ROAR empowering victims of cybercrime | APAV Apoio à Vítima

Co-funded by the European Union's Internal Security Fund - Police

Policy Paper: challenges in the field of cybercrime and recommendations to overcome them

1. Description of the context and importance of the problem

Considering current globalisation and the constant use and growing dependence on the internet, cybercrime continues to evolve becoming more complex and sophisticated by the day. Estimates suggest that by 2030, there will be 125 billion devices connected to the internet, and 90% of individuals older than 6 will be online, increasing significantly the reach of possible victims.[1] In this context, cybercrime poses a great threat to society and democracy as it causes not only damage (at various levels) but it also affects fundamental rights of individuals and rule of law.[2]

Action must therefore be taken in order to catch up with the development of information technology attacks and effectively tackle cybercrime. This action must be based on a synergy between all relevant stakeholders, particularly the network and information security sector and the cyber law enforcement agencies (LEA) to improve the overall cyber resilience and cybersecurity.[3]

Having said that, this paper intends to explore the challenges faced by all relevant stakeholders in the combat of cybercrime at the European level, followed by the Portuguese, Romanian and German scenario, and, lastly, sheds light upon promising measures that can have a positive impact in achieving higher degree of cybersecurity and finally overcome the identified challenges.

[1] European Parliament, Cyber: How big is the threat? https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

[2] P8_TA(2017)0366, The fight against cybercrime, European Parliament Resolution on the fight against cybercrime (2017/2068(INI)) (2018/C 346/04), 3 October 2017.

[3] Internet Organised Crime Threat Assessment, European Cybercrime Centre EC3, Europol 2019.

1.1. Europe

In Europe, numbers are increasing every year and it is estimated that they will keep growing drastically. According to the EUROPOL 2019 report on Internet Organised Crime Threat Assessment, the current most prominent threats in Europe are:[4]

1- Cyber-dependent crime:
   a. Phishing and vulnerable remote desktop protocols (RDPs) are the key primary malware infections, ransomware the top threat but overall volume has declined;
   b. Data compromise represents the second-most prominent cyber-threat (most frequently relates to the illegal acquisition of financial data, such as credit card information, online banking credentials or cryptocurrency wallets, through means such as phishing, data breaches and information gathering malware);
   c. Dos/DDoS attacks (denying others access to that entity's data or services was the third most significant threat);
   d. Attacks on critical infrastructures;
   e. Website defacement.

2- Child sexual exploitation online:
   a. Amount of child sexual exploitation material (CSEM) continues to increase, the m.o. is unchanged;
   b. Self-generated explicit material (SGEM) becomes more and more common, intensified by the growing access of minors to smartphones and lack of awareness of the risks;
   c. Sexual coercion and extortion of minors for new CSEM;
   d. Live distant child abuse (LDCA) is increasing.

3- Payment fraud:
   a. Card not present (CNP) fraud;

[4] IOCTA 2019 Europol

b. Skimming and shimming tools are evolving;
c. Jackpotting is evolving and becoming more accessible and successful;
d. Business email compromise (BEC).

4- The criminal abuse of the dark web:
   a. Remains the key online enabler for trade of criminal products and services;
   b. Increased fragmentation on Tor markets, single-vendors, making it harder for law enforcement (e.g. traceability);
   c. Encrypted communication applications enhance single-vendor trade on the dark web, enabling closed communications between direct users and services.

5- The convergence of cyber and terrorism:
   a. Wide range of online service providers (OSPs) exploited by terrorist groups;
   b. Platforms for their online communication and distribution strategies;
   c. Even though it is still limited, it is an imminent problem.

6- Cross-cutting crime factors
   a. Social engineering:
      i. Phishing – a core attack tool for all cybercrime
   b. Money Mule
      i. Second most prominent cross-cutting threat
   c. The criminal abuse of cryptocurrencies; non-cash payment fraud (NCPF) used as tools in the arsenal of cybercrime.

To better grasp the importance of improving cybersecurity, besides the identification of the main threats, it is crucial to look at how people are perceiving and dealing with the situation. According to Eurobarometer on Europeans' attitudes towards cyber security, the following was found:

- 76% of responders use the internet daily – daily use of internet is rising;

- 85% of respondents access internet through smartphones, while the use of computers overall to access internet continues to decline;
- Most common activities carried out on the internet are social activities and online banking;
- Regarding concerns about cybersecurity, 93% of respondents said to have changed their behaviour in some way;
- Under the age of 55 people are more likely to have taken more security measures;
- 52% of respondents think they are well informed about cybercrime but considerable differences between MS;
- 76% of respondents believe that the risk of becoming a victim of cybercrime is increasing, but only 52% of respondents think they can protect themselves sufficiently against it;
- 22% of respondents are aware of the existence of an official channel to report a cybercrime or other illegal online behaviour;
- 83% of respondents have never reported a cybercrime or other illegal online behaviour;
- Out of 17% of responded who reported: 7% had reported to the police or authorities, 6% to a website and 5% to a service provider.

In brief, these data show that people are becoming more aware of cybersecurity problems and of the risk of becoming a victim, however, only roughly half of the respondents think they are well informed about cybercrime. Besides, only approximately half of the respondents think they can protect themselves. In addition, the daily use of internet is rising, which increases the reach of potential victims, and only a minority of respondents are aware of official channels to report incidents, which highlights the underreporting issue of the phenomenon.

1.2. Portugal

In Portugal, cybercrime incidents are also on the rise. According to the National Centre for Cybersecurity, the most common threats in 2019 were as follows:[5]

- Phishing and malware (including ransomware) are the most prominent threats;
- Intrusion into a system, component or network through the commitment of a user or administrator account (Account Compromise);
- Vulnerabilities exploitation (vulnerability as in failure in the software or hardware components that enable the attack);
- DoS/DDos attacks – those with an extortion element were the most prevalent;
- Botnets;
- Data breaches;

It is predicted an evolution and rise of the following threats:

- CEO Fraud (form of BEC);
- Account compromise;
- Vulnerabilities exploitation;
- False flag techniques;
- Cybercrime on demand, purchase of hacking and misinformation campaigns;
- New vulnerabilities due to latest technologies, such as Internet of Things (IoT), 5G, Artificial Intelligence (AI), and cryptojacking which will increase the surface prone to attacks.

According to the latest barometer on Portuguese people perceptions on cybercrime, the following were found:[6]

- 60% of respondents are always connected to the internet

[5] Cybersecurity in Portugal: Risks and Conflicts Report, National Centre for Cybersecurity, June 2020.
[6] APAV Barometer Intercampus on People's perception on cybersecurity, March 2020.

- 99% of respondents say emails are the main activity online, followed by social media
- The majority (97%) still accesses internet through a computer or laptop
- 76% of respondents use home banking services
- 75% of respondents who do online shopping are concerned with data breaches
- 82% of respondents declare to have changed their behaviour regarding cybersecurity, namely they do not open unknown emails. 78% installed anti-virus software and 76% uses more complex passwords than in the past;
- However, only 62% of people said to have changed their email passwords, 56% in social media, 55% in home banking services and 48% in online shopping
- These safer cyber behaviours are more relevant in people under 55 years old
- Out of total malware attacks (45%), only 3% reported it, as opposed to online fraud, which was reported by a majority of respondents
- Only 24% of respondents think they are well-informed about risks of cybercrime
- 46% of respondents believe cybercrime is on the rise
- 51% of respondents are worried that their personal data is not being adequately protected and secured by the public sector
- The biggest threat concern is about identity theft (50%), followed by malware attack (47%)
- Only 10% of respondents are aware of a victim's support structure for victims of cybercrime in Portugal. Out of those, the majority is aware of APAV (42%), followed by the Judiciary Police (25%)
- Regarding the LIS (Portuguese hotline and helpline), only 17% of respondents are aware of it. Out of those, 27% think it is intended to provide advice on the use of internet, 25% think it is intended to provide support to victims of cyber bullying
- As to parental monitoring of children's online activities, 74% say they monitor the online activity, 58% say they discuss the risks with their children. However, only 45% of parents limit the time children spend online and 42% use parental control features.

In short, the top threats are common to both scenarios: phishing and infection through malware. However, there are some threats identified at the European level and not so common in Portugal, but can be seen as a trend and become more relevant in Portugal in the future, such as ransomware, card not present fraud, CEO fraud, DoS/ DDoS attacks, supply chain attacks, data compromise and increasing digitisation of terrorism. As to people's perception, there are some cross-cutting traits found: **the lack of adequate information and awareness of cybercrime by a large percentage of people and the problem of underreporting.**

1.3. Romania

According to the 2017 Special Eurobarometer 464a, 82% of Romanians consider cybercrime a very or fairly important security issue, a number similar to the EU average of 87% of respondents who are of the same opinion.[7] In addition, about one in three Romanians are concerned about their personal information being misused online, as well as about the security of online payments, and fear that they might not receive the goods or services ordered online.[8]

Nevertheless, Romania is the EU country with the largest proportion of people who never access the Internet – 41% in 2017, a 10% increase since 2015. In the same time, an almost equal proportion of people – 47% – state that they access the Internet on a daily basis,[9] which speaks of the polarisation of Romanian society with regard to access to information and communications technology (ICT). This is also reflected in the relative low number of people who feel informed about the risk of cybercrime: roughly one in three (only 4% feel very well informed and 27% fairly well informed), whereas 66% feel uninformed.[10]

On the topic of perceptions about law enforcement, 55% of Romanians agree (totally and tend to agree) that the police and law enforcement are doing enough to fight cybercrime (similar to the EU

[7] European Commission, *Special Eurobarometer 464a: Europeans' Attitude towards Cybersecurity*, 2017, p. 8.
[8] Ibid., p. 40.
[9] Ibid., p. 14.
[10] Ibid., p. 52.

average of 49%).[11] These numbers have increased by 11% – the highest increase in the EU[12] – since the last barometer in 2015, potentially indicating intensified efforts on the part of the Romanian Police in tackling cybercrime.

The Special Eurobarometer also surveyed victimology rates. The most common form of cybercrime indicated by respondents in 2017 was malicious software, with 39% of Romanians having discovered it on their devices.[13] The other forms of cybercrime that Romanians have fallen victim to are (in order of their frequency): receiving fraudulent emails and phone calls requesting personal information, such as access to computer, banking information, etc. (22% of respondents);[14] having had their email or social network account hacked (18%);[15] online identity theft (11%),[16] and bank card or online banking fraud (9%).[17]

With regard to child pornography, 30% of Romanians, the highest proportion in the EU by far, have accidentally encountered such materials online.[18] However, alarmingly, only 52% of overall respondents indicated that they would contact the Police in this situation,[19] indicating an urgent need for the general population to be the target of educational activities and information campaigns aimed to increase reporting of child sexual abuse material (CSAM). There is also a need for more education and training on the safe usage of the Internet by children, as the most common measures taken by Romanians to protect children under the age of 16 against cyberstalking, cyberbullying and blackmail is to talk to them about the risks of the Internet (a measure taken by 43% of respondents) and to limit their use of the Internet (41%). Other measures include monitoring the child's Internet

[11] Ibid., p. 11.
[12] Ibid., p. 11.
[13] Ibid., p. 77.
[14] Ibid., p. 69.
[15] Ibid., p. 74.
[16] Ibid., p. 68.
[17] Ibid., p. 75.
[18] Ibid., p. 71.
[19] Ibid., p. 99.

usage and adjusting the security settings on devices. An issue of concern is that 19% of respondents indicated they do nothing to protect children against cyber risks.[20]

According to the Direction for the Investigation of Organised Crime and Terrorism (in Romanian: *Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – DIICOT*), the most frequently encountered forms of cybercrime in 2018 were:

- **ransomware** attacks, especially the self-propagating **ransomworms**, such as WannaCry, Arena Dharma, which produce substantial material loss among their victims, as well as negatively impact them emotionally. These attacks are expected to increase in the future and constitute a real challenge for the public and private sector.

- **man-in-the-browser** and **man-in-the-middle** attacks, where a Trojan horse is interposed between two parties, allowing the attacker to intercept communication, such as sensitive information, bank transfers, etc.

- **malware directed towards banks**, which involve viruses sent through executable files with backdoor capabilities, created through the platform Cobalt Strike, which permit attackers to transfer money to fraudulent bank accounts.

- illegal trade through the **Darknet** has also witnessed an increase in 2018, and the fact that the main means of payment are cryptocurrencies (especially Bitcoin, Ethereum, and Monero) makes it challenging to identify the attackers. There has also been an increase in **fraudulent cryptomining**.

- complex attacks on ATMs and bank systems are also on the rise, including but not limited to **deep insert skimming**, which involves copying data on the magnetic strip of credit cards.

- **child sexual exploitation materials** (CSAM) continue to be a challenge. Although these materials are generally produced by perpetrators, there is an increase in self-generated

[20] Ibid., p. 89.

material, which is then used to constrain and blackmails victims. Also on the rise is **live-streaming** involving minors.[21]

These trends are in accordance with international trends in cybercrime, as outlined in the IOCTA (Internet Organised Crime Threat Assessment) Report for 2018.[22]

Official data from the Romanian Police indicate that the majority of **criminal complaints and reports** concern, in order of their frequency, fraudulent financial transactions (approximately 3000 annual complaints), illegal access to a computer system (an average of almost 700 complaints a year), cyberfraud (an average of roughly 350 complaints a year), and child pornography (approximately 200 reports a year). For in-depth official Police statistics on the number of criminal reports filed and of criminal investigations of cybercrimes from 2015 up to September 2019 please see *Appendix 1*.

With regard to the number of **convictions** on accusations of cybercrime, official data from the Ministry of Justice indicate relatively low rates of conviction where such crimes constitute the main offence. The most frequent cybercrimes which resulted in convictions between January 2015 and June 2019 were child pornography, followed by illegal access to a computer system and performing fraudulent financial transactions. For four offences – accepting fraudulent financial transactions; illegal interception of a computer data transmission; disrupting the functioning of computer systems; and unauthorised transfer of computer data – there were no convictions in the aforementioned period.

For acts of **child pornography**, in the period between 2016 and 2019, final convictions range between 63 in 2016 and 95 in 2018.

The number of criminal reports and convictions of cybercrime, especially regarding child pornography, appears to be rather low and to not reflect the true extent of these phenomena. With cybercrime victimisation rates on the rise and with an increasing number of people encountering

[21] Direction for the Investigation of Organised Crime and Terrorism, *Activity Report 2018* [DIICOT, *Raport de activitate 2018*], February 2019, pp. 29-30.

[22] Europol, *IOCTA - Internet Organised Crime Threat Assessment 2018*, available at https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018 (accessed December 20th, 2019).

CSAM online, of whom only a half would, in theory, report it to the Police, as indicated by the Eurobarometer, law enforcement needs to expand its effort to combat, but also prevent cybercrime, and to actively involve public authorities, the industry, as well as the general public in the process.

1.4. Germany

According to the German Federal Office for Information Security (BSI)[23], recent incidents have occurred in Germany in the area of cybercrime. The most common threats in 2019 were as follows:

- Ransomware incidents increased significantly causing serious disruptions across all sectors;
- Malware infections are still one of the biggest IT-related threats to private users, businesses and public authorities, especially one piece of malware: Emotet;
- Incidents of identity theft are also becoming more common;
- Recent developments have shown that the risk of becoming part of a botnet is high, especially for mobile end-user devices and Internet of Things (IoT) systems;
- Server-based botnets offer a huge pool of resources for the execution of distributed denial of service (DDoS) attacks.;
- Although the absolute volume of malware spam is in sharp decline, spam still represents a serious potential threat. The quality – and thus the effectiveness – of malware spam continues to rise.

A number of phenomena can be identified as trends for APT (advanced persistent threat) Attacks[24]:

- A wide range of publicly available APT tools;
- A growing number of international APT service providers;
- The use of legitimate services as a cover for illicit activities;

[23] Annual report on the state of IT security in Germany in 2019 of the Federal Office for Information Security (BSI), p. 7
[24] Attacks neither opportunistic nor motivated by financial gain, but which follow strategic or tactical goals"; source: Annual report on the state of IT security in Germany in 2019 of the Federal Office for Information Security (BSI), p. 7

- Hindrances to malware analyses and the integration of APT techniques into criminal operations.

The development of internet usage in Germany are as follows[25]:

- 90 % of respondents are using the Internet;
- 71% of respondents are using the Internet on a daily basis;
- 33% of respondents have used a smart speaker.

According to the latest barometer on German people perceptions on cybercrime, the following were found[26]:

- 24 % of respondents became a victim of cybercrime in 2019 (of which 36 % in online shopping, 28 % in phishing und 26 % in viruses or Trojans);
- 29 % of respondents consider the danger to become a victim of cybercrime to be high or particularly high;
- 61 % of respondents have an up-to-date antivirus software;
- 58 % of respondents have a secure password;
- 36 % of respondents install available updates every time;
- 19 % of respondents use encrypted email;
- Only 31 % of respondents obtain information about cybersecurity regularly;
- 42 % of respondents only obtain information about cybersecurity if a problem occurs;
- 36 % of respondents protect themselves against the risks of cybercrime;
- A majority of the German population (82 %) are concerned regarding their safety while on the internet. More than half (51 %) are rarely concerned, while under a quarter of the respondents are concerned most of the time (24 %) or always (7 %).

[25] Internet usage in Germany: ARD/ZDF-Onlinestudie 2019

[26] Cybersecurity in Germany: Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit of the Federal Office for Information Security (BSI) and Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) 2019, p. 4 and 5

In short, the trends confirm the expectations that there is a new quality to cyber-attacks, which have now taken place as of today. Ransomware continues to pose the biggest threat to companies, public authorities, other institutions and private users. There was also a series of serious cases of identity theft. The huge volume of the personal data leaked and subsequently posted on the Internet is significant here. Around 114 million new malware variants were identified. Attackers of the botnet threat landscape are exploiting the digital transformation and focusing on mobile end-user devices and IoT systems. In general, the German population is aware of the potential risks of cybercrime and they already know some strategies to protect themselves. But there is still a lack of safety awareness and a lack of knowledge about cybersecurity. Those who already were a victim of cybercrime are more concerned about their safety while on the internet. Others who were not affected yet and don't inform themselves on a regularly basis are less sensitized about the subject.

2. Current legal framework

Successfully preventing and fighting cybercrime involves an accurate understanding of the evolving and ever-changing character of the criminal phenomena, alongside the role each key-stakeholder has in enabling a comprehensive, cross sectorial and multi-disciplinary collaboration in this endeavour.

Cybercrime has vast and long-lasting economic, social and individual impacts in both citizens and companies, to which State's infrastructures themselves are exposed to. Thus, governments must prioritize cybersecurity, as well as develop and execute national plans to tackle it. In parallel, they must foster existing policies and implement new ones effectively to ensure cross-border cooperation and national responses to borderless and often organised criminal phenomena.

In this regard and bearing in mind the global and pan-European character of cybercrime, the European Union (EU) itself takes on the responsibility to support Member-States in ensuring

security, upholding the fight against cybercrime as one of the three priorities of the European Agenda on Security (EAS).

Taking into account the European legal landscape, which outset is marked by the adoption of the Convention on Cybercrime[27] in 2001, followed by the adoption of the Convention of the Protection of Children against Sexual Exploitation and Sexual Abuse[28] in 2012, the EU's legislative and policy efforts started with the adoption of two Directives on combatting child sexual exploitation and abuse (CSEA) and attacks against information systems (Directive 2011/93/EU of 13 December 2011[29], and Directive 2013/40/EU of 12 August 2013[30], respectively). In 2013, the European Parliament, the Council, the European Economic and Social Committee, and Committee of the Regions issued a joint communication on Cybersecurity Strategy of the EU[31]. This Strategy identifies as main priorities the achievement of cyber resilience, developing a cyberdefence policy, industrial/technological resources for cybersecurity and establishing a coherent international cyberspace policy for the EU. In a more recent communication[32] (Sept. 2017), the European Parliament and the Council reinforced such concerns calling for: awareness raising campaigns, particularly in schools and universities; closer cooperation between civil society and public authorities; efforts to prevent and mitigate the impacts of cybercrime on end-users; among others. These instruments specifically mention the importance of tackling online CSEA and the special protection that should be provided to children, internet users who are more susceptible to cybercrime. Complementing its legislative and policy efforts, the EU created the EU Agency for Network and Information Security (ENISA), a centre of expertise for

[27] Council of Europe Convention on Cybercrime of 23 November 2001 (Budapest Convention), available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[28] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 25 October 2007 (Lanzarote Convention), available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201

[29] Directive 2011/93/EU of the European Parliament and of the Council on combatting the sexual abuse and sexual exploitation of children and child pornography, 13 December 2011. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN

[30] Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems, August 2013. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

[31] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, and Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7 February 2013. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

[32] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final, Brussels, 13.9.2017. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en

cybersecurity in Europe. The Agency works closely with MS and the private sector, providing advice and solutions, including the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies, capacity building, and studies on several matters, such as Cloud adoption, privacy technologies and data protection. More specifically related to CSEA, the Global Alliance Against Child Sexual Abuse Online was launched by the EC and the United States of America to raise standards and unite efforts in order to more effectively tackle CSEA. This Alliance introduces new commitments, focused on identifying and prosecuting offenders and enhancing victim protection.

EU MS, in particular Portugal, Romania and Germany, which form part of ROAR's partnership, have not only ratified the Budapest Convention and implemented its provisions in their criminal codes, but have also taken the necessary steps for the adoption of the Convention of the Protection of Children against Sexual Exploitation and Sexual Abuse (2012), alongside effectively transposing the two Directives on combatting CSEA and attacks against information systems (Directive 2011/93/EU of 13 December 2011, and Directive 2013/40/EU of 12 August 2013).

2.1. Portugal

In Portugal, the most important legal instrument to take into account in this respect is the **Law no. 109/2009**, also known as **the Cybercrime Law**. This Law criminalises conducts that fall under the narrower definition of cybercrime (also partially adopted by the Budapest Convention on Cybercrime), that is **cyber-dependent crimes** as they require an ICT infrastructure for its perpetration, namely:

- Computer-related forgery (art. 3.º);
- Data interference (art. 4.º);
- System interference (art. 5.º);
- Illegal access (art. 6.º);
- Illegal interception (art. 7.º); and

- Computer program copyright infringement (art.º 8).

In addition to these crimes, there are **cyber-enabled crimes** that can occur in the offline world but can also be facilitated by information and communication technology. Portuguese law has established in the **Criminal Code** some cyber-enabled offences that **specifically mention the use of computers as a means of committing the crime**, *v.g.*:

- Computer fraud (art. 221.º, CP);
- Child pornography (art. 176.º, CP);
- Child grooming (176.º-A, CP);
- Intrusion through computer means (art. 193.º, CP);
- Domestic violence (art. 152.º, no. 2, b) CP); and
- Aggravated disturbance of private life, intrusion in closed location, intrusion in private life, interception of communications, secret violation (art. 190 to 195.º and 197.º, CP).

Finally, the **Portuguese legal framework includes a multiplicity of provisions establishing** crimes that, **despite the fact that they can be carried out through computer systems**, **have no specific mention to technology of any kind**, namely:

- Homicide (art. 131.º, CP);
- Assault (art. 143.º, CP);
- Coercion (art. 154. º);
- Stalking (art. º 154-A, CP).
- Defamation (art. 180.º, CP);
- Mail or e-mail interception (art. 194.º, CP); and
- Illegal recording and photographs (art.º 199, CP);
- Intentional damages (art.º 212.º, CP);
- Fraud (art. 217.º, CP);

- Discrimination and hatred incitement (art.º 240, CP)
- Extortion (art.º 223, CP);
- Tax fraud (art. 103.º do RGIT);
- Copyright infringement (art. 195.º, 196.º and 199.º, CDADC);
- Industrial property infringement (art. 319.º to 327.º, CPI);
- Anti-economic offenses (art. 22.º to 41.º of DL n.º 28/84);
- Illegal gambling operating (art. 108. º do DL n. º 422/89)
- Terrorism (art. 2.º and 4.º, Lei n.º 52/2003)

In addition, the **Portuguese Cybercrime Law also defines the procedural rules for several computer investigation measures**:

- Expedited preservation of stored computer data (art.º 12);
- Expedited partial disclosure of traffic data (art.º 13);
- Production order to submit or grant access to data (art.º 14);
- Search and seizure of stored computer data and e-mail account (art.ºs 15 and 16 and 17), which can also allow to determine the blocking of access to certain sites;
- Real-time collection of traffic data and Interception of content data (art.º 18);
- Undercover actions (art.º 19); and
- Requirements for admissibility of telecommunications interception (art.º 187, CP ex vi art.º 189, CP);

Furthermore, there are some other diffused legal provisions closely connected to illegal contents online and to processing data in the context of cybercrimes investigation, such as the following:

- Decree-Law 7/2004 of January 7th transposed Directive 2000/31/EC and went further by setting out the obligation for information service providers to report illegal content upon obtaining such knowledge or awareness, as well as the obligation to comply with removal orders from the competent authorities and, in case of manifestly illegal content, the

obligation to immediately block or remove it, in spite of being generally liberated from monitoring the information they transmit or store (art.ºs 13, 16 and 15, respectively).

- Law 32/2008 of July 17th, as known as the Data Retention Law, transposed Directive 2006/24/EC and has put forward an obligation for electronic communications services or public communications networks to preserve and retain traffic data for a period of one year for the purposes of investigation, detection and repression of serious crimes (art.º 6). Albeit the Directive has been declared as invalid by the ECJ, the Portuguese Law is still in force.
- Law 59/2019 of August 8th transposed Directive (EU) 2016/680, establishing rules on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Especially important is the prohibition of profiling conducive to discrimination, on the basis of sensitive data, which is laid down on art. º 6 / 2 in conjunction with art.º 11.

Lastly, Law 46/2018 of August 13th, along with Council of Ministers Resolution 92/2019,[33] set out the cybersecurity legal framework and Portugal's strategy on cybersecurity 2019-2023, respectively. In a nutshell, the former establishes minimum standards of cybersecurity and reporting obligations to all levels of governmental and public institutions, critical infrastructures service providers, essential service providers and digital service providers. It also sets up the Superior Council for Cybersecurity, a consultation body to the Prime-Minister and the utmost authority in the country for cybersecurity matters, as well as the CERT.PT (computer emergency response team). At last, the former defines the strategy and its guiding principles, namely; the subsidiary principle of state intervention, the complementary principle of action (coordination between different relevant actors) and the principle of proportionality between resources allocation and threats' dimension. Besides, it outlines 5 pillars of action, focusing on a solid structure of cybersecurity agencies, prevention and awareness-raising, protection of cyberspace and critical infrastructures, capacity-building in identifying cyber-threats

[33] https://www.cncs.gov.pt/recursos/noticias/governo-aprova-nova-estrategia-nacional-de-seguranca-do-ciberespaco/. The full text can be found in https://data.dre.pt/eli/resolconsmin/92/2019/06/05/p/dre

and fighting cybercrime, development of investigation and innovation techniques, and sturdy cooperation between national agencies and at the international level.

2.2. Romania

In the case of Romania, national legislation does not have a distinct law dedicated to cybercrime, as these types of crimes are sanctioned under the country's Criminal Code and under Law no. 161 of April 19, 2003 on certain measures to ensure transparency in the exercise of public dignity, public office and in the business environment, the prevention and sanctioning of corruption. The Criminal Code recognises the following cybercrimes, which fall into different titles and chapters:

Title II. Offences against patrimony. Chapter IV. Fraud committed through computer systems and means of electronic payment:

- Cyberfraud (Art. 249), defined as "introducing, modifying or deleting computer data, restricting access to this data or in any way impeding the functioning of a computer system, in order to obtain a material benefit, if a loss has been caused";
- Performing fraudulent financial transactions (Art. 250) – "carrying out an operation of withdrawing cash, loading or unloading an electronic currency instrument or transferring funds through the usage, without the consent of the holder, of an electronic payment instrument or of data permitting its identification", including fictitious data;
- Accepting fraudulent financial transactions (Art. 251) – accepting the aforementioned transactions in full knowledge of their fraudulent nature;

Title VII. Offences against public safety. Chapter VI. Offenses against the security and integrity of computer systems and data:

- Illegal access to a computer system (Art. 360), which differentiates between unlawful access to a computer system, unlawful access to a computer system with the purpose of obtaining

computer data, and unlawful access to a computer system which has programmes, devices or procedures to restrict access to it. The three offences have increasingly severe sanctions.

- Illegal interception of a computer data transmission (Art. 361);
- Altering the integrity of computer data (Art. 362) – "unlawfully modifying, deleting or damaging computer data or restricting access to such data";
- Disrupting the functioning of computer systems (Art. 363) – "severely disrupting, without right, the functioning of a computer system, by entering, transmitting, modifying, deleting or deteriorating computer data or by restricting access to computer data";
- Unauthorised transfer of computer data (Art. 364);
- Illegal operations with computer devices or software (Art. 365) – producing, importing, distributing, providing or unlawfully possessing devices, programmes, passwords, and access codes that permit partial or total access to a computer system for the purpose of committing the offences under articles 360 to 364.

Title VIII. Offenses that affect relations regarding social coexistence. Chapter I. Offenses against public order and peace:

- Child pornography (art. 374), which is defined as "producing, possessing, procuring, storing, exposing, promoting, distributing, and providing, in any way, pornographic material with minors"[34], as well as "extorting or recruiting a minor for the purpose of participating in a pornographic show, obtaining benefits from such a show or exploiting a minor in any other way for performing pornographic shows."[35] Viewing of pornographic shows with minors is also punishable by law. The cybercrime component of child pornography is evident in paragraph 2 of article 374 which explicitly mentions sanctions for the abovementioned

[34] Pornographic materials with minors is defined as "any material that presents a minor or an adult as a minor, having explicit sexual behaviour or who, although not presenting a real person, credibly simulates a minor having such behaviour, as well as any representation of genital organs of a child for sexual purposes." (Art. 374, paragraph 4, Criminal Code).

[35] Pornographic show is defined as "live exposure to a public, including through information and communication technology, of a child involved in sexually explicit behaviour or the genital organs of a child for sexual purposes." (Art. 374, paragraph 4^1, Criminal Code).

offences, should they be committed through a computer system or any other means of electronic communication. In addition, paragraph 4 explicitly included information and computer technology (ICT) as media for pornographic shows.

The attempt to commit the abovementioned crimes also constitutes a crime, according to articles 252, 366, and 374 (5) of the Romanian Criminal Code.

In addition to the Criminal Code, some forms of cybercrime are also criminalised under Law no. 161 of April 19, 2003 on certain measures to ensure transparency in the exercise of public dignity, public office and in the business environment, the prevention and sanctioning of corruption, hereinafter Law 161/ 2003. Articles 36 to 41 of this law refer to the prevention of cybercrimes, in the form of a series of activities, such as: prevention programs; policies, procedures, and minimal standards for cybersecurity; awareness campaigns, implemented by public authorities, service providers, NGOs, and other representatives of civil society. These articles also nominate the institutions in charge of data collection, conducting studies and report, and of the training of professionals – the Ministry of Justice, The Ministry of Internal Affairs, The Ministry of Communication, the Romanian Information Service, and the External Information Service.

Law 161/ 2003 doubles some of the crimes sanctioned under the Criminal Code. Articles 42 to 47 fall under the category of *Crimes against data and information system confidentiality and integrity*, and include: the illegal access to an informatic system (Art. 42); illegal interception of data transmitted through an informatic system (Art. 43), illegal modification or erasure of informatic data or the restriction of access to such data (Art. 44); illegal disturbance of an informatic system (Art. 45); producing, selling, distributing, owning a device or informatic program, as well as password of access data with the goal of carrying out the crimes stipulated in Articles 42 to 45 (Art. 46). The attempt to commit the abovementioned crimes also constitutes a crime (Art. 47). Articles 48 to 50 refer to *Cybercrimes* and include: the illegal modification, introduction, erasure or restricting the access to informatic data with the goal of producing legal consequences (Art. 48); causing material loss to

someone by committing the aforementioned crimes (Art. 49); the attempt to commit these crimes (Art. 50). The same law also criminalises child pornography (Art. 51).

In addition, Article 52 of Law 161/ 2003 considers the failure to respect Article 41 ("Owners or administrators of computer systems to whom access is prohibited or restricted for certain categories of users have an obligation to warn users about the legal conditions of access and use, as well as about the legal consequences of unauthorized access to these computer systems. The warning must be accessible to any user.") a misdemeanour, punishable with a fine.

The country's commitment to tackling cybercrime was reinforced in 2011 when the Romanian Government created the National Computer Security Incident Response Team – CERT-RO (in Romanian: *Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică – CERT-RO*), an independent research, development, and expertise centre on cybersecurity. In 2013, Romania adopted a National Strategy on Cybersecurity, which also included the creation of the National System for Cybersecurity (in Romanian: *Sistemul naţional de securitate cibernetică - SNSC*), a general framework on cross-sector cooperation in the field which reunites public authorities and institutions and representatives of industry.

Furthermore, in July 2020 Law 217/ 2003 on the prevention and combatting of domestic violence was amended and cyber violence was included among the recognised forms of domestic violence, alongside verbal, physical, sexual, psychological, economic, spiritual, and social violence. According to Law 217/ 2003, cyber violence is defined as "online harassment, online hate speech, online stalking, online threats, non-consensual publication of information and intimate graphic content, illegal access to interception of communications and private data and any other form of misuse of information technology and communications via computers, smartphones or other similar devices that use telecommunications or connect to the Internet and may transmit and use social or e-mail platforms for the purpose of embarrassment, humiliation, intimidation, threaten or silence the victim."[36] It is important to note that these provision refer to intentional actions or inactions that

[36] Article 4 (h) of Law 217/ 2003, amended through Law no 106 of July 3, 2020.

include any of the forms of violence mentioned above and which occur "in a domestic or family environment, among spouses former spouses, between partners or former partners, regardless of whether the aggressor resides or has resided with the victim" (Art. 3).

Last but not least, at the moment of the completion of the current policy paper, a proposal to sanction **non-consensual pornography** (or so-called "revenge porn"[37]) was being analysed in the Romanian Parliament. The proposal seeks to amend Article 226 of the Criminal Code (the violation of private life), to include sanctions for **non-consensual pornography**, and it was adopted by the Senate on October 21st, 2019, and subsequently sent to the Chamber of Deputies for debate. According to the legislative proposal, sharing, presenting or transmitting intimate images, regardless of the means used, of a person without their consent may carry a prison sentence of between 3 months to 2 years or may be sanctioned with a criminal fine.[38]

2.3. Germany

With the entry into force of the Cybercrime Convention in Germany on July 1st, 2009, German criminal law was adapted to the current developments in the area of internet and computer crimes, as well as to the Lanzarote Convention and to the EU legislation on that matter. In that sense, cybercrimes were mainly included in the German Criminal Code (StGB), showing fewer dispersed provisions on cyber-related offences.

The following illustration provides an overview of cyber-dependent and cyber-enabled offenses in the Criminal Code (StGB):

1) Cyber-dependent offences that specifically require ICT for its perpetration:

[37] The author recommends against the usage of the terms "revenge porn", as this implies that the victim is at fault and the perpetrator is disseminating the material as a form of punishment. Additionally, "porn" implies material produced for a wider audience and/ or to elicit sexual arousal, while in many of these crimes the purpose is mainly to control and abuse the victims. Therefore, the preferred terminology is "non-consensual distribution of sexual material".

[38] For more information about the draft bill on non-consensual pornography, go to https://www.senat.ro/legis/lista.aspx?nr_cls=L512&an_cls=2019 (accessed July 28th, 2020).

- §202a StGB Data espionage - The unauthorised provision of access to data that is not intended for the perpetrator and that is specially secured against unauthorised access, while overcoming access security;
- § 202b StGB Interception of data / Phishing - The unauthorised procurement of data from a non-public data transmission or from the electromagnetic radiation of a data processing system using technical means;
- § 202c StGB Acts preparatory to data espionage and phishing - The preparation of an o. G. Criminal offense by producing, procuring, selling, transferring, distributing or making passwords, security codes or computer programs available, the purpose of which is to commit such an offense;
- § 202d StGB Data theft - The creation, transfer, dissemination or making available to yourself or of another of data which is not generally accessible and which has been obtained by another person from an unlawful act with the intention of enriching yourself or a third party or harming another;
- § 269 StGB Forgery of data intended to provide proof - Saving or modifying relevant data for deception in legal transactions, so that if they were perceived there would be a fake or falsified document, or the use of such data;
- § 270 Meaning of deception in the context of data processing;
- § 303a StGB Data tampering - The illegal deletion, suppression, rendering unusable or changing data;
- § 303b Computer Sabotage - The significant disruption of data processing that is essential to someone else:
    - Inspection of a data change (§ 303a);
    - Entering or transmitting data with the intention of causing another disadvantage;
    - Destruction, damage, rendering it unusable, removing or modifying a data processing system or a data carrier.

2) Cyber-enabled offences that can be facilitated by information and communication technology, albeit not exclusively committed by those. In this regard, German Criminal Code lays down some offences that specifically mention the use of computers as a means of committing the crime, such as:

- § 206 Violation of the postal and telecommunications secret
- § 263a Computer fraud
- § 265a Obtaining services by deception
- § 86 Dissemination of propaganda material of unconstitutional organisations
- § 88 Sabotage against the constitution (regarding interference with critical infrastructures)
- § 201a Violation of intimate privacy by taking photographs
- § 238 Stalking
- § 176 (2) child abuse, specifically child grooming
- § 184d Distribution of pornographic performances by broadcasting, media services or telecommunications services

The Criminal code also establishes other ICT-related criminal offences despite not expressly stating so but through a reference to § 11 (3) of the Criminal Code, which sets out a general provision of equivalence: "*For the purposes of this law, audiovisual media, data storage media, illustrations and other depictions shall be equivalent to written material in the provisions which refer to this subsection*."[39] In this context, in sections which do not envisage the use of ICT but instead refer to section 11 (3) as a means of perpetration, ICT shall be considered as an equivalent method of perpetration of that offence. Some examples of those:

- § 91 Encouraging the commission of a serious violent offence endangering the state, ex vi 11(3)

[39] This provision is currently under review and will be adapted to the new challenges of cybercrime. In the Government Draft of the law from September 4th, 2019, section 11(3) reads as follows: „Contents within the meaning of the provisions referring to this paragraph are those which are contained in writings, on sound or image carriers, in data storage media, illustrations or other embodiments or are transmitted independently of storage by means of information or communication technology". The law has not yet been adopted.

- § 130 Incitement to hatred, ex vi 11(3)
- § 131 Dissemination of depictions of violence, ex vi 11(3)
- § 176 (4) 3 child abuse, presents a child with written materials (section 11(3)) to induce him to engage in sexual activity, ex vi 11(3)
- § 184b Distribution, acquisition and possession of child pornography, ex vi 11(3)
- § 184c Distribution, acquisition and possession of juvenile pornography, ex vi 11(3)

3) Meanwhile, the term cybercrime in a broader sense extends to almost all offences where the Internet is used to commit them.

The following list makes no claim to completeness, but merely mentions the most prominent offences. Cybercrime is developing very quickly and the way it is handled must therefore be constantly adapted.

- § 253 of the Criminal Code, blackmailing;
- Copyright violations under the German Copyright Act;
- § 284 of the Criminal Code, Unauthorised organisation of a game of chance;
- Drug Trafficking under the German Federal Narcotics Act;
- Arms Trade under the German Weapons Act;
- White-Collar crimes.

In addition to the StGB provisions on computer-related crimes, there are other legal instruments which play a crucial role when investigating and detecting cyber offences, namely:

1) The Telecommunications Act (TKG) reinforces privacy in the context of telecommunications and establishes retention periods for certain types of data, as well as an obligation to report acts that may jeopardize the privacy of communications. The most relevant sections for the purpose of this policy paper are the following:

- § 109a data and information security – establishes an obligation to report in case of possible data protection breach

- § 113b Obligations to store traffic data - this section lays down an obligation to store traffic data up to 10 weeks and location data up to 4 weeks, excluding the content of communications, data about websites accessed and data from electronic mail services. After this period, data shall be permanently deleted.
- § 113c (1) Use of data – stored data can be transmitted to a LEA insofar as the transfer is based on a legal provision that allows it to collect the data specified in section 113b for the prosecution of particularly serious crimes;

In respect of § 113b, it shall be noted that the validity of this section has been called into question since the German Federal Administrative Court (*Bundesverwaltungsgericht*) decided to refer to the European Court of Justice on 09/25/2019 in order to clarify whether the German data retention law is compatible with Union law.[40] Beforehand, the Higher Administrative Court for the State of North Rhine-Westphalia had rendered a judgment on June 22nd 2017, where it ruled that Internet Service Providers (ISPs) are not obliged to store the telecommunications traffic data specified in § 113b (3) TKG until the main proceedings have been legally concluded.[41] This appears to mean that in the meantime, no fine proceedings can be initiated against the service providers for failure to implement the storage obligation.

On the other hand, on the basis of § 100g of the Code of Criminal Procedure (StPO), the criminal prosecution authorities can collect traffic data from telecommunications companies if there is initial suspicion and a corresponding court order. However, this only applies to data that will be collected in the future and to data that is still stored at the time of the inquiry, for example because it is still needed for business reasons.[42]

[40] https://eucrim.eu/news/federal-administrative-court-refers-german-data-retention-law-european-court-justice/ and https://www.bverwg.de/pm/2019/66

[41] https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html

[42] https://www.bundesgerichtshof.de/DE/Bibliothek/GesMat/WP18/V/Verkehrsdaten.html

2) Telemedia Act (TMG) also sets out data security provisions and obligation to report in case of data breach or illegal access, upon their knowledge or awareness (§ 13 (7) and § 15a, respectively)
3) IT Security Act (IT-Sicherheitsgesetz)[43] gives jurisdiction to federal prosecutors to investigate crimes under sections 202a, 202b, 202c, 263a, 303a e 303b of the StGB and generally reinforces the national strategy on cybersecurity. Additionally, it sets out an obligation upon the BSI (Federal Office for Information Security) to periodically communicate to end-users about digital threats, information on security gaps, malware, attempted attacks, as well as the procedure adopted in the process.
4) Network Enforcement Act (Netzwerkdurchsetzungsgesetz – NetzDG) came into force in 2017 and aims at combating dissemination of illegal contents and fake news in social networks. In this sense, it deems illegal the display of contents concerning sections 86, 86-A, 89-A, 91, 100-A, 111, 126, 129 to 129-B, 130, 131, 140, 166, 184-B in conjunction with sections 184-D, 185 to 187, 201-A, 241 and 269 of the StGB, in addition to place an obligation upon the social network to regularly provide information on illegal contents though a publicly accessible report (§ 2). Finally, it sets out obligations to block and take down manifestly illegal content in 24h upon the knowledge of it (§ 3 (2) 2), whereas the general rule is to block or take down illegal content in a 7-day period (§ 3 (2) 3) and to submit that decision to the monitoring agency § 3 (2) 3 b). In case of taking down illegal content, it shall be preserved for the purposes of evidence during a period of 10 weeks (§ 3 (3)).[44]

[43] At the present moment, an amendment to this law is being voted at the parliament, so called IT-Sicherheitsgesetz 2.0. This draft bill envisages a change of tactics in the fight of cybercrime, namely from defensive to offensive, through the use of different IT tools (such as the ability to hack unsafe systems and have data deleted remotely). Besides, it intends to aggravate penalties of sections 202a, 202b, 202c, 202d, 303a e 303b StGB. Lastly, it criminalises two new conducts under sections 200e and 202f (non-authorised use of ICT systems and particularly serious offence against the secrecy and integrity of ICT systems.

[44] The Network Enforcement Act is currently under review and will be amended. The German Parliament and Council have already consented, but the law has not yet entered into force. The new law will include an obligation of social media operators to pass on relevant data to police forces. Aims are: strengthen user rights, make reporting channels more user-friendly, Simplifying the enforcement of information claims and Increase the informative value of transparency reports.

German Criminal Code of Procedure (StPO) establishes some essential procedural laws to the investigation of cybercrimes:

- § 94 e § 98 general seizure of tangible property which includes computer systems and data
- § 95 duty to hand over relevant tangible objects for evidence in criminal proceedings
- § 100g real-time interception of traffic data has to comply with the requirements laid down in this section. Besides, it also sets out the list of serious crimes that allow the collection of data pursuant to § 113b TKG
- §§ 100a e 100b interception of telecommunications or data collection in real-time, upon request of the prosecutor followed by a court order
- Online research and the use of spywares is generally prohibited, unless in the cases described in § 100b.
- §§ 110 (3) research and access to remote storage systems if they are somehow connected to the main one who is under investigation
- § 100j in conjunction with § 113 TKG set out the obligation of service providers to to provide information or to transfer data to competent authorities

Germany's Strategy on Cybersecurity 2016, continues pursuing the objectives set out in 2011 Strategy, in addition to four new branches of intervention; safe and self-determined action in a digitised environment; joint mandate of the State and companies; robust and sustainable nationwide cybersecurity plan and Germany's active positioning in European and international cybersecurity policies.

3. Current challenges and future projections. Portugal, Romania, and Germany

Despite all legislative and policy efforts to tackle cybercrime at national, European and international level, many difficulties and challenges remain. Some of these challenges are related to the effective application of the rule of law in practice, whereas others relate to technical and human factors.[45]

In this connection, the investigation of cybercrime is particularly difficult for several reasons pointed out *infra*.

The main challenges identified at the EU level are:

- Confliction between legal frameworks across MS regarding crucial matters due to inexistence of EU legislation, such as:
  - Data retention lawfulness
  - Where it is allowed, periods of data retention vary
  - Procedural rules as to cybercrime investigation
  - Detection and investigation tools vary widely from MS
  - Different definitions of crimes
  - Blocking mechanisms vary

[45] Information of this chapter is mainly retrieved from Conclusions of Expert Workshop on the implementation of Article 25 of Directive 2011/93/EU, organised by the European Commission on 19 June 2019; Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final, Brussels, 13.9.2017; ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends, January 2019; Common challenges in combatting cybercrime, Europol & Eurojust Report, June 2019; Payment Threats and Fraud Trends Report 2019, European Payments Council; Research Agenda the Human Factor in Cybercrime and Cybersecurity, Rutger Leukfeldt (editor), Eleven International Publishing, 2017; Liability for Artificial Intelligence and other emerging digital technologies, Report from the Expert Group on Liability and New Technologies – New Technologies Formation, Publications Office of the European Union, © European Union, Luxembourg 2019; Human Factor Report ProofPoint 2019; Cybersecurity in Portugal: Risks and Conflicts Report, National Centre for Cybersecurity, June 2020; Internet Organised Crime Threat Assessment, European Cybercrime Centre EC3, Europol 2019; ECSO Barometer 2020: "Cybersecurity in light of Covid-19", Report on the results of surveys with ECSO members and the cybersecurity community, © European Cyber Security Organisation (ECSO), 2020.

- Which all leads to legal uncertainty and hampers investigations and positive outcomes across MS;
- Lack of clarity as to cybercrime investigations in compliance with fundamental rights;
- Lack of understanding regarding the impact of cybercrime on victims;
- Lack of European capacity on assessing the encryption of products and services used by its citizens within the digital market;
- Lack of technical mechanisms to combine national, EU and international high-quality hash databases – that are crucial to detect automated illegal content and remove it quickly;
- Deficiency of international cooperation with third countries, for instance, disclosure rate of big US service providers in response to requests from European criminal justice authorities fell short of 60 % in 2017;[46]
- Imminent expansion of terrorism networks and activities across online platforms;
- Vacuum of legislation regarding IoT.

Portugal, Romania, and Germany

The prosecution of cybercrimes faces increasing difficulties in executing the computer analysis necessary to the investigation since these crimes are becoming more and more complex and demand very powerful tools and/or equipment for data processing.

In the case of **Portugal**, even though the Portuguese General Prosecutor's Office has contracted access to powerful tools to execute computer analysis, they are still not enough to meet the demands of criminal investigation that, in many cases, involve the analysis and cross-referencing of several Terabytes of data. Furthermore, difficulties in the investigation also arise from a constant "race against time" to obtain pertinent data. This becomes even more difficult because although the abovementioned Law 32/2008 offers the possibility of an extension up to one year when a "serious

[46] P8_TA(2017)0366, The fight against cybercrime, European Parliament Resolution on the fight against cybercrime (2017/2068(INI)) (2018/C 346/04), 3 October 2017.

crime" is under investigation, the general suppletive rule is to keep IP records for a six months period.

In accordance to the Portuguese Law that sets the organisation of criminal investigation, the Criminal Police (*Polícia Judiciária*) has the sole competence to investigate *stricto sensu* cybercrimes, whilst the other police forces (GNR, PSP and other) have the competency to investigate crimes committed through computer means.

Public Prosecution Service advise LEA to adopt the following measures to ensure that they collect as much evidence as possible and that they provide the necessary information to the victim: (i) Collect a detailed statement from the victim, as well as any communications they exchanged with the offender (with the technical headers and mention of the respective time and date), and any additional information that they possess and may allow the identification of the perpetrator; (ii) Collect and print the content of the websites or social network profiles, mentioning the date and URL's; (iii) Request that the plaintiff provides any relevant bank information; (iv) Inform the victim that he/she should preserve the communications and other relevant files in his/her computer, and that he/she should change the passwords of the systems illegally accessed by the perpetrator

Finally it should be highlighted that the Portuguese Public Prosecution Service has been able to secure agreements with several companies that allow prosecutors to obtain data from Apple, Facebook, Skype, Instagram, YouTube, Microsoft and Blogger in a more expedite manner (specifically, without resorting to international judiciary cooperation).

In the case of Romania, the criminal investigation of fraud committed through computer systems and means of electronic payment (Art. 249-251 of the Criminal Code) and for child pornography is conducted by the Prosecutor's Office of the Court of First Instance (in Romanian: *Parchetul de pe lângă Judecătorie*), the latter being charged with the administration of justice for these crimes. For offenses against the security and integrity of computer systems and data (Art. 360-365 of the Criminal Code), criminal investigation is carried out by the Prosecutor's Office of the Tribunal (in Romanian: *Parchetul de pe lângă Tribunal*), with the legal disputes settled by the Tribunal. If the

aforementioned offenses involve organised crime, they are investigated by DIICOT – Directorate of the Investigation of Organised Crime and Terrorism (in Romania: *Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism*). In addition, investigation is also carried out by the police, concretely by the Criminal Investigation Service of the County Police Inspectorate, which includes judicial police agents that are subordinated to prosecutors from the Prosecutor's Offices attached to the Courts of First Instance and Tribunals. The Directorate for Combating Organized Crime is the specialized structure within the General Inspectorate of the Romanian Police, which is subordinated to the territorial structures of DIICOT. Within the Directorate functions the Service for Combating Cybercrime which comprises 4 offices: Office for Combating Cybercrime and Crimes with Means of Payment, Office for Searches and Investigation of Information Systems, Office for the Investigation of Crimes against Information Systems, Office for the Investigation of Child Pornography through Computer Systems.

While LEA are generally well prepared to tackle cybercrime, although understaffed, prosecutors and judges are often not. With the growing complexity and number of cybercrimes, it is a challenge to ensure continuous specialist training to magistrates in Romania. There are also issues with awareness among the general population about the nature and consequences of cybercrimes, and public campaigns on the issue continue to be scarce. For instance, the authors identified only one awareness campaign conducted by the Romanian Police on cybercrimes: a campaign against malware, implemented in 2016 at EU level.[47] A third challenge concerns support for victims of cybercrime. In April 2019, Romania took steps to ensure support (legal and psychological counselling, social assistance) for all victims of crime[48], thus including victims of cybercrime, by mandating the creation of generic victim support services within the county social services (*DGASPC – Direcția Generală de Asistență Socială și Protecția Copilului*). However, these services were not fully functional by the time the current report was finalised, meaning that throughout the country support is available mostly to child victims, victims of domestic violence, and victims of human

[47] For more information about the malware campaign, go to https://www.politiaromana.ro/ro/prevenire/campanii-proiecte/campania-de-informare-mobilemalware.
[48] See Emergency Ordinance no. 24/ 3 April 2019 amending Law 211/ 2004 on the protection and support of victims of crime.

trafficking, as these categories are perceived as more vulnerable. Moreover, even when generic support will become available, the staff providing these services need to receive specialist training on cybercrimes. With regard to victims of child pornography, the Police does not refer them to ANITP – The National Agency against Human Trafficking (in Romanian: *Agenția Națională Împotriva Traficului de Persoane*), which may conduct an initial needs assessment, provide support and further refer victims to other services.[49] Better cooperation should be instated between these entities in order to provide better support for victims, as well as to improve data collection and reporting, including at an international level, with ANITP being the official rapporteur at an international level of cases of human trafficking.

In the case of **Germany** the prosecution of cybercrimes also face difficulties, since these crimes are becoming more and more complex thus demand strong countermeasures. In terms of dealing with this phenomenon, the new police division "Cybercrime" (CC) has been established inside of the German Federal Criminal Police Office (BKA - Bundeskriminalamt) in April 2020. In addition to classic central office tasks such as coordinating the international exchange of information on this phenomenon, the new department will expand their analysis competence of the BKA. An example would be, on how to deal with new cybercrime phenomena and digital attack patterns. Investigations against criminal activities, networks and structures are going to be increasingly managed here. Networking at national and international police levels will become just as important as cooperating with a wide range of actors as well as other authorities and businesses.[50]

Germany continues to be an attractive target for cybercriminals. To make reasonably valid statements on the actual dimension of cybercrime and to be able to combat cybercrime effectively, law enforcement/prosecution and security authorities are required to initiate various measures considering personnel, financial and, above all, technological aspects, such as the teaching of basic skills, additional basic and advanced training and the provision of appropriate hardware and software. Enhanced co-operation with research institutes and the private sector may also contribute

[49] According to Law 678/2001 on preventing and combating human trafficking, Art. 2 Let. c, victims of child pornography are assimilated with victims of human trafficking and are granted the same rights as the latter.
[50] press release of the German Federal Criminal Police Office (BKA - Bundeskriminalamt)

to clearing up (at least some) undetected cases of cybercrime. The users themselves are also encouraged to ensure the security of their technical devices and to avoid careless disclosure of information on the Internet. In this context, it is imperative that users obtain relevant information and become acquainted with instruments and measures that will help them to protect themselves from attacks of various kinds.[51]

Despite all legislative and political efforts to combat cybercrime domestically, some difficulties and challenges remain transversal to Portugal, Romania and Germany. In that sense, the investigation of cybercrime is particularly difficult for several reasons:

- The complexity of the tools considered necessary to carry out computer analysis;
- The short legal basis for Internet service providers to keep records of data, crucial for the preservation of evidence in cybercrime;
- Lack of systematic procedures for the timely collection of evidence;
- Rapid transnational cooperation with countries hosting illegal content;
- National borders are of no relevance or importance in this specific crime phenomenon. It is all the more necessary to further expand national and international co-operation;
- General difficulties in implementing Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse, sexual exploitation of children and child pornography.

All in all, the **following findings provide an overview of challenges of different nature**, faced by law enforcement and judicial agencies, as well as other relevant stakeholders, in tackling cybercrime.

N.B.: Unless otherwise specified, the following challenges apply to Portugal, Romania, and Germany.

i) Rule of law challenges

[51] Cybercrime, National Situation Report 2018, page 53.

The ever-growing and fast development of technologies makes it not only difficult for states to keep up with it, but it has been also calling into question some European fundamental principles, such as the rule of law.

In this context, the boundaries between cybercrime, cyber espionage, and the tools used by states to tackle cyber-attacks are getting more and more blurred, posing considerable difficulties when ensuring fundamental rights and freedoms.

If states must be equipped with the adequate technological tools to effectively counter cyber-attacks and therefore protect their citizens, on the other hand questions are being raised whether fighting cybercrime by using the same tools as cybercriminals, even though for different purposes, can be legitimately accepted as a lawful and proportionate limitation to one's right to privacy.

Furthermore, blocking measures and removal of contents that are deemed as illegal may be questioned as an unlawful curtailment of one's freedom of speech, worsen if it is done by private entities such as ISPs.

Some practical examples of these difficulties are:

- Blocking and removal of illegal contents depends on a court order unless it is manifestly illegal, thereby increasing significantly the time that the content is still online;
- Difficulties in the implementation of Article 25 of Directive 2011/93/EU for possible encroachment with fundamental rights;
- More advanced tools of investigation, such as hacking techniques;
- Challenges regarding access to stored computer data ('cloud evidence'), as it could result in unregulated remote access to servers and computers located in other jurisdictions by LEA, which, in turn, could amount to a violation of the right to privacy and a breach of the principle of territoriality/sovereignty;
- Online misinformation and disinformation campaigns, fake news on social media aimed at undermining democratic processes and European values;

- Government's unwillingness to share cybersecurity-relevant information as it could result in undesired disclosure of national security vulnerabilities or operations, which could result in interference in the principle of sovereignty.

Bearing in mind that these challenges cannot remain unaddressed for the sake of democratic values, such as public safety and the prevention of crimes, solutions have to be studied and put in place. In any case, adequate procedural safeguards shall be ensured, as well as the respect for fundamental rights, namely the right to privacy, the right to fair trial, freedom of speech and ultimately the principle *in dubio pro reo*.

ii) Law enforcement and judicial community challenges

Law enforcement and judicial agencies face great challenges in the investigation of cybercrime, which has a twofold effect; on the one hand these challenges prevent effective investigations and consequently also victim's redress, and on the other hand they give rise to impunity, which, in turn, encourages the perpetration of crime. In this sense, sturdy law enforcement mechanisms and investigations are therefore crucial in deterring cybercriminals.

Here can be found some practical examples of challenges faced by law enforcement and judicial agencies:[52]

- <u>The loss of data</u>
  - Access to data is limited or denied;
  - Where data can be stored, there is a short legal basis for ISPs to keep records of pertinent data crucial for evidence;
  - The overturning of the Data Retention Directive in 2014 and the implementation of the General Data Protection Regulation (GDPR) gives rise to uncertainty of procedural rules as to digital evidence, and in some cases may cause investigation to be discontinued or delayed;

[52] The criteria formulated by Europol Common challenges in combatting cybercrime, Europol & Eurojust Report, June 2019 is adopted.

- Implementation of carrier-grade network (CGN) address translation technologies by ISP results in often excessively large volumes of data (as one IPv4 address may be shared by multiple end-users at one);
- Old tools are not able to tackle new methods: Criminal abuse of encryption technology, anonymisation via VPNs or Tor and obfuscation of digital evidence renders lawful interception ineffective;
- Fast moving content of CSEM.

- The loss of location
  - Difficulties in traceability and attribution of cyber offenses: the use of encryption and/or anonymisation tools, crypto-currencies and the Dark Web, as well as the growing use of cloud-based technologies, have also led to situations in which law enforcement can no longer establish the physical location of perpetrators, criminal infrastructure or electronic evidence;
  - Anonymous Web Hosting Provider shields websites' owners from being identified;
  - Use of CGN technology by ISP seriously jeopardises investigations as it makes it technically impossible to determine the IP address;
  - Territoriality-based investigative powers and jurisdiction of the competent national authorities offer no appropriate tools to tackle cross-border cybercrime nature.

- Challenges associated with national legal frameworks
  - Differences between domestic legal frameworks in the MS:
    - Divergent definitions and categorisations of CSEM-related crimes;
    - Blocking mechanisms are not uniformly approached;
    - Divergent definitions of cyber-related offenses (criminalisation of conduct);
    - Different forensic procedural law and thus divergent procedures for the gathering of e-evidence in cybercrime investigations;
    - Divergence between detection and investigation tools;

- Lack of procedural guidelines on how to carry out investigations taking into account a victim-centred approach;
- The lack of international binding instruments with obligations for companies regarding sharing of information with LEA and judicial authorities of other states continues to be a serious impediment to the international criminal investigation and prosecution of cybercrime."

- Obstacles to international cooperation
  - Lack of common legal framework for international cooperation, such as on expedited sharing of evidence;[53]
  - Mutual Legal Assistance is perceived as too slow to gather and share electronic evidence effectively;
    - Lack of law enforcements ability to respond to large-scale cyber-attacks, particularly where multiple industries across a range of sectors and geographies are affected.

- Challenges of public-private partnerships
  - Lack of a comprehensive legal framework to facilitate effective and trust-based cooperation as a well-oiled machine with the private sector;
  - Lack of clarity regarding legal and transparency issues surrounding cooperation with industry and particularly regarding industry's active role in fighting cybercrime
  - Criminal misuse of technology; technologies such as quantum computing and AI (e.g. facial recognition) may be deployed at both ends of the lawful spectrum.

- Challenges associated with the system and the personnel
  - Lengthy court proceedings;
  - Lack of solid human expertise on CSEM and other cyber-related offences;

[53] See, for example, https://www.bakermckenzie.com/en/insight/publications/2019/10/uk-us-data-access-agreement

- Lack of technical tools to effectively pursue law enforcement;
- Very complex tools and means deemed necessary to run computer analysis;
- In the case of Romania and Germany, the understaffing of LEAs charged with the investigation of prosecution of cybercrimes, including CSEA.

- Challenges associated with victimisation of cybercrime
  - Lack of understanding of the nature, extent and impact on victims which not only hinders prevention of crime but also limits comprehension of cyber-attacks;
  - Lack of understanding of consequences for society at large.

iii) Cyber resilience challenges

As societal degree of digitalisation continues to rise, cyber-resilience shall follow since humans are often considered as the weakest link in cybersecurity.[54]

The generalised access to internet, the amount of time spent online, the diversified purposes why people make use of internet (ranging from information finding activities to social networks, shopping, gaming, online banking, e-governance, etc.) are circumstances that increase the chances of ever experiencing a cyber offence.

In fact, some routine activities seem to be related to a higher risk of cybercrime victimisation, such as being online more, opening attachments from unknown sources, clicking on pop-ups, internet banking, online purchase and not having up-to-date antivirus software.[55] This understanding highlights the need for improved cyber resilience as poor digital literacy poses enormous threats to cybersecurity. There is therefore a human dimension to cyber threats, and it is urgent to address it

[54] Research Agenda the Human Factor in Cybercrime and Cybersecurity, Rutger Leukfeldt (editor), Eleven International Publishing, 2017, p. 50.
[55] Research Agenda the Human Factor in Cybercrime and Cybersecurity, Rutger Leukfeldt (editor), Eleven International Publishing, 2017, pp 48-49.

by improving understanding of the risks and increasing awareness, thus educating cyber resilient citizens.

Some examples of challenges in this regard are pointed out *infra*:

- Lack of digital literacy due to the drastic boom of internet's access and use;
- Lack of awareness about cybersecurity and human error;
- Lack of awareness about cybercrime's seriousness;
- Increasing self-generated exploitation material mostly driven by growing access of minors to high quality smartphones and a lack of awareness of the risks;
- Increased vulnerability of children due to access to internet earlier in life;
- Lack of public and individual awareness about sexual duress and extortion offences, which leads to victims feeling guilt and shame and prevents reporting;
- Lack of public and individual awareness about other cyber-related offences, such as property offences, which leads to victims feeling guilt and shame for being misled and prevents reporting;
- Lack of enlightenment on reporting vs. perpetrating a crime, particularly misconceptions about which acts constitute in fact a crime, which in turn also contributes for underreporting;
- Underreporting issue (private persons and organisations), which not only leads to impunity but is also detriment for a better understanding of the phenomenon;
- Lack of insight into the economic factors (costs and benefits) and the psychological factors (emotions and attitudes) that influence willingness to report crimes by individuals as well as organisations;
- Lack of understanding of cybercrime impact on victims;
- Lack of specialised training for carers, teachers, media regarding prevention of CSEM;
- Lack of human expertise within civil society organisations and SME that may not have dedicated personnel and technology to deal with requests for removal;
- Lack of information dissemination about cyber threats and cyber resilience tips by broadcast media;

- Insufficient financial, technical and human resources deployed in cybersecurity;
- Research on factors that may contribute to the long-term effectiveness of technical security measures, awareness campaigns, education and training programs is lacking.

iv) Cooperation challenges

Bearing in mind the cross-border dimension of cybercrime, traditional internal relations and frameworks seem no longer suitable for tackling it. In this context, principles of sovereignty and territoriality hamper effective investigations of crimes that know no physical boundaries, and therefore evidence cannot be found in a motionless location due to internet particular traits. As a result of the fast movement of online contents, a swift transnational cooperation with countries hosting illegal contents is crucial.

Moreover, cooperation presents other challenges, namely cooperation between law enforcement and industry and multi-sector cooperation.

Some cases in point are the following:

- Fast moving content of CSEM;
- Online information can be located in different places at the same time;
- Bulletproof hosting (if hosting services are located outside Europe);
- Array of sovereign jurisdictions gives rise to legal uncertainty as it makes it harder to ascertain the applicable law;
- Confliction between different legal frameworks at the EU level
    - Precautionary storage of data: uncertainty of procedural rules as to digital evidence since data retention provisions are in question or have been abolished in several EU countries;
    - Different limitation periods of data retention;
    - Divergent legal definitions of CSEM-related crimes and of cyber-related offenses among EU' MS;

  - Divergent forensic and procedural rules for cybercrime investigation;
  - Blocking mechanisms are not uniformly approached in different MS, resulting content that is blocked in some MS but not in others;
- Lack of mechanisms to combine national, EU and international high-quality hash databases – that are crucial to detect automated illegal content and remove it quickly;
- General difficulties in the implementation of Article 25 of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography;
- Difficulties with channelling legal requests to ISPs outside MS's jurisdictions caused by a lack of hotlines in a number of 3rd countries
- Governments' and public authorities' unwillingness to share cybersecurity-relevant information for fear of compromising national security or competitiveness;
- Problems in exchange of information and cooperation between different key-actors at the national level, e.g. LEA, judicial bodies, industry, academia, NGOs;
- Private companies are reluctant to share information on their cyber vulnerabilities and resulting losses for fear of compromising sensitive business information, risking their reputation or breaching data protection rules.

4. Policy discussion and recommendations

Due to the complexity of cybercrime nature, evolution and cross-border dimension, it has never come in more useful the motto "Think globally, act locally". As the internet knows no borders, cybercrime spreads to all areas of crime and presents overreaching impacts; on victims, states, sovereignty, democracy and rule of law, fundamental rights, critical infrastructures, banks, businesses and overall security and safety both at the public and individual level.

In this sense, it is urgent to re-shape relations between states, promote public-private cooperation and invest in people's awareness and education on cyber resilience in order to have in place a

coherent and comprehensive strategy to prevent cyber-attacks from entering our lives by means of eliminating all possible weakest leaks. The aim is to create a solid protection and response network at the domestic level and, ultimately, at the international level.

This holistic strategy shall be designed to achieve five main goals:[56]

1) To build cyber resilience among people;
2) To be able to anticipate possible security incidents;
3) To build strong protection;
4) To be able to recover quickly from any cyber-attack;
5) To have a deterrence effect on possible criminals.

For that purpose, this paper sets out some recommendations to be taken into account when designing cybersecurity holistic strategies.

4.1. Europe

Taking into account the abovementioned challenges, the following is recommended:

a) At the internal level:

- Legislation that regulates law enforcement presence and action in an online environment must be harmonised at EU level, which would allow for more effective joint operational actions such as large-scale botnet takedowns, or increased possibilities to monitor criminal activities online and to lawfully collect critical evidence on the Deep Web and Dark Web. That said, cohesion between MS regarding cybercrime tools and investigation rules must also be ensured by means of legislating on:
    - Data retention and digital evidence;

[56] Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final, Brussels, 13.9.2017. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en

  - Standardised procedural guidelines for investigations
  - Standardised investigative tools
  - Standardised blocking mechanisms
  - Common forensic standards across MS
- Bring clarity on how to carry out effective investigations of cybercrime without encroachment with fundamental rights, concerning investigation, procedural safeguards and due process rules, e.g. handbook on European law relating to cybercrime and fundamental rights will prove to be of immense added value; [57]
- Develop mechanisms to rapidly detect and take down online misinformation and disinformation campaigns aimed at undermining EU democratic values, respecting transparency principles and taking action against the criminals or companies behind;
- Invest in research on cybercrime and victimisation;
- Promote victim-sensitive approach;
- Set up a one-stop-shop at the EU level, for enlightenment and support of people and all relevant stakeholders, including states;
- Set up a comprehensive mechanism where CSEM hosted in a MS, detected by another MS, can be removed swiftly;
- Set up a European mechanism of blocking access, from any MS, to websites storing illegal content;
- Standardise judicial cooperation forms;
- Facilitate cross-border access to electronic evidence;
- Set up an electronic platform to exchange information within the EU regarding criminal investigations;
- Legislate on a framework for illegal contents posted on online platforms, namely social media platforms;[58]

[57] https://fra.europa.eu/en/project/2018/handbook-european-law-relating-cybercrime-and-fundamental-rights
[58] Cf. https://ec.europa.eu/digital-single-market/en/digital-services-act-package

- Implement standardised transparency reports among industry and relevant businesses across the Digital Single Market, in order to improve sharing of information;
- Development of common strategies, facilitating joint cyber defence training, EU taxonomies and standards;
- Invest in technology and development;
- Develop capabilities (human and technical) to address the needs for CTI (Cyber Threat Intelligence) knowledge management;[59]
- Increase independence from currently available CTI sources (mostly from outside the EU) and enhance the quality of CTI by adding a European context;
- Develop and share "baseline CTI", covering sectorial and low-maturity needs of organisations;
- Remove existing barriers to collect CTI
- Implement the collection and analysis of CTI, as crucial activity in the implementation of proper defence strategies;
- Deploy resources in capacity building of MS, ensuring strong protection, fast and effective responses and quickly recovering;
- Set up a liability framework for producers of vulnerable product/software concerning AI;[60]
- Regulate crypto currency;
- Regulate IoT;
- Create hubs for law enforcement and technology innovation;
- Research on the possible impacts of IoT;
- Study mechanism and approaches to counter the convergence of cyber and terrorism;
- Promote public-private cooperation, across industry, between MS;
- Facilitate cooperation and share of good practices between MS;
- Stronger public funding for research and innovation;

[59] ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends, January 2019.
[60] Liability for Artificial Intelligence and other emerging digital technologies, Report from the Expert Group on Liability and New Technologies – New Technologies Formation, Publications Office of the European Union, © European Union, Luxembourg 2019.

- Improve and shorten cycle from research to innovation to cope with potential new disruptive challenges;
- Increased need to raise awareness on cyber threats during the COVID-19 crisis, with emphasis on cyber risks, misinformation and disinformation;
- Advocacy and cyber resilience measures (networking, fostering strategic public-private partnerships and advocate for a reliable, safe and secure European IT support).

b) At the external international relations level:

- Use EU leverage for making robust alliances with third countries, in order to better articulate requests to ISPs outside MS jurisdictions;
- Build on good practices and invest in capacity building of third countries;
- Reinforce a joint diplomatic response from the EU MS with view of standard setting, by means of:
    - Leveraging European assets: focusing on investment, capacity-building & competitiveness and therefore standing as drivers of research, industrial innovation and data & privacy frontrunner;
    - Developing training, policy and legislation developments efforts;
    - Building rights-based capacity building model;
    - Reinforce principles of due diligence and state responsibility.

Strengths

- Executive power
- Legislative power
- Judicial power
- Financial power
- Regulatory power
- Well-Resourced
- Political, economic, technological and social leverage
- Cooperation facilitator
- Strong stakeholder input
- Single EU market – wide reach
- EU *acquis* on cybersecurity and cybercrime
- Strong position diplomatically with third countries
- Powers to conclude agreements with non-EU countries
- Horizontal expertise of MS cybersecurity policies
- EUROPOL
- Cooperation with INTERPOL

Weaknesses

- Lack of in-depth understanding regarding the impact of cybercrime on victims by the policy and decision makers
- Difficulties in the investigation of cybercrime
- Lack of procedural standardised guidelines for investigations
- Detection and Investigation tools are not standardised among the MS
- Confliction between different legal frameworks at the EU level
- Uncertainty of procedural rules as to digital evidence
- Blocking mechanisms are not uniformly approached in different MS
- Lack of European capacity on assessing the encryption of products and services used by its citizens within the digital market

Opportunities

- Transform weaknesses into opportunities
- Leverage European structures and powers to:
  - Foster digital literacy
  - Set up a liability framework for producers[61]
  - Develop a handbook on European law relating to cybercrime and fundamental rights[62]
  - Push MS forward enhancing digital literacy
  - Push MS to adopt victim-sensitive approach
- Leverage European assets and:
  - Increase R&I funding
  - Increase capacity building
  - Foster hub for law enforcement innovation
- Invest in Europe & foster strategic partnerships:
  - Promote public-private cooperation, across industry, between MS
  - ICT standardisation framework[63]
  - Standardisation of judicial cooperation forms
  - Platform to exchange information within the EU
  - Cross-border access to electronic evidence
  - Boost competitiveness and make Europe as the frontrunner of cybersecurity

Threats

- The Complexity of cybercrime's nature, evolution and dimension and its fast pace of development makes it hard for LEA and industry to catch up with:
  - Dissemination, detection, traceability, attribution of cyber offenses
  - Fast moving content of CSEM
  - Use of malware (ransomware, phishing, etc.)
  - Payment fraud
  - The criminal abuse of cryptocurrencies
  - DNS High jacking
  - IoT, 5G, AI (e.g. the ongoing improvements of so-called deepfakes), cloud services, quantum computing
  - Cross-cutting crime methods
  - Fast spreading to all areas of crime
  - Fast development of technologies; technologies available for investigation soon get obsolete;
- The criminal abuse of the dark web
- The convergence of cyber and terrorism
- The use of encryption, anonymization and obfuscating techniques
- Lack of cooperation between EU MS
- Lack of transnational cooperation with third countries
- Difficulties with channelling legal requests to ISPs outside MS's jurisdictions
- Online misinformation and disinformation campaigns (aimed at undermining EU democratic values)

[61] Liability for Artificial Intelligence and other emerging digital technologies, Report from the Expert Group on Liability and New Technologies – New Technologies Formation, Publications Office of the European Union, © European Union, Luxembourg 2019.

[62] https://fra.europa.eu/en/project/2018/handbook-european-law-relating-cybercrime-and-fundamental-rights

[63] https://ec.europa.eu/growth/single-market/european-standards/ict-standardisation_en

4.2. Portugal, Romania, and Germany

Having regard of the challenges faced in the Portuguese, Romanian, and German setting concerning prevention and fight against cybercrime, as well as victim's protection, the following policies are recommended.

It shall be noted, however, that some challenges mentioned concerning Europe also apply to the three Member States, hence a possible overlap in recommendations. In any case, a comprehensive interpretation shall be taken when examining both sets of recommendations.

1) Research and technology

Improving understanding of cybersecurity is crucial for designing effective solutions to tackle cybercrime. In that sense, academia and industry play a fundamental role in shedding light upon issues that are still not well-documented or researched due to the very complex nature and development of cybercrime.

Once there is a general better understanding of the phenomenon, policymakers, industry and civil society will be better equipped to deal with the actual and emerging challenges that stem from the use of ICTs. Consequently, research promotes change, development and sharing of good practices.

From the victim's standpoint, unless there is a better understanding of the phenomenon and its human dimension, prevention cannot be fully accomplished. That said, researching on the impacts of cybercrime on victims will not only improve the support given to victims but will provide adequate tools to effectively engage people in adopting safer behaviours. It is therefore of utmost importance to focus on victimology in the context of cybercrime in order to understand, effectively prevent and mitigate the effects of crime.

- Continue studying the evolving and ever-changing character of cybercrime *modi operandi;*
- Research to better understand attack practices, malware evolution, malicious infrastructure evolution and threat agent profiling;

- Study the impact of cybercrime victimisation on online behaviour, online risk perception and the risk of repeat victimisation;
- Conduct disaggregated studies, i.e., studies that look at the impact of cybercrime in specific groups, and if there are types of personality, such as impulsive people, that respond differently to victimisation than the average victim, in order to better understand patterns of repeat victimisation;
- End users' behaviour can, for example, be studied using log files;
- Study how security tools and processes can be designed in such a way that users are motivated and encouraged to act safely without interfering too much in their daily routines;
- Study the relation with psychological needs such as control, autonomy, efficiency and social constructs.
- Computer Telephony Integration knowledge management needs to be subject to standardisation, particularly regarding the developments of standard vocabularies, standard attack repositories, automated information collection methods and knowledge management processes.[64]

2) Raising awareness and specialised training

People are the major enabling factor of cyber incidents. In 2019, 99% of the malware attacks observed required at least some degree of human interaction to infect user devices. In fact, cyber criminals continue to resort to the use of social engineering methods, relying on human interaction to install malware, steal data and engage in other malicious activities. On the other hand, less than 1% of the attacks exploited system vulnerabilities.[65]

For that reason, it is paramount to increase cyber resilience and awareness on cybercrime and to ensure that victims have effectively access to information in order to prevent and mitigate impacts of crime. This holds true for all end-users, including people in general and personnel from

[64] ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends, January 2019.
[65] Human Factor Report, Proofpoint, 2019.

organisations that deal at some point with cyber threats, ranging from companies' staff to law enforcement and judicial agencies and the media.

Accordingly, based on collection of best practices that we can provide, it is recommended to take a people-centric approach in this regard, starting from adopting the following:

- Promote a comprehensive understanding of cybercrime among the general public and particularly among professionals and policy makers;
- Raising social awareness towards cybercrime, including its causes and consequences, through online and offline campaigns and materials dissemination, targeting the public, civil society, media, business community, research bodies and, particularly, schools;
- Raising special awareness and conduct preventive campaigns about CSEM for:
  - Children and youngsters on CSEM, by informing and empowering them to adopt safety online measures;
  - For carers and teachers in primary and secondary education in order to better deal with possible cyber incidents and to improve detection among their pupils;
- Mainstreaming cybersecurity education into school curricula when acquiring general digital competences;
- Increase digital literacy in every layer of society in order to broaden prevention behaviours and to develop cyber-safety protective habits while using the internet;
- Set up a one-stop-shop (a single portal providing information, offering advice on prevention, detection of malware, links to reporting mechanisms, links to victim support organisations (VSO) and specialised units and explanation of steps to take after falling victim of a cybercrime);
- Improving reporting by:
  - Training users to spot and report malicious email;
  - Raising awareness on victim's rights and ensuring that victim support services are widely known, namely the Specialised Unit to Support Victims of Cybercrime that will be created by APAV (in Portugal) and ACTEDO (in Romania);

- Ensuring that people and victims have effectively access to information, for instance, by setting up an online platform containing information on victim's rights and on the steps to take in case of victimisation, namely cybervictimisation;
- Empowering people with the enhanced possibility of being able to take part in the broader fight against cybercrime, through the adoption of digital best practices and the importance of reporting;

- Specialised and continuous training on CSEM specifically and other cyber offenses for:
  - Victim support officers;
  - Lawyers who want to represent victims of cyber offenses;
  - Law enforcement and judicial bodies, in order to improve the quality of investigations, the assessment of digital evidence and the judgments, therefore contributing to give clarity to the phenomenon and to end impunity;
  - Policy makers who design cybersecurity and cybercrime frameworks in all relevant areas (not only internal security and justice but rather in a broader scope, e.g. Education, Health, etc.)

3) Law enforcement, judicial agencies and justice system

Taking into account the challenges pointed out in this respect, there is an overriding interest in addressing those in order to conduct effective investigations, ensure and enforce victim's rights and redress, secure positive judicial outcomes and consequently end impunity and deter perpetration of new offences.

For that purpose, we set forth some recommendations, in addition to the others already made hereto:

- Adopting a victim-sensitive approach to criminal investigations show several advantages, namely:
  - Respects victim's rights and prevents secondary and repeated victimisation;

  - Promotes victim's cooperation, which consequently increases the quality of investigations (informed and rights afforded victims' are more cooperative as they feel more confident and aware of the importance of their role in the criminal procedure);
  - Promotes strict cooperation between LEAs and victim support services which also facilitates investigation;
  - Improves general understanding of cybercrime and of that particular *modus operandi*.
- Given the specialised training within the justice and law enforcement system, set up specialised units to investigate and to trial cases of CSEM and other cyber offenses;
- Ensure that LEA are provided with all the necessary tools to effectively conduct investigations, e.g. better processing tools for large amounts of data, cutting-edge technology, etc.;
- Invest more resources in these specialised units, namely technical and human resources;
- Provide more transparency regarding the legal framework for fighting cybercrime, viz. investigation tools and methods allowed;
- Provide simplification of the digital proof gathering regime (very important for e-mails);
- More flexibility in gathering testimonial evidence (Skype or other means) in order to avoid secondary victimisation;
- Ensure procedural safeguards when resorting to undercover methods;
- Adoption of necessary measures to combat cases of bullet proof hosting and to make such hosts compliant in different cases;
- Legal recognition of the role of entities such as NGOs in combatting the dissemination of children sexual exploitation materials, e.g. hotlines' attributions are not legally set out. However, were they given vaster competences due to their specialised training in detecting and taking down CSEM, investigations would be facilitated and streamlined, as well as it would reduce the time contents are still online. Lastly, it would also accelerate the full implementation of Article 25 of the Directive 2011/93/EU on combatting the sexual abuse and sexual exploitation of children and child pornography.

4) Cooperation

The pace of evolution of cybercrime requires joint efforts to tackle its overreaching effects. In this sense, there is a growing need for enhanced cross-cutting cooperation. This calls for the adoption of a holistic approach to cybercrime, promoting cross sector multidisciplinary interaction and collaboration; namely inter-state and cooperation between policy and governance, criminal justice system, victim and VSO, societal, industry and media and communications.

This synergy is of utmost importance as one key-actor by itself is not enough to prevent, counter and mitigate attacks. In this context, it is essential to highlight the role of VSOs. There are plentiful advantages in establishing strict collaboration with VSOs as they work in various fronts: prevention, supporting and mitigating impacts of victimisation. In addition, VSOs provide all relevant information on victim's rights and establish a trust relationship with them, which ultimately makes them more cooperative with justice system, hence enabling better judicial outcomes.

At the same time, VSOs also play a key-role in preventing secondary and repeated victimisation, by providing support in all phases of criminal proceedings and designing safety strategies with victims to avoid falling victim of new offences. In this respect, the impacts of cyber victimisation are especially devastating due to specific features of the crime and taking into account the speed of online content dissemination, difficulties in counter dissemination and in stopping immediately the offences, e.g. cyberbullying, cyberstalking, etc.

As to victims of cybercrime specifically, it is also relevant to point out the role of Safer Internet Centres. In **Portugal**, this helpline (LIS, *Linha Internet Segura* in Portuguese) has a twofold mission: Helpline and Hotline. The former aims at providing safety advice on the use of internet, information on cybercrime and on victim's rights, including methods to preserve digital evidence. The latter, on the other hand, has specialised training in detection and flagging illegal contents online. Due to this specialised competence, it is considered as a trusted flagger of various online platforms such as Facebook, YouTube, etc., and it has special protocols with LEA, which speeds up the process of taking down illegal content. In **Romania**, the corresponding hotline is managed by the NGO Save the

Children, who can be contacted via phone, email and Facebook by children and adults alike regarding concerns or issues related to the Internet or technology. In addition, due to an existing partnership with the Police, Save the Children is a civilian reporting hub for illegal cyber content and for CSEM.[66]

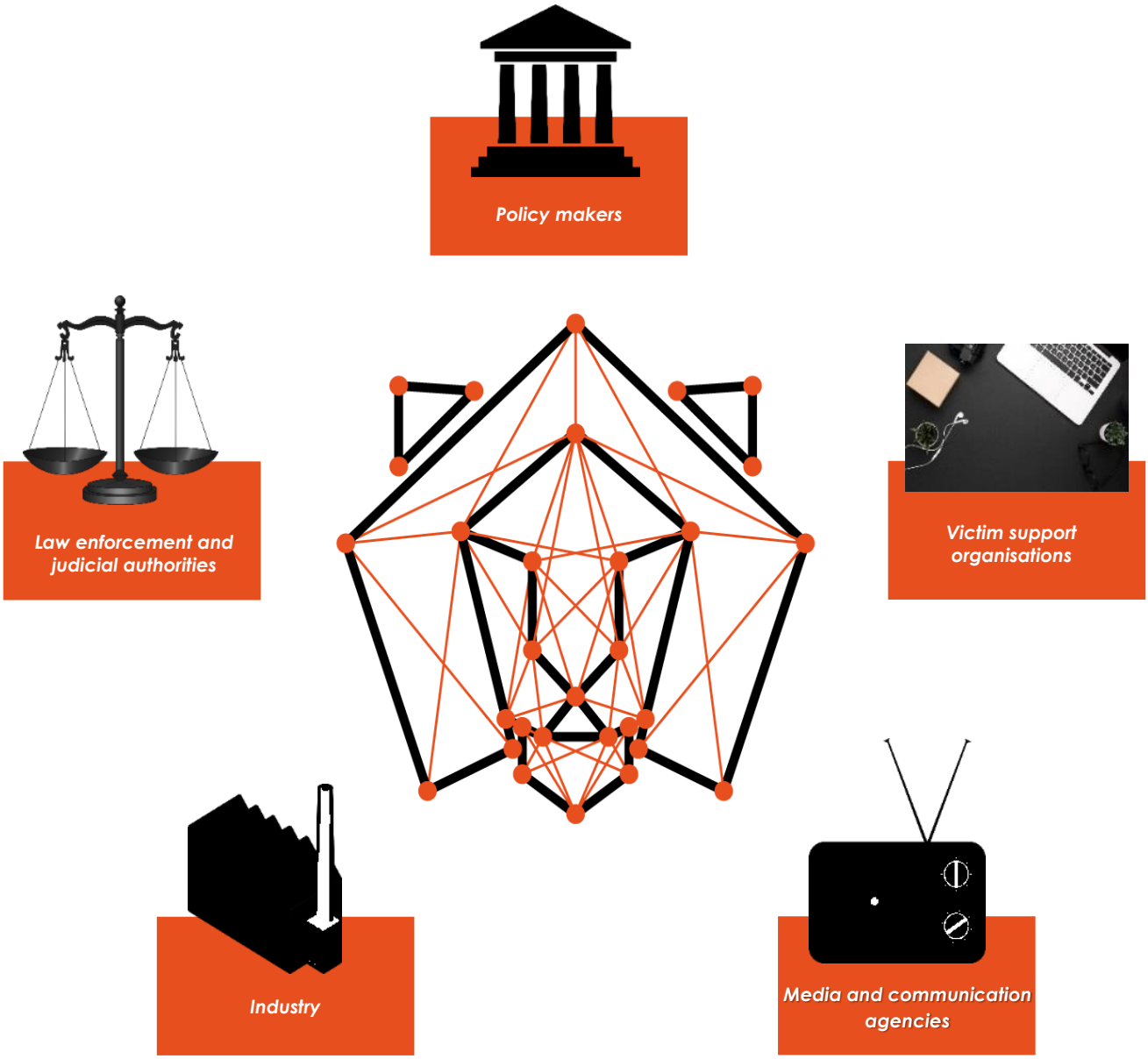
Lastly, as a result of VSOs' vast experience in raising awareness on crimes, VSO's close cooperation with communication and marketing agencies and with media, it is of added value to forge public-private partnerships also in this sense as these campaigns are proven to foster prevention and the adoption of safety behaviours.

Having said that, in order to ensure successful outcomes, law enforcement shall adopt a victim-centred approach, placing victim's right at the centre of the action and taking full account of victim particular needs, in addition to multi-sector cooperation with other stakeholders. There is consequently an emergent need to invest in prevention, increase sharing of information and broaden the reach of strategies, focusing on a comprehensive model, thus better equipping combating cybercrime strategies.

In this context, ***the following actions are recommended***:

[66] More information about *Ora de Net*, Save The Children's Cybercrime prevention and combating program here: https://oradenet.salvaticopiii.ro/.

Co-funded by the European Union's Internal Security Fund - Police



1. Inter-state cooperation

- Invest and take part in networks for furthering cybersecurity competences
- Take part in cybersecurity exercises;
- Deploy capacity building effort and the sharing of experiences and good practices;
- Develop common solutions for investigations;
- Develop common responses and strategies in order to facilitate joint cyber defence;
- Develop and take part of international use of tools for automated content detection, such as database of hashes;
- Develop tools and strategies for preventing reappearance, e.g. regularly filter out content which has been already identified as illegal;
- Regularly check international blacklists and keep the content up to date;
- Establish points of contact with ISPs and LEA and similar institutions in other states;
- Reinforce cooperation with EUROPOL and INTERPOL;
- Reinforce diplomatic responses to cyber threats;
- Promote capacity building in third countries in order to facilitate exchange of information;
- Create protocols, alliances and partnerships with third countries for coordinated and swift action;
- Reinforce principles of due diligence and state responsibility;
- Reinforce emergency response structures.

2. Public-private cooperation

- Promote public-private partnerships with all key-actors; industry, banks, businesses, academia, civil society (with particular emphasis to VSO);
- Multi-sector cooperation enables development of good practices and strengthens trust in the structure of combating cybercrime by tailoring the response to it, as well as it ensures enhanced protection of victims;

- Make cybersecurity language clear in raising awareness campaigns, with the aid of human expertise to make clarifications as the degree of technical orientation of information is at times the reason why people disengage with the content and refrain from adopting digital hygiene and safety habits;
- Put in place mechanism to retain human expertise, as public organisations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents;
- Promote skills programmes for public administration, in partnership with industry and relevant stakeholders;
- Create smooth action between law enforcement and judicial agencies and industry and other key-actors in view of sharing information and vulnerabilities;
- Create swift information exchange channels between all key players at national level;
- Ensure fast and effective response for mitigation of cyber attacks' impact, which in turn builds trust in public authorities and works as a deterrence mechanism;
- Cooperation across hosting service providers and with competent authorities
- Set up a liability framework for producers of vulnerable product/software concerning AI, applicable to all supply chain, to address the problem of attribution and ensure victim's redress;[67]
- Bridge the gap in security knowledge among the operated services and end-users;
- Build a robust email fraud defence mechanism in order to anticipate incidents;
- Address the absence of know-how and technical expertise for low-capability organisations/end-users, by setting up special programmes to help them designing intelligence solutions;
- Setting up protocols and referral mechanisms between state authorities involved in in combatting and preventing cybercrime and other relevant stakeholders;
- Set up protection mechanisms in low-end IoT devices and services.

[67] Liability for Artificial Intelligence and other emerging digital technologies, Report from the Expert Group on Liability and New Technologies – New Technologies Formation, Publications Office of the European Union, © European Union, Luxembourg 2019.

2.1. Regarding ICT industry:

- As the custodians of decisive data and wielding the power of blocking and removing contents, industry shall deploy its capabilities in improving cyber investigations and cybersecurity activity, taking into account its expertise skills;[68]
- Ensure engagement of industry as it plays a central role in fighting cybercrime, in supporting prevention and raising awareness, e.g. create spaces for awareness-raising programmes or events;
- Building on best practices;
- Developing duty of care and codes of conduct, promoting the adoption of proactive measures regarding the stored contents thereto;
- Provide advice on safe and responsible use of ICT platforms and networks and, thus, support preventive and awareness raising efforts towards online risks;
- Sharing of vulnerabilities and other relevant information;
- Implement mandatory report of illegal content and serious incidents;
- Implement mandatory take down of illegal content, subject to judicial confirmation;[69]
- Encourage other key-sectors to engage with the competent authorities in sharing information and regularly assess vulnerabilities, such as financial services, energy, health, transportation, civil society (namely VSO and Safer Internet Centres (CIS), etc.;
- Availability of a wide range of new innovative solutions to prevent and tackle cybercrime;
- Improve speed of information sharing;
- Develop understanding on emergent technologies such as IoT.

[68] Internet Organised Crime Threat Assessment, European Cybercrime Centre EC3, Europol 2019.
[69] In this regard, it is important to look at bill n.º 187/XIV, to be voted in the Portuguese Parliament, which aims at, amid other things, implement mandatory removal of CSEM content upon knowledge in article 19-A of the draft version.

2.2. Regarding LEA

- Improve structure and resources of national security centres and its relationship with LEA;
- Improve law enforcement response by focusing on better strategies for detection, traceability, prosecution of cyber criminals and positive outcomes, alongside mechanisms ensuring victim's rights, e.g. access to timely and easily understandable information, and access to victim support services;
- Put in place adequate frameworks for securing digital evidence, e.g. retention of data;
- Put in place enhanced procedures allowing for timely collection of evidence;
- Adjust current procedures to the speed of cyber-attacks;
- Facilitate cross-border access to evidence;
- Improve cybersecurity capabilities of LEA, e.g. in understanding and identifying malicious actors;
- Engage with VSO to provide specialised support to victims:
    - Improve strategies to enable law enforcement and judicial agencies to perform victim-sensitive investigations, e.g. by establishing cooperation protocols or referral mechanisms of victims to victim support services (*vide* Directive 2012/29/EU) ;
    - Set out victim's compensation schemes;
    - Establish specialised victim support services to victims of cybercrime and/ or establish clear referral procedures to existing support services;
    - Develop tailored information to victims of cybercrime, e.g. easy-to-understand information concerning the most technical terms associated with cyber offenses;
    - Engage ICT industry to be more active in reducing secondary victimisation.

2.3. Regarding victim support organisations

- Develop, consolidate and/ or expand support services so as to cater to the needs of victims of cybercrime. In the case of Romania, ensure that generic victim support services are created at a national level;

- Encourage close collaboration with all relevant stakeholders, including ICT industry and law enforcement and judicial agencies and VSO due to their central role in preventing and providing specialised support to victims of cybercrime;
- Ensure information on rights within the criminal justice system, emotional, psychological and social support;
- Promote awareness-raising campaigns on cybercrime and make sure that the information imparted can be fully understood by the public, taking into account the technical jargon related to cyber offences;
- Ensure that information on cyber offenses is deconstructed in a way that victims can easily understand;
- Ensure a victim's-needs sensitive approach to victim support;
- Develop instruments to periodically measure the nature, extent and impact of victimisation of cybercrime (including consequences for victims and for society);
- Develop mechanisms to increasing victims' willingness to report crimes, explaining the importance of having more police investigations (and in turn to a better chance of catching the perpetrator) and better insight on cybercrime for designing countering measures and preventing other crimes;
- Set up special units for preventing and mitigating effects of cybercrime and supporting victims - Specialised Support Units to Victims' of Cybercrime;
- Develop own internal specialist support procedures to victims of cybercrime, learn and exchange best practices with other VSOs that already run their specialised units;
- Implement Barnahus model[70];
- Ensure close collaboration with policy makers when designing justice and investigation policies;

[70] More on the Icelandic model here: https://childhub.org/en/promising-child-protection-practices/what-barnahus-and-how-it-works

- Due to the close contact with victims and their relatives and friends, set up channels for sharing of information and good practices with other relevant stakeholders, particularly with LEA;

2.4. Regarding research institutes, academia and media

- Promote close collaboration of academia and research with the competent authorities for improved insight of the phenomenon and study on vulnerabilities;
- Research into factors that influence the willingness to report crime and differentiate between the various types of victims (e.g., individual citizens, small and medium-sized enterprises, international organisations) and different types of cybercrime;
- Encourage media to disseminate relevant information on cyber defence mechanisms and common threats and attacks, using easily understood terms;
- Create hub for law enforcement innovation.

2.5. Regarding end-users, as it shall be done with their consent[71]

- Use online data and data from internal networks at organisations for mapping user behaviour and to better ascertain the nature and extent of cybercrime victimisation;
- Analysing users' computers could provide a better picture of malware infections and provide insight into the security measures installed by victims;
- Computer log files can be used to study real rather than reported respondent behaviour;
- Increasing insight into the nature of hacking incidents.

3. Multi-sector cooperation

- Sharing on a voluntary basis of experiences, technological solutions and best practices among industry and relevant stakeholders;
- Designate points of contact for hosting service providers;

[71] All retrieved from Research Agenda the Human Factor in Cybercrime and Cybersecurity, Rutger Leukfeldt (editor), Eleven International Publishing, 2017.

- Promote company's duty of care and strict codes of conduct;
- Ensure transparency towards the general public:
    - *Ex ante* disclosure of codes of conduct, terms of services and internal policies on the removal or disabling of access to any content that they store, including illegal content;
    - *Ex post* incidents regularly publish reports about the mechanisms in place to detect and take down illegal contents and about the contents removed in fact, in order to shed light upon incidents among industry and stakeholders
    - Considering establishing these transparency reports would benefit from some standardisation across the Digital Single Market.
- Adopt effective risk-management practices;
- Set up internal processes in place that deal with investigation, triage and resolution of vulnerabilities, to the extent of their supply chain where applicable;
- Advance technology to more effectively detect illegal content (the use of automatic detection and filtering technologies);
- Having in place technology (such as databases of hashes) for preventing dissemination of illegal content across different hosting services (through automated detection) and also for preventing the reappearance of illegal content online, making sure there is human oversight and verifications *a posteriori*;
- Develop security by design approach, by means of introducing qualitative measures into its production processes, perform end-to-end security assessments and adhere to certification schemes in order to enhance security of products and software, reducing its vulnerabilities;
- Business shall work towards making cybersecurity available to all stakeholders, especially the ones that lack technical knowledge;
- Security software industry needs to develop solutions to help end-users and organisations mitigating most of the low-end automated cyber threats, with minimum human intervention;
- Encourage partnerships between business and industries to ensure safe channels for customers;

- Encourage capacity building through cooperation with industry in order to enhance understand of the phenomenon and handling of technical tools.

Strengths

Policy makers

- Executive and political power
- Enforcement power
- Procedures in place
- Public authority
- International cooperation
- Diplomacy
- Human capital

Industry

- Cutting-edge technology
- Field work and experience
- Takedown procedures and blocking mechanisms

Civil Society, including Academia, Media, etc.

- Research skills
- Think tank groups
- Engagement and galvanizing skills
- Reach at grass-roots level
- Ethical information and dissemination
- Transformation avenue
- Development and democracy aid
- Awareness-raising skills
- Specialist support to victims

Weaknesses

- Difficulties in the implementation of Article 25 of Directive 2011/93/EU (blocking and removal measures)
- Lack of awareness about cybercrime seriousness by the public
- Lack of awareness about cybersecurity by the public and policy makers
- Human error
- Underreporting
- Difficulties in the investigation of cybercrime
- Lack of understanding regarding the impact of cybercrime on victims
- Lack of procedural standardised guidelines for investigations
- Self-generated explicit material
- Detection and Investigation tools are not standardised among the MS
- Confliction between different legal frameworks at the EU level
- Uncertainty of procedural rules as to digital evidence
- Blocking mechanisms are not uniformly approached in different MS
- Not enough financial, technical and human resources deployed in cybersecurity
- Difficulties in multi-sector cooperation at the national level
- Government's unwillingness to share cybersecurity-relevant information
- Companies' reluctance to share information (trade secret and reputation)

Opportunities

- Transform weaknesses into opportunities
- EU *acquis* on cybersecurity and cybercrime
- EU support and openness to cooperation
- Access to funds
- Deploy research on the subject into legal frameworks and strategies
- Leverage in promoting companies' assets:
- Keeping up with fast development of technologies and investing in ICT and development
- Promote duty of care

Threats

- Complexity of cybercrime nature, evolution and dimension makes it difficult for LEA and industry to keep up with:
  - Use of malware (ransomware, phishing, etc.)
  - Fast moving content of CSEM
  - Payment fraud
  - DNS High jacking
  - Cryptominers (cryptojacking)
  - Cross-cutting crime methods
  - IoT, 5g, AI (e.g. the ongoing improvements of so-called deepfakes), cloud services, quantum computing
  - Fast development of hacking technologies

- Use policy and governance powers to push forward decision makers and other key-actors to:
- Prioritise cyber-awareness information
- Prioritise combating CSEM
- Invest in digital literacy and prevention
- Promote specialised and regular training
- Mainstream cybersecurity education into school curricula
- Improve structures and resources of national cybersecurity centre and LEA
- Create hub for law enforcement innovation
- Improve traceability and attribution in investigations
- Promote public-private cooperation, across industry, between MS
- Facilitate cross-border access to electronic evidence
- Adopt and promote victim-sensitive approach
- Provide specialised support to victims of cybercrime

  - Fast spreading to all areas of crime

- The criminal abuse of the dark web
- The convergence of cyber and terrorism
- The criminal abuse of cryptocurrencies
- The use of encryption, anonymization and obfuscating techniques
- Cyber-attack on demand industry: bought as online shopping
- Cooperation between EU MS is still insufficient
- Current transnational cooperation with third countries shows several gaps and shortcomings as it depends on the willingness of States
- Difficulties with channelling legal requests to ISPs outside MS's jurisdictions
- Online misinformation and disinformation campaigns
- Criminal abuse of State-sponsored attacks

5. The Covid-19 pandemic and cybercrime. Recommendations.

5.1. Europe

The current Covid-19 pandemic has impacted severely the scale of cybercrime and changed drastically future projections in this field. Unsurprisingly, there was a significant increase in cyber-attacks of varying nature during the COVID-19 crisis.

The fact that people have more access to internet and spent more time online, together with the overall feeling of uncertainty and fear, represent a rather deadly combination for cybercrime to happen. Criminals have been taking advantage of COVID-19 crisis to carry out more ingenious attacks targeting and abusing the demand that people have for information and supplies.

It is therefore essential to understand its impact on cybercrime and the expected challenges post-crisis in order to tackle this new reality. In this connection, the main threats found since March 2020 were as follows:[72]

- Social engineering attacks, namely phishing emails through spam campaigns and more targeted attempts such as business email compromise;
- Prevalence of phishing campaigns that distribute malware via malicious links and attachments designed to executing malware and ransomware attacks;
- Fraud schemes have been used to target citizens, businesses and public organisations through bogus websites, fake apps, fake investment opportunities, and money mulling.

The most affected sectors by cyber threats were public services, e-government, and digital citizenship sector due to digital transformation. With respect to critical infrastructures, there was a significant increase in cyber-attacks experienced by the healthcare and financial sectors. In addition, pharmaceuticals were also under heavy attacks intended to obtain confidential data about vaccines, treatments and tests.[73]The registered threats were enabled/enhanced by the following factors:

- Increased Internet traffic;
- Increased reliance on secure remote access technologies which employees are not always familiar with and with potentially sensitive links between professional and personal computers and associated devices;
- Increased use of smartphones for remote conferences, exchange of documents etc.;
- Increased attack surface as more individuals work from home and part of the internal company network could be reachable from outside.

[72] ECSO Barometer 2020: "Cybersecurity in light of Covid-19", Report on the results of surveys with ECSO members and the cybersecurity community, © European Cyber Security Organisation (ECSO), 2020.
[73] See, for example: https://www.europeanpharmaceuticalreview.com/news/117304/covid-19-pandemic-spurs-cyber-attacks-on-healthcare-sector-says-report/; https://www.bbc.com/news/technology-53429506; https://www.labiotech.eu/medical/covid-19-vaccine-cyber-attack/.

All things considered; this crisis presents the following challenges:

- Many organisations and businesses show concern about potential lack of understanding of how the market has changed and is being evolving;
- Increased need to help SMEs protect their ICT infrastructures;
- Strong need for research & innovation across all areas of cybersecurity, prioritising infrastructure resilience and data & AI (including privacy);
- It is expected an accelerated digitalisation (more than anticipated in the pre-COVID era), denoting a drastic evolution of IoT, AI, 5G, Cloud & Edge computing, blockchain, high performance computing, automated decision making and management of large amounts of data, aiming at speeding up the recovery of manufacturing.

Having this background, a set of recommendations is suggested:[74]

- Stronger public funding for research and innovation is needed, according to the cybersecurity community;
- Shorter cycle from research to innovation to cope with potential new disruptive challenges;
- Increased need to raise awareness on cyber threats during the COVID-19 crisis, with emphasis on cyber risks, fake news and misinformation and disinformation, in which civil society and media may be of great help;
- Advocacy and cyber resilience measures (networking, fostering strategic public-private partnerships and advocate for a reliable, safe and secure European IT support);
- Leveraging European assets: focusing on investment, capacity-building & competitiveness and therefore standing as drivers of research, industrial innovation and data & privacy frontrunner.

[74] ECSO Barometer 2020: "Cybersecurity in light of Covid-19", Report on the results of surveys with ECSO members and the cybersecurity community, © European Cyber Security Organisation (ECSO), 2020.

5.2. Portugal

Covid-19 pandemic's impact on cybercrime in Portugal follows the European trends.[75]

Specific registered threats:

- Phishing/smishing (via email, SMS and social networks) unlawfully using the names of health-related organisations, seeking to capture personal data or infecting devices with malware;
- Malware and ransomware, distributed through email or DNS (Domain Name System) redirection;
- Apps allegedly providing services related to Covid-19 pandemic but instead distributed malware, in some cases ransomware;
- Digital fraud collecting donations through crowdfunding for the false purchase of medical materials to help fight the disease;
- Fake Internet pages, or fraudulent offers, for the sale of medical materials;
- Sale on the darkweb of Covid-19 sets, which allowed cyber-attacks to individuals in telework;
- Misinformation campaigns blaming the pandemic on specific groups and/or states.

In respect of numbers, in March 2020, it was registered an increase of 84% reported attacks over February 2020. Also, cyber incidents rose by 176% in March 2020, compared to the same period in 2019. As for phishing, data show an increase by 217% in March 2020 over February of the same year, amounting to 57 and 18 reported incidents respectively.

Impacts and projections of new trends:

- Continue using Covid-19 subject for social engineering attacks;
- Intensification of attacks that use the weaknesses of the human factor (resorting to social engineering methods) such as phishing, ransomware, fraud, taking advantage of the growing use of data;

[75] Cybersecurity in Portugal: Risks and Conflicts Report, National Centre for Cybersecurity, June 2020.

- Increasing attacks on critical infrastructure, taking advantage of greater reliance on digital;
- Biggest threat to personal data due to the increased collection and storage of personal data in the fight against the disease;
- Technologies that run personal data, such as the IoT, AI and Cloud Computing, have the potential to become even more relevant;
- Challenge to democratic states and rule of law regarding the security vs. privacy quandary. In fact, the use of citizens' data for the purposes of keeping track and controlling the public health situation has led to general acceptance of its use. However, there is a risk that some measures will not be overturned in the post-pandemic scenario, which may facilitate the misuse of personal data;
- In case of economic crisis due to the pandemic, cybercriminals may take advantage of social and economic weaknesses linked to unemployment;
- Economic crisis and social instability may be a fertile soil for misinformation campaigns and cyber-attacks against states, as well as a risk-factor for spreading of terrorist and radicalisation online campaigns;
- Also, economic and social instability may give rise to increasing attacks seeking to cause reputational damage with political purposes, through social media, such as DDoS, data breaches or account commitments;
- Increased pressure on international bodies to advance international cooperation on cybersecurity on the one hand, but also the risk that restrictive measures taken in the context of the pandemic could reinforce national closure;
- Social, psychological, economic and financial impact on victims.

5.3. Romania

Romania has also seen an increase in cybercrimes since the beginning of the COVID-19 pandemic, with the country being among the first 10 European countries targeted by cyberattacks. Cybercrimes during the lockdown generally followed European trends, as the main themes chosen by attackers to

lure potential victims were cures to the illness and vaccines to prevent infection with the new Coronavirus, usually sent via email and containing malware. [76]

5.4. Germany

Although there is still a lack of recent studies to the extent and development of cybercrimes since the beginning of the COVID-19 pandemic, it can be said that Germany has also seen an increase in cybercrimes and it generally followed European trends. It is clear that those affected include private users as well as businesses, public authorities, hospitals or health authorities. The threats were as follows:

- Fake internet pages were selling breathing masks, test kits, covid-19 medication, or immunity preparations, which were never delivered or which turned out to be faulty;
- Donation fraud, such as forged appeal for funds via social network;
- Fraud incidents when applying for the application of funds or government support;
- Phishing emails, such as using the names of health-related organisations or health authorities and CEO-Fraud were also a subject of cyber-attacks;
- An increased number of DoS/DDos attacks, malware via malicious links and attachments, ransomware and spyware;
- Fraud schemes have been used to target citizens, businesses and public organisations through bogus websites, fake apps, fake investment opportunities.

[76] Bitdefender, *Un nou vârf al amenințărilor informatice care exploatează subiectul coronavirus. Zilele lucrătoare, momentul preferat al atacatorilor*, May 1st 2020: https://www.bitdefender.ro/news/un-nou-varf-al-amenintarilor-informatice-care-exploateaza-subiectul-coronavirus-zilele-lucratoare-momentul-preferat-al-atacatorilor-3840.html

5.5. General recommendations

- Investment in cybersecurity at both technical and human level;
- Educating and raising awareness is a key-solution as social engineering is the leading method of these cyber-attacks;
- Investment in promoting multisector and interdisciplinary cooperation with all relevant stakeholders;
- Investment in specialist support to victims of cybercrime, establishing avenues for strict cooperation with industry, LEA and judicial authorities, governmental and non-governmental entities that work in preventing and fighting cybercrime, media, marketing and communication agencies, amongst others.

Glossary

AI – Artificial Intelligence: technology designed to use computers to do things that traditionally require human intelligence. This means creating algorithms to classify, analyse, and draw predictions from data.

BEC – Business Email Compromise: form of cybercrime which uses email fraud to attack commercial, government and non-profit organizations to achieve a specific outcome. It relies heavily on social engineering tactics to deceive unsuspecting employees and executives.

CEO – Chief Executive Officer

CERT – Computer Emergency Response Team: expert team that handles computer security incidents, involving any device belonging to a network.

CGN – Carrier-Grade NAT: technology that translates one public network address into several different private addresses. The adoption of Carrier Grade NAT is mainly due to the ability to share a global (public) IP address among multiple remote sites.

CNP – Card Not Present fraud: type of credit card scam in which the customer does not physically present the card to the merchant during the fraudulent transaction. CNP can occur with transactions that are conducted online or over the phone.

CSEA – Child Sexual Exploitation and Abuse

CSEM – Child Sexual Exploitation Material

CTI – Cyber Threat Intelligence

DNS – Domain Name System: is an internet service where internet domain names and location are translated into internet protocol (IP) addresses.

DoS/DDoS attack – Denying of Service/Distributed Denial of Service attack: form of cybercrime in which the perpetrator seeks to make a machine, network, and webpages unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

ICT – Information and Communications Technology

IoT – Internet of things: network of physical objects in which are inserted sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet, e.g. mobile phones.

IP – Internet Protocol: most common set of requirements/protocol by which data is sent from one computer to another on the Internet.

IPv4 address – Internet Protocol version 4 address is a 32-bit number that uniquely identifies a identify hosts (computer) by an IP addressing scheme.

ISP – Internet Service Provider: organisation that provides services for accessing, using, or participating in the Internet.

LDCA – Live Distant Child Abuse

LEA – Law Enforcement Agency

MS – Member States of the EU

NCPF – Non-Cash Payment fraud: transactions where no real cash is involved, mainly used in the e-commerce. NCPF involves scams such as

credit card or payment details theft, skimming or phishing.

OSP – Online Service Provider: any company, organization or group that provides an online service, e.g. chat rooms.

RPDs – Remote Desktops Protocols: most common used software to access desktop computer remotely.

SGEM – Self-Generated Exploitation Material: production of self-generated sexual/indecent material. Such material, initially shared with innocent intent, often finds its way to "collectors", who often proceed to exploit the victim, in particular by means of extortion.

SME – Small Medium Enterprises

SMS – Short Message Service

Tor – (Anonymity Network): software/tool for internet privacy. Its technology bounces back traffic from Internet users and websites through retransmission to thousands of volunteers around the world, making it extremely difficult for anyone to identify the source of the information or the location of the user.

URL – Uniform Resource Locator: protocol for specifying addresses of webpages or documents accessible over the Internet.

VPN – Virtual Private Network: technology that creates a private network from a public internet connection, enabling users to send and receive data anonymously. As VPNs mask internet protocol address, online actions are virtually untraceable.

VSO – Victim Support Organisation

Appendices

Appendix 1: Romanian Police statistics on the number of criminal reports and criminal investigations on cybercrimes for the period January 2015 – September 2019.[77]

INDICATORS	CRIMINAL REPORTS/ COMPLAINTS					Crimes for which CRIMINAL INVESTIGATION towards the suspect was ordered				
	2015	2016	2017	2018	first 9 months of 2019	2015	2016	2017	2018	first 9 months of 2019
1. Cyberfraud (art. 249, CC)[78]	275	286	460	444	328	8	35	30	80	67
2. Performing fraudulent financial transactions (art. 250, CC)	3011	2962	3319	3303	3773	77	43	159	313	320
3. Accepting fraudulent financial transactions (art. 251, CC)	7	9	11	9	5	4	1	0	0	0
4. Illegal access to a computer system (art. 360, CC)	561	725	803	787	708	3	1	81	189	202
5. Illegal interception of a computer data	5	6	7	8	10	0	0	0	0	0

[77] Reply to ACTEDO's request for public interest information, Annex to Letter no. 405802 of October 23rd, 2019, General Inspectorate of the Romanian Police.

[78] CC stands for The Criminal Code of Romania. For definitions of these offences, refer to the section on the legal framework governing cybercrimes in Romania.

transmission (art. 361, CC)										
6. Altering the integrity of computer data (art. 362, CC)	31	22	36	46	42	0	0	0	0	0
7. Disrupting the functioning of computer systems (art. 363, CC)	20	16	16	36	12	0	0	0	0	0
8. Unauthorised transfer of computer data (art. 364, CC)	1	9	5	14	6	1	0	0	0	0
9. Illegal operations with computer devices or software (art. 365, CC)	27	23	22	63	29	0	0	0	0	0
10. Child pornography (art. 374, CC)	132	162	242	212	258	0	0	0	0	0

Please note that the table contains only those crimes whose criminal investigation falls under the competence of the Police.[79]

Appendix 2: Romanian Ministry of Justice statistics on the number of cybercrime convictions for the period January 2016 – June 2019.[80]

Main offence	Number of persons that received a final conviction in the year:			
	2016	2017	2018	2019, until June 30th
Cyberfraud (art. 249, CC)	6	8	27	4
Performing fraudulent financial	49	47	66	33

[79] According to the Criminal Code of Procedure, Art. 56, paragraph 3 (d), only prosecutors, hence not police officials, may order the criminal investigation of crimes indicated at art. 361, 362, 363, 364, 365 and 374 of the Criminal Code, as well as of crimes indicated at art. 249, 250, 251 and 360 of the Criminal Code, when they have been committed by an organised crime group or when they have produced severe consequences.

[80] Reply to ACTEDO's request for public interest information, Annex to Letter no. 86769 of October 18th, 2019, Ministry of Justice Romania.

transactions (art. 250, CC)				
Illegal access to a computer system (art. 360, CC)	61	64	38	21
Altering the integrity of computer data (art. 362, CC)	0	0	1	1
Illegal operations with computer devices or software (art. 365, CC)	7	5	9	5
Child pornography (art. 374, CC)	63	63	95	47

Appendix 3: Convictions on charges of child pornography in Romania between January 2016 and June 2019[81]

YEAR	NUMBER OF CONVICTED INDIVIDUALS	OF WHOM
2016	63	12 minors, 36 with suspended sentences, 7 with detention exceeding 10 years, 2 with detention between 5 and 10 years, 1 with detention between 3 and 5 years, 4 with detention between 1 and 3 years and 1 with detention below 1 year;
2017	63	11 minors, 36 with suspended sentences, 4 with detention between 5 and 10 years, 6 with detention between 3 and 5 years, and 6 with detention between 1 and 3 years;
2018	95	17 minors, 41 with suspended sentences, 6 with detention exceeding 10 years, 7 with detention between 5 and 10 years, 9 with detention between 3 and 5 years, 15 with detention between 1 and 3 years;
January 1st - June 30th, 2019	47	6 minors, 28 suspended sentences, 1 postponement of sentence execution, 1 with detention exceeding 10 years, 1 with detention between 5 and 10 years, 6 with detention between 3 and 5 years, 4 with detention between 1 to 3 years.

[81] Reply to ACTEDO's request for public interest information, Annex to Letter no. 86769 of October 18th, 2019, Ministry of Justice Romania.

Bibliography

APAV Barometer Intercampus on People's perception on cybersecurity, March 2020.

Annual report on the state of IT security in Germany in 2019 of the Federal Office for Information Security (BSI).

Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online, 1 March 2018.

Common challenges in combatting cybercrime, Europol & Eurojust Report, June 2019. Retrieved from https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime

Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online, Towards an enhanced responsibility of online platforms, com(2017) 555 final, Brussels, 28.9.2017.

Conclusions of Expert Workshop on the implementation of Article 25 of Directive 2011/93/EU, organised by the European Commission on 19 June 2019.

Council of Europe Convention on Cybercrime of 23 November 2001 (Budapest Convention), available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 25 October 2007 (Lanzarote Convention). Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201

Cybersecurity in Portugal: Risks and Conflicts Report, National Centre for Cybersecurity, June 2020.

Directive (EU) 2019/713 of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, 17 April 2019.

Directive 2011/93/EU of the European Parliament and of the Council on combatting the sexual abuse and sexual exploitation of children and child pornography, 13 December 2011. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN

Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems, August 2013. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JH, 12 August 2013.

ECSO Barometer 2020: "Cybersecurity in light of Covid-19", Report on the results of surveys with ECSO members and the cybersecurity community, © European Cyber Security Organisation (ECSO), 2020.

ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends, January 2019.

European Commission, *Special Eurobarometer 464a: Europeans' Attitude towards Cybersecurity*, 2017

European Parliament, Cyber: How big is the threat? https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

Expert Workshop Removal and blocking of web pages containing or disseminating child sexual abuse material (CSAM), Preparation of workshop discussion, European Commission Directorate-General Migration And Home Affairs.

European Commission, *Special Eurobarometer 464a: Europeans' Attitude towards Cybersecurity*, 2017

https://ec.europa.eu/growth/single-market/european-standards/ict-standardisation_en

https://fra.europa.eu/en/project/2018/handbook-european-law-relating-cybercrime-and-fundamental-rights

https://www.bakermckenzie.com/en/insight/publications/2019/10/uk-us-data-access-agreement

https://www.cncs.gov.pt/recursos/noticias/governo-aprova-nova-estrategia-nacional-de-seguranca-do-ciberespaco/ . texto em https://data.dre.pt/eli/resolconsmin/92/2019/06/05/p/dre

https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation

https://childhub.org/en/promising-child-protection-practices/what-barnahus-and-how-it-works

Human Factor Report ProofPoint 2019.

Internet Literacy Handbook, Supporting users in the online world, Council of Europe Publishing, © Council of Europe, October 2017.

Internet Organised Crime Threat Assessment, European Cybercrime Centre EC3, Europol 2019.

Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final, Brussels, 13.9.2017. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, and Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7 February 2013. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

Liability for Artificial Intelligence and other emerging digital technologies, Report from the Expert Group on Liability and New Technologies – New Technologies Formation, Publications Office of the European Union, © European Union, Luxembourg 2019.

P8_TA(2017)0366, The fight against cybercrime, European Parliament Resolution on the fight against cybercrime (2017/2068(INI)) (2018/C 346/04), 3 October 2017.

Payment Threats and Fraud Trends Report 2019, European Payments Council-

Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, WeProtect Global Alliance, November 2016.

Research Agenda the Human Factor in Cybercrime and Cybersecurity, Rutger Leukfeldt (editor), Eleven International Publishing, 2017.

Special Eurobarometer 499, Europeans' attitudes towards cyber security report, January 2020.

Threats of the Year, A look back at the tactics and tools of 2019, Cisco Cybersecurity Series 2019, December 2019.

As to legal frameworks:

Portugal:

Criminal Code

Code of Criminal Procedure

Cybercrime Law, Law no. 109/2009

Council of Ministers Resolution 92/2019

General Framework of Tax Infringements

Copyright and Related Rights Code

Industrial Property Code

Decree-Law 7/2004 of January 7th

DL n. º 422/89 of December 2nd

Law 52/2003 of August 22nd

Law 32/2008 of July 17th

Law 59/2019 of August 8th

Law 46/2018 of August 13th

Draft bill no. 187/XIV, to be voted in the Portuguese Parliament, which aims at, amid other things, implement mandatory removal of CSEM content upon knowledge in article 19-A of the draft version. Retrieved from https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=44369

Romania

Criminal Code

Law no. 161 of April 19, 2003 on certain measures to ensure transparency in the exercise of public dignity, public office and in the business environment, the prevention and sanctioning of corruption

Law 217/ 2003 on the prevention and combatting of domestic violence

For more information about the draft bill on non-consensual pornography, go to https://www.senat.ro/legis/lista.aspx?nr_cls=L512&an_cls=2019 (accessed December 16th, 2019).

Germany:

Criminal Code (StGB)

Criminal Code of Procedure (StPO)

The Telecommunications Act (TKG)

Telemedia Act (TMG)

IT Security Act (IT-Sicherheitsgesetz)

Network Enforcement Act (Netzwerkdurchsetzungsgesetz – NetzDG)

https://eucrim.eu/news/federal-administrative-court-refers-german-data-retention-law-european-court-justice/ and https://www.bverwg.de/pm/2019/66

https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html

https://www.bundesgerichtshof.de/DE/Bibliothek/GesMat/WP18/V/Verkehrsdaten.html