BRIEFING
EU policies – Insight

European Parliament

Understanding cybercrime

SUMMARY

Cybercrime is a major threat to society that generates billions of euros for its perpetrators. It is a form of crime that is continuing to grow, with criminals showing increasing sophistication and resourcefulness. These criminal activities occur at all levels of society and take many forms, from investment fraud to phishing and the creation of bogus entities, including fake charities.

The rise in the use of digital solutions for everyday activities in business and public services is matched by the number of digital devices being used by citizens. People are now connecting to numerous digital accounts and are spending more time online than ever before. Coupled with this, cyberattacks and digital scams are on the rise. Not only is the number of incidents growing, but the complexity and the subsequent negative impact is also increasing.

Cybercrime can be relatively simple in appearance, such as spurious emails and text messages, or complex, involving a number of actors spreading malicious content through entire business or public service systems in order to block access for ransom purposes or to disable critical entities for ideological reasons.

The EU is active in tackling cybersecurity and cybercrime, as demonstrated by its cybersecurity strategy. It has a number of pieces of legislation in place or in the pipeline to tackle vulnerabilities, increase the resilience of essential services and address associated cybersecurity risks. Likewise, EU agencies are proactively dealing with the threat posed by cybercrime by supporting Member States and stakeholders in addressing emerging threats and strengthening resilience.

IN THIS BRIEFING

EPRS | European Parliamentary Research Service

Author: Colin Murphy
Members' Research Service

PE 760.356 – March 2024

EN

Introduction

While there is no universally accepted definition of cybercrime, it is essentially an act using information technology to perpetrate or facilitate a crime. Specifically, in its glossary, the International Organisation for Standardisation (ISO) defines cybercrime as 'the commission of criminal acts in cyberspace'. More informally, it is understood as the use or exploitation of information and communication technology (ICT) and/or the internet to commit crime. It may be argued that cybercrime is not a new crime; it is merely a new way of perpetrating crime in general. Where once criminals stole from banks, post offices and individuals in face-to-face encounters, criminals now use electronic means and have often escaped before it is realised that a crime has been committed.

Cybercrime can be characterised into two different categories, cyber-dependent crimes, and cyber-enabled crimes. **Cyber-dependent crime** is 'any crime that can only be committed using computers, computer networks or other forms of information communication technology'. Such crimes target ICT systems and are typified by hacking, and malware including ransomware. **Cyber-enabled crimes** are traditional crimes facilitated by the internet and digital technologies.[1] They have evolved in scale and form through the increased use of the internet and communication technology and include fraud through phishing, piracy and counterfeiting.

More sinister is the rise in cyberbullying, cyberstalking and harassment, online grooming and child sexual abuse. Online sexual coercion and extortion is one of the new crime phenomena of the digital age. It is a heinous crime that has evolved with the constantly evolving technical world. In the past, paedophiles had more difficulty in accessing and sharing child pornography, with most of the offences occurring in person and in closed environments. Today, largely due to the popularisation of social media, it is easier for offenders to share and generate content. The 2022 Interpol Global Crime Trend Summary Report pointed to online child sexual exploitation or abuse as one of the top 10 crime trends.

Cybercrime knows no physical or geographic boundaries and can be carried out with relative ease. This lack of borders allows criminals to carry out their crimes in other countries and makes investigations and prosecutions difficult, with law enforcement relying on cooperation at an international level to tackle it.

Impact of cybercrime

The impact of cybercrime can be significant for its victims. It can cause serious economic and reputational damage to businesses and public services and can have a negative financial and emotional impact on individuals. The perpetrators of cybercrime are numerous, with a variety of motivations from those seeking purely financial gain to those who are ideologically influenced, including nation states. According to the World Economic Forum's (WEF) 2023 Global Risks Report, cybersecurity is in the current and future top 10 risks globally, and the cost of cybercrime is projected to hit an annual US$10.5 trillion by 2025. According to a 2019 report from the European Commission, the annual cost of cybercrime to the global economy was estimated to have reached €5.5 trillion.[2] In a survey carried out by the Commission in 2021 on small and medium-sized enterprises (SMEs) and cybercrime,[3] the overwhelming majority of SMEs indicated that they used some manner of online tools in their business and a majority used five or more. A similar study on citizens' attitudes to cybersecurity indicated rising levels of internet use and a corresponding increase in cybercrime.[4]

The impact of cybercrime on businesses can be significant. For instance, according to IBM's 2023 Cost of a Data Breach Report, the average cost of a cyber-breach is US$4.45 million.[5] The report gives some insight into the cost of dealing with a breach of data security. It stated that it takes organisations an average of 204 days to identify a breach and 73 days to contain one. The majority of companies also indicated that the costs of these are passed on to consumers through increased prices. In ransomware attacks, the report found that organisations that paid a ransom were likely to

end up spending more than if they had not paid the ransom. One of the biggest victims of cyber-breaches is the healthcare industry, with it reporting the largest costs associated with a cyber-attack.

The increasing sophistication of criminals is resulting in increasing numbers of tech-savvy and security-conscious individuals being fooled by fraudsters, both in private and professional capacities. Victims are convinced by websites and phone numbers that appear genuine; fraudsters may use the same telephone hold music as genuine organisations for instance. The amounts involved can range from very small amounts to sums of up to six figures. Often these scams, in addition to monetary losses, leave their victims feeling embarrassed, foolish and vulnerable.

Cybercrimes and behaviours

Trends

The growth in the use of information and communication technology in everyday life and the increase in connectivity of household items and the development of e-commerce have created increased opportunities for criminals who are harnessing advances in technology to perpetrate crime. The ease of access to such technology, allowing anyone to employ the power of artificial intelligence (AI), has in some instances increased the effectiveness of cyber scams.[6] For example, one of the indicators of a phishing email was poor spelling or grammatical errors. Now, however, criminals creating such emails can simply use AI tools to create more authentic-looking fraudulent messages and calls, making it less obvious to potential victims that they are the target of criminals. Deep fakes can also be used to create supporting 'evidence' to lure victims into believing in fake products or investment scams and ultimately have their money stolen.

Another growing trend in cybercrime is what is known as 'cybercrime as a service', i.e. the provision of malicious software to other criminals. The availability of illegal digital services, in an increasingly complex technological environment, makes it easy for people with low levels of technical skills who are attracted to the lucrative nature of anonymous cybercrime to engage in such activities, leading to further growth in cybercrime. The activities include providing access to security vulnerabilities in infrastructure, the provision of malware in an 'off-the-shelf' manner and the provision of access to compromised credentials, which are a commodity.

Offenders

The offenders who engage in cybercrime are diverse in their motivation and include the following:

- **State-sponsored actors** who are government funded, well trained and skilled and generally politically motivated. This group often focus their attacks on high-profile or high-value targets such as critical infrastructure, which is increasingly reliant on digital support. The ongoing war in Ukraine has demonstrated the persistent nature of these players, with numerous attacks documented against Ukraine but also against EU Member States, including Poland, Lithuania and Germany.[7]
- **Cybercriminals** engaging in such activities for purely financial gain. Criminals respond swiftly, adapt quickly to circumstances and new trends, and are becoming ever more creative, with the ability to deceive customers easily, for instance with the creation of scam-shopping sites designed to look like official ones. These sites offer 'bargains' and put customers under pressure to avail of the low prices. Criminals also hack into the email and customer systems of businesses and use stolen details to defraud their customers. Hackers using cloned email addresses request payments into fraudulent accounts leading to the theft of large sums of money. With a reputation for striking on a Friday afternoon, many victims may not realise that they have been scammed until checking the following Monday morning.
- **Insiders**, including personnel (current or former employees), contractors, organisation members and business partners; the threats are multiple and can be

intentional and malicious, or negligent, complacent or simply unintentional. According to IBM's Cost of a Data Breach Report 2023, data breaches initiated by malicious insiders were the most costly, at US$4.9 million on average.

- **Hacktivists**, generally motivated by political or social ideals, whose aim is to cause disruption. While the rationale behind their actions is different, with a stated ideal of holding governments and organisations to account for what they believe are just causes, their impact on their targets remains the same.[8] For example, they employ denial of service tactics to disrupt the websites and services of those they oppose, and also replace website content with their own messages or steal data from governments and organisations and release it to attract attention to their cause. Hacktivism had been on the decline according to some analysis, but has seen a resurgence as a result of the current geopolitical climate.[9]
- **Cyber terrorists**, similarly to state-sponsored actors, are often motivated by political or extreme ideology; they use digital technology through politically motivated attacks on networks and systems with the clear aim of disrupting services and creating fear and uncertainty. There is little specific data on the impact of cyber-terrorism, for reasons including the blurred lines between it, state-sponsored activities and criminal intent. However, the threat is real, with both nations and organisations taking appropriate steps to counter it.

Forms of cybercrime

Cybercrime takes many forms and has numerous targets; it can be a complex incident or a relatively simple one, with the subsequent impact being widespread or local. Criminals can direct their efforts towards individuals, property, governments or organisations. It would be lengthy and time-consuming to list all cybercrimes and their sub-divisions; however, outlined below are a number of the most common cybercrimes.

Phishing: This type of crime involves the perpetrators sending malicious email attachments or links to an individual in order to gain access to their accounts or computer. Users are tricked into reacting to emails claiming to be from a bona-fide business or organisation informing them that they need to change their password or update their billing information, giving criminals access to their accounts and their funds.

Malware: Malware, simply put, is malicious software that 'infects' systems and individual devices which either damage or gain access to computers or networks with criminal intent. Common variants of malware are viruses, worms, spyware and ransomware. Malware is usually spread through emails and untrustworthy websites, or hidden in other files such as documents or images. It will spread when opened, which allows the malware to install itself. In many instances, users unintentionally introduce malware into computers or systems by clicking on a link or downloading content from unverified or malicious sites. The intent behind the distribution of malware is to gain control over a system or device and to steal information or data.

Ransomware: Ransomware is the crime that regularly hits the headlines. It is a form of malware employed by criminals, which usually takes control of a system or network, preventing users from accessing their records. The criminal will then either continue to lock the files until the payment of a ransom is made, or threaten to release the data, often confidential, unless payment is made. Payment is typically requested to be made in cryptocurrency and the victim will receive a key to decrypt the files if the ransom is paid. Ransomware kits are available to criminals to buy or rent relatively cheaply, enabling this crime to be relatively common. The European Union Agency for Cybersecurity (ENISA) has identified substantial increases in ransomware attacks centred on European Union countries.[10]

Social engineering: This is the act of deceiving or manipulating individuals into providing confidential or personal information that is subsequently used to carry out a fraudulent activity. The

criminal will employ tactics that gain the trust of the victim and exploit common actions of human behaviour.[11] Criminals employ numerous methods to achieve their aim, such as creating a sense of urgency or curiosity in the victim. Criminals can also be more targeted and create content which appears authentic and deceives victims into thinking it is legitimate and thus either revealing sensitive information or performing a task that they would not have done without verification. The availability of AI tools has allowed criminals to create ever more convincing material. It is now possible for fraudsters to create tailored messages across multiple countries in different languages; AI tools make this possible in a fraction of the time such fraudulent activity previously took.

Denial of service: Attacks known as denial of service (DoS), or distributed denial of service (DDoS) (using control over others' computers), are the act of bombarding connections to a website or system with requests which then overloads the system and prevents an organisation from operating their normal business. This influx in the volume of requests to a system effectively shuts it down and denies service to regular clients and customers. The cyber assault can go undetected for some time, resulting in prolonged damage to a business. The time and cost for a business and damage to professional reputations can be significant. This type of attack has variants, one of which is referred to as an 'advanced and persistent' DoS attack, which have a tendency to be carried out by attackers that are more sophisticated.

Disinformation/misinformation: The spread of false or misleading information is nothing new; it has always been a feature of political, business and social discourse. Its impact and volume would rise and fall with social changes and upheavals, most notably at times of war and plague. In the modern era, the internet and the ubiquity of social media has magnified the reach and super-charged the speed at which false information can spread. The wane of traditional media and the rise of partisan websites and platforms has generated content for a world that consumes information in a completely new way. The damage to civil society is enormous, from the spread of false information on infectious diseases and vaccine hesitancy to climate change rejection and the spread of extreme views against segments of the population. It can also have a significant effect on democratic institutions, according to the OECD, which stressed that the combination of AI language models and disinformation can lead to deception on a large scale and damage public trust. Significant disinformation campaigns targeting the European Union and its allies have increased from Russian-associated social media accounts, raising fears over its impact on the 2024 European elections. The European Commission published a 2018 Code of Practice on Disinformation,[12] followed in 2021 by detailed guidance in addition to the code of practice; this was the subject of a review process, with the resultant publication of a strengthened code of practice in 2022.[13] A recent Commission report on the application of the risk management framework in response to Russian disinformation campaigns found that the Kremlin's ongoing campaigns not only form an integral part of Russia's military agenda, but also cause risks to public security, fundamental rights and electoral processes inside the EU.[14] The WEF, in its 2024 Global Risks Report, said that politics could be disrupted by the spread of AI-driven misinformation and disinformation. It expressed concern that the propagation of false information could influence key looming elections, potentially posing the biggest short-term threat to the global economy.

Legal, policy and institutional framework

International efforts

As illustrated above, cybercrime is a widespread and lucrative illicit business. State actors are increasingly resorting to cyber interference to weaken opponents and other states. Accordingly, the international community takes cybersecurity seriously, as illustrated by initiatives such as those from the Council of Europe, notably the 'Budapest Convention' on cybercrime, which serves as a guideline for any country developing domestic legislation on cybercrime and as a framework for international cooperation between State Parties to the Convention. It provides for: (i) the criminalisation of conduct – ranging from illegal access, data and systems interference to computer-related fraud and

child pornography; (ii) procedural powers to investigate cybercrime and secure electronic evidence in relation to any crime; and (iii) efficient international cooperation. It is open for accession by any country. The Convention is supplemented by a First Additional Protocol covering the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189), and a Second Additional Protocol on enhanced international cooperation and disclosure of electronic evidence. Under Council Decision 2023/436, EU Member States are authorised to ratify the Second Additional Protocol. The Cybercrime Programme Office of the Council of Europe (C-PROC) assists countries worldwide to respond to the challenges of cybercrime on the basis of the Budapest Convention. It has a capacity-building function, complementing the work of the Cybercrime Convention Committee (T-CY), which represents the State Parties to the Budapest Convention.

EU policy and legislative framework

The EU has developed a comprehensive policy and legislative framework to address cybersecurity and cybercrime, reflecting its commitment to safeguarding digital spaces. Key directives and regulations focus on protecting critical infrastructure, enhancing network security, and defining cybercrimes and related sanctions, as well as regulating access to electronic evidence, the operation of online platforms, and AI.

The EU has a dedicated cybersecurity strategy for the Digital Decade, which forms a key component of Shaping Europe's Digital Future, the Commission's Recovery Plan for Europe and the Security Union strategy 2020-2025. The strategy shows how the EU has addressed cybersecurity and cyber-enabled threats. It addresses the security of essential services, such as hospitals, energy grids, railways and the proliferation of connected objects in homes, offices and factories. It also outlines plans to work with partners around the world. Moreover, it highlights how a Joint Cyber Unit can be an effective response to cyber threats. The strategy aims to ensure a global and open internet with strong safeguards where there are risks to security and the fundamental rights of people in Europe. Following the progress achieved under the previous strategies, it contains concrete proposals for deploying three principal instruments. These instruments are regulatory, investment and policy initiatives, and will address three areas of EU action:

- resilience, technological sovereignty and leadership;
- building operational capacity to prevent, deter and respond; and
- advancing a global and open cyberspace.

The EU is committed to supporting this strategy through investment in the EU's digital transition, which would quadruple previous levels of investment. Beyond the strategy, the focus on cybercrime is evident in the delineation of the EU's priorities in combating serious and organised crime as outlined in the European Multidisciplinary Platform against Criminal Threats (EMPACT 2022-2025). The aim is to 'target the criminal offenders orchestrating cyber-attacks, particularly those offering specialised criminal services online'.

Based on Article 83 of the Treaty on the Functioning of the European Union (TFEU), Directive 2013/40 on attacks against information systems is the principal EU act specifically addressing cybercrime. The directive aims to fight cybercrime, promote information security, and enable greater cooperation between relevant authorities. It introduces new rules in relation to a number of offences directed against information systems, including outlawing the use of so-called 'botnets' – malicious software designed to take remote control of a network of computers. The main types of criminal offences covered are attacks against information systems, including denial of service attacks, interception of data and botnet attacks.

The 2019 Directive (EU) 2019/713 on non-cash payments updated the legal framework, which enabled more effective law enforcement against fraud and counterfeiting of non-cash means of payment. The directive includes common definitions in the areas of fraud and the counterfeiting of non-cash means of payment and has extended criminal liability to virtual currencies and digital wallets. The directive defines the constituent elements of criminal conduct, including fraud related

to information systems and tools used to commit offences. While the directive includes rules on jurisdiction, investigative tools, exchange of information and the setting up of reporting channels for the offences, it also strengthens assistance to and support for victims. It adapts the rights of victims under Directive 2012/29 to the special needs of victims of fraud in conjunction with non-cash means of payment. It also obliges Member States to ensure that natural and legal persons can obtain specific information and advice on how to protect themselves against the negative consequences of the offences.

A report from the European Commission, the first under Article 21 of Directive 2019/713, assessing the extent to which Member States have taken the necessary measures to comply with the Directive, noted that fraud concerning non-cash payments was a source of income for organised crime and enabled other criminal activities such as terrorism, drug trafficking and trafficking in human beings. Moreover, it noted the cross-border nature of the crime and the significant losses incurred, pointing out that fraud where a card was not physically present amounted to €1.5 billion and accounted for 80 % of card fraud in 2019. The report did find, though, that the Directive has led to substantive progress in criminalising fraud and counterfeiting of non-cash payments.

The Network and Information Security Directive (NIS2) aims to bring about a high level of cybersecurity across the EU for both countries and economic entities. The Directive is modernising the existing legal framework in order to keep up with the expanding use of digital solutions and the increasing and evolving cyber threats. The Directive will ensure that key sectors take appropriate cybersecurity measures, thereby protecting services for EU citizens.

In December 2023, Member States agreed to a common position on the Cyber Solidarity Act. The proposal is intended to strengthen the EU's capacity to deal with cybersecurity threats and incidents through, among other measures, the establishment of cross-border and national security operations centres (SOCs), creating a 'European Cyber Shield'. It aims to support detection and awareness of cyber threats and strengthen preparedness of critical infrastructure for such threats. The agreement will allow the Council to enter into trilogue negotiations with the European Parliament on the final version of the proposed legislation.

Regulation (EU) 2023/1543 and Directive (EU) 2023/1544 are part of the legislative package on electronic evidence in criminal matters. Regulation (EU) 2023/1543 is intended to allow competent authorities from one Member State to request directly from a service provider established or represented in another Member State access to or preservation of electronic data needed for investigation and prosecution of crimes. Directive (EU) 2023/1544 lays down harmonised rules on the designation of establishments and the appointment of legal representatives of certain service providers that offer services in the EU for the purpose of gathering electronic evidence in criminal proceedings.

The Digital Services Act (DSA) regulates online platforms and intermediaries. Its aim is to harmonise and address illegal and harmful content and to tackle the spread of disinformation. It is designed to safeguard users and protect consumers and their fundamental rights online. The DSA will be enforced by the European Commission in collaboration with national authorities, who will ensure compliance of platforms established in their country. Taken together with the Digital Markets Act, which will regulate large digital platforms, providing services, such as online search engines, app stores, and messenger services, it aims to create a safer digital space.

The AI Act is an initiative to regulate AI through a risk-based approach to protect the public. The Council presidency and the European Parliament's negotiators reached a provisional agreement on the AI Act on 9 December 2023. It aims to regulate AI through a tiered system, with the highest level of regulation applying where the highest risk exists to fundamental rights, human values and health and safety. Obligations are placed on service providers, including basic rules on the disclosure of the data they use for machine learning.

A provisional agreement has also been reached on the proposed Cyber Resilience Act. The new legislation introduces cybersecurity requirements for the design, development and upgrade of all

products that are connected directly or indirectly to another device or network. This will close the gaps and ensure that products with digital components are made secure throughout the supply chain and throughout their lifespan. This will place responsibility for compliance with cybersecurity requirements on manufacturers. It will also allow consumers to factor cybersecurity into their requirements when choosing and using digitally connected products.

Agencies and operational mechanisms

Europol is the EU's law enforcement agency assisting Member States with their fight against serious international crime and terrorism. In response to the growing threat that cybercrime posed to EU Member States and their citizens, Europol set up the European Cybercrime Centre (EC3). EC3 provides specialised assessments of emerging trends and the methods employed by criminals; supports training and capacity building of Member States' police forces; and cooperates with EU institutions, international organisations, law enforcement agencies and the private sector to help strengthen capabilities in response to cybercrime.

Since its establishment in 2013, EC3 has made a significant contribution to the fight against cybercrime and has been involved in many high-profile operations and hundreds of operational-support deployments. It publishes the Internet Organised Crime Threat Assessment (IOCTA), its flagship strategic report on key findings and emerging threats and developments in cybercrime – threats that impact governments, businesses and citizens in the EU – the most recent of which is the IOCTA 2023 report. Moreover, EC3 launched the **Joint Cybercrime Action Taskforce (J-CAT)** in September 2014. It is situated in Europol's cybercrime centre, helping to fight cybercrime within and outside the EU, and tackling cyber-dependent crimes, payment fraud and online child sexual exploitation. J-CAT has been involved in a number of high-profile operations, with notable successes.

The **European Union Agency for Cybersecurity (ENISA)** was created by Regulation (EC) No 460/2004. It has since been enhanced by the Cybersecurity Act, which gave it a permanent mandate and important new tasks for the digital single market, such as its future role in the European cybersecurity certification framework. This is a scheme at EU level that aims to provide criteria with which products, services and processes will have to comply in order to achieve certification conformity. ENISA contributes to EU cyber policy and enhances cybersecurity with its certification schemes; works with Member States, EU bodies and key stakeholders to strengthen the EU's infrastructure and resilience; and promotes cooperation between Member States, EU institutions and agencies in relation to cybersecurity issues. One of its aims is to eliminate duplication of effort among stakeholders, with more efficient use of limited expertise in the field of cybersecurity. It is also promoting the horizontal implementation of cybersecurity across future EU policy.

MAIN REFERENCES

Negreiro M., High common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, EPRS, European Parliament, October 2023.

Shahidullah S., Coates C. and Kersha-Aerga D. (eds), Global Cybercrime and Cybersecurity Laws and Regulations: Issues and Challenges in the 21st Century, Nova Science Publishers Inc., 2022.

Kononenko V., Improving the common level of cybersecurity across the EU, EPRS, European Parliament, February 2021.

Cybersecurity, our digital anchor, European Commission, Joint Research Centre, 2020.

Juniper Research, The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024, September 2018.

European Crime Prevention Network, Cybercrime: A theoretical overview of the growing digital threat, 2016.

ENDNOTES

1 S. Cross, S. Hirrle and M-A. Lim, Cybercrime Strategy Guidebook, Interpol, 2021.

2 A 2016 EPRS study estimated the cost of non-Europe in the field of organised crime (including cybercrime), and the cost of corruption was at least €71 billion annually.

3 Flash Eurobarometer FL496: SMEs and Cybercrime, European Commission, 2022.

4 Europeans' attitudes towards cyber security, European Commission, 2020.

5 Cost of a Data Breach Report, IBM, 2023.

6 Global ransomware threat expected to rise with AI, NCSC.

7 Cyber Dimensions of the Armed Conflict in Ukraine Q3 2023, Cyber Peace Institute.

8 Insights Into the Footprints of Hacktivists, Radware, 2023.

9 Dutch organisations targeted by DDoS attacks, Netherlands National Security Centre, 2023.

10 ENISA Threat Landscape 2023, pp. 51-60.

11 How fraudsters can use the forgotten details of your online life to reel you in, *The Guardian*, 2021.

12 Code of Practice on Disinformation, European Commission, 2018.

13 Strengthened Code of Practice on Disinformation, European Commission, 2022.

14 Digital Services Act: Application of the risk management framework to Russian disinformation campaigns, OPOCE, 2023.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)