevention, but also about the training of specialists, both technically and legally, that can counteract the phenomenon of cybercrime.

In terms of crime, cybercrime is the future, and the future is happening right now.

[38] For example, in Romania, within the Direction for the Investigation of Organized Crime and Terrorism, there is a specialized section in the fight against cybercrimes.

[39] https://edwps.com/cyber-the-insider-threat-by-mellisa-wagner/, accessed on 26.03.2018.