MTA Law Working Papers
2024/16

The Latest Trends in Cybercrime and Their Impact on Cybersecurity Regulation – Cyber Threats and Cyber Resilience in the European Union

Mezei Kitti – Nagy Tamás

ISSN 2064-4515
http://jog.tk.mta.hu/mtalwp
Társadalomtudományi Kutatóközpont – MTA Kiválósági Kutatóhely
HUN-REN Centre for Social Sciences – MTA Centre of Excellence

MEZEI, KITTI[1] – NAGY, TAMÁS[2]

THE LATEST TRENDS IN CYBERCRIME AND THEIR IMPACT ON CYBERSECURITY REGULATION
– CYBER THREATS AND CYBER RESILIENCE IN THE EUROPEAN UNION[3]

Abstract

The research paper examines the evolving landscape of cybercrime and its implications for cybersecurity regulation within the European Union. The analysis highlights significant trends in cyber threats, including the escalation of phishing attacks, mobile banking fraud, and ransomware incidents in the post-COVID-19 era. The study elucidates the increasing sophistication of cybercriminal techniques, with a particular emphasis on integrating artificial intelligence and social engineering methodologies to enhance the effectiveness of cyber attacks. Furthermore, the paper scrutinises the European Union's regulatory responses, notably the Digital Operational Resilience Act (DORA), the NIS2 Directive, and the Markets in Crypto Assets Regulation (MiCA), which collectively aim to strengthen cybersecurity and resilience across vital sectors. By assessing these developments and legislative measures, the research underscores the critical need for comprehensive and adaptive cybersecurity frameworks to mitigate the escalating risks posed by contemporary cyber threats.

Keywords

Cybercrime, cybersecurity, phishing, mobile banking, cryptocurrencies

I. Introduction

According to Eurostat, 22% of EU businesses experienced negative consequences from security incidents involving information and communication technology (ICT) systems in 2021 (Eurostat, 2023), compared to 12% in 2018 (Eurostat, 2018). These consequences include downtime, unavailability of services, or misuse of data. While a significant proportion of incidents are due to hardware or software failures (see, one of the largest IT outages was triggered by a botched software update from security vendor CrowdStrike, affecting millions of Windows systems around the world), cyber-attacks are also rising. For example, exploiting unknown or unpatched software flaws is becoming more common in zero-day attacks as attackers react quickly to discovered vulnerabilities. The number of ransomware attacks

[1] Senior Research Fellow, HUN-REN Centre for Social Sciences, Institute for Legal Studies.

[2] Police Major.

[3] The publication was prepared in the framework of the Hungarian Academy of Sciences' high-risk grant for research on post-COVID phenomena and supported by the European Union project RRF-2.3.1-21-2022-00004 within the framework of the Artificial Intelligence National Laboratory and by the Ministry of Innovation and Technology NRDI Office within the framework of the FK_21 Young Researcher Excellence Program (138965).

increased by 41%, and email-related attacks (IBM Security, 2022), including phishing, also increased by 48% in 2022 (Security Staff, 2022). Attackers have also focused on disrupting supply chains (Chikán and Gelei, 2005) that have been present since the COVID-19 pandemic and even more so since the outbreak of the Russia-Ukraine war (Bulletproof, 2022).

Cybercrime damage extends beyond organisations, with over 45% of security breaches involving personal data. Citizens worldwide are exposed to various risks, such as identity theft and financial fraud. The damage can also be non-economic, with hospitals and critical infrastructure such as nuclear power plants increasingly targeted, and human life can also be at risk. For instance, in Germany, a patient died when the nearest hospital could not provide emergency care due to a ransomware attack (Vandezande, 2024.)

Europol's Internet Organised Crime Threat Assessment (IOCTA) highlights that cyber threats are evolving both in quantity and quality. The COVID-19 pandemic has permanently transformed personal and professional life, creating new demands and opportunities for cybercriminals. Cybercriminals target not only corporate and government sectors but also the general public, facilitated by widespread teleworking. Attackers exploit network vulnerabilities, and malware has proliferated, threatening both computers and mobile devices due to the extensive use of mobile banking and financial applications (e.g. for crypto or exchanges).

One of the most visible trends was the increased number of frauds related to online shopping and related delivery and logistics services. The volume of e-commerce has barely decreased, even compared to the COVID-19 pandemic era, which suggests that the sector will likely continue to show stable indicators in the coming years. With a wide range of methods, online shopping and sales are now one of the most common starting points for phishing attacks. Perpetrators aim to trick their victims into downloading malicious applications they distribute or to obtain their credit cards and credentials (Europol, 2023b).

Europol's previous reports (Europol, 2021) have also addressed the phenomenon of perpetrators favouring complex systems over the IT systems of one organisation or company, which, due to the nature of their supply chain, can access dozens or hundreds of other systems. The rapid transition in this regard is illustrated by the number of incidents in recent years that have revealed intrusions into hundreds or even thousands of customers' IT systems. One such incident was the SolarWinds incident, which is interesting because it did not directly target a specific network but was compromised via a third party. Unaware of the cyber attack, the company started sending out updates of Orion software, used by large corporations and governments, to thousands of users in March 2020, which already contained the malicious code of the perpetrators. Over 18,000 users have installed this update, including major players like FireEye, Microsoft and Deloitte (Oladimeji and Kerner, 2023).

In 2022, global attention shifted from the COVID-19 pandemic to the conflict between Russia and Ukraine. This geopolitical shift highlighted the agility and adaptability of cyber criminals, who swiftly exploited the evolving situation to develop a range of sophisticated exploits. Under the pretext of supporting Ukraine, fake websites were set up to raise money under the guise of humanitarian efforts, using URLs that contained misleading keywords. In some cases, the fraudsters posed as celebrities who were running or supporting real campaigns or spoofed the domains of humanitarian organisations and asked people to donate in cryptocurrency (Europol, 2023c).

II. Post-COVID trends in cybercrime and challenges for cybersecurity

A. New techniques of phishing

Phishing is a special form of psychological manipulation (social engineering) attack in which the perpetrator poses as a trusted person or organisation (e.g. a bureaucrat, bank officer, etc.) to trick the victim into providing confidential information. This type of fraud commonly employs a sense of urgency to disrupt the victim's ability to analyse the situation critically. If urgency fails, attackers may resort to scare tactics to coerce compliance. Examples include threats to suspend user accounts, warnings of supposed hacking incidents, impersonation of government officials with threats of fines or legal action, fabricated pleas from friends or family members in urgent need, blackmail with compromising content or posing as technical support to address a non-existent bug. Phishing campaigns can be indiscriminate, targeting large groups, or highly specific, focusing on individual victims (Alkhalil et al., 2021).

Phishing can be a threat on its own and when combined with other methods. One of the best examples of this is Open Source Intelligence (OSINT), which is the collection and processing of information available to anyone (Me, 2023). OSINT can be sourced from any source and any interface, but the most common way is that perpetrators or groups of perpetrators use the online space to collect data on their intended targets.

Applications such as Facebook or Instagram store and display much information that can be misused, especially if the profile is public. In addition to social networking sites, professionally themed sites are becoming increasingly popular, which aim to build and maintain professional contacts, which can also play an important role in job search or career development. One example is LinkedIn, where a quick registration allows you to see not only the career history or current position of a user (e.g. a senior executive) but also a list of people working for a company and their positions. In many cases, this and similar information can be supplemented by leaked passwords and usernames, which, even through typical password- building logic, can facilitate access to a particular interface or mail system. The latter is an ideal example, as accessing an email account can make any perpetrator feel like a goldmine, as it can provide information about the user and others that may be essential for later use.

The most significant threats continue to be forms of fraud involving cashless payment systems, in particular, business e-mail compromise (BEC). Despite its lower volume, this type of crime causes more financial damage than any of the other methods of perpetration described above. The most common types of BEC are CEO fraud, where perpetrators impersonate the head of a company and make urgent payment requests to finance staff, and payment fraud, where fraudsters pose as business partners and request payment from fictitious invoices or use real invoices with bank details of real suppliers altered (spoofing). In spoofing, attackers spoof different identifiers - such as IP addresses, email addresses, websites, and phone numbers - to get confidential information from us. To carry out the fraud, the fraudsters may gain unauthorised access to the company's mail system in advance through various cyber-attacks, thus gaining insight into internal structures and operational procedures. In some cases, fraudsters use phishing techniques to obtain personal data, which they then use to monitor and influence corporate communications (Nagy, 2018).

This type of crime is becoming more targeted every year, which shows that, in most cases, it is committed after a more extended preparation period. The modus operandi of the offences under investigation is also becoming more sophisticated, which is also since the attacks rely heavily on psychological manipulation, which also means that classical protection measures are no longer sufficient to avoid victimisation. The increasing sophistication of CEO fraud is reflected in the use of deepfake technology. In one case, the perpetrators used a voice recording generated using the new technology to impersonate the CEO of a company during a telephone conversation. The deception was successful, as the perpetrators could swindle the transfer of an amount equivalent to €35 million (Europol, 2022b).

In February 2024, Pepco's Hungarian business was attacked by phishing attacks, causing around HUF 6 billion in damages to the company. According to the company's statement, the incident resulted from a BEC attack, a specific type of phishing attack in which attackers are believed to have posed as company employees, business partners or executives to authorise fraudulent transactions. The emergence of artificial intelligence has given fraudsters an additional significant advantage, allowing them to create phishing emails in different languages that are more convincing and free of grammatical errors. These tools can mimic the language and style of corporate communications, even the person's own vocabulary, increasing the likelihood of deception (Pepco, 2024).

Phishing attacks and payment fraud are typically criminal offences, and, in terms of domestic legislation, they correspond to traditional fraud under Section 373 of Act C of 2012 on the Hungarian Criminal Code, as they cause damage by defrauding a natural person for unlawful gain (Mezei, 2020).

B. Mobile banking and online fraud

With the widespread adoption of mobile banking, mobile malware, particularly Trojans, is an increasingly severe threat. In 2020 and 2021, Cabassous and FluBot were the most prevalent mobile malware, causing significant damage across Europe and the US. The key to the success of these attacks is the so-called overlay feature, which allows the malware to mask the original application when running applications such as financial/payment or crypto stock market applications by opening a phishing interface similar to the original. This fake interface extracts and transmits user data (username, password). FluBot uses the Domain Generation Algorithm (DGA) to create random domains and then connects to them to send the acquired data to the C2 (Command and Control) server. Malware such as FluBot is characterised by the fact that it obtains the infected device's contact details (contact list) and sends text messages to ensure its own propagation (Europol, 2022a).

Phishing scams using social engineering techniques that specifically target banks' customers have become increasingly common in recent times. The modus operandi is relatively simple: the perpetrators call the victims, typically via VoIP, and pretend to be employees of a financial institution (normally used by the victim) or a public authority (law enforcement, banking supervision). During the call, victims are informed that a suspicious transaction has been detected and are asked to provide personal information to protect the customer or are instructed to transfer their money to an account considered secure. In customer cooperation cases, it is common for victims to be asked to download remote desktop access programs (e.g. AnyDesk) and then use this to take control of the victim's device or net bank.

It is also typical to refer to the reconciliation of personal data, where the customer is asked to reconcile personal data to prevent or avoid suspicious transactions. This includes access and card details, as well as the provision of the two-factor authentication code. Such and similar (vishing-type) scams can be well combined, in this case, with other phishing techniques, such as sending fraudulent emails using the branding, logo, language and other elements of a well-known (and trusted) financial and credit institution. The older generation is more vulnerable to phishing attempts, especially via telephone (vishing) and text messages (smishing). Quishing, or QR code phishing, also emerged in 2023 (Europol, 2024b). Because social engineering techniques work well with minor changes, criminals can launch increasingly targeted campaigns by fine-tuning the technical details (Iacono et al., 2022).

Tokenised bank cards have become a popular payment instrument. These cards are issued after tokenisation, which converts the cardholder's sensitive data into a randomly generated sequence of numbers known as tokens. Tokenisation protects the cardholder; the data is highly secure, and the token is unique, unbreakable and fraud-proof. Tokenised cards are typically found in mobile payment services and digital wallets and can be linked to subscriptions to online services and other online payments. Multiple tokens can be issued for a single payment card, each with a unique number and used only for one application or device. Tokenisation has been described as the next evolution of digital payments, triggered by the introduction and uptake of contactless payments. Instead of using their plastic cards, cardholders increasingly use their smartphones to make payments, which would only be possible with the tokenised cards stored in these devices. At the same time, fraudsters use various techniques to obtain the one-time passwords associated with tokenised cards that banks send to customers to authorise money transfers. They can then link the obtained bank card details to existing mobile payment systems to buy products or withdraw cash (in countries where this is allowed) (Europol, 2023c).

From a criminal law point of view, if the perpetrators only obtain the login data required for Internet banking or other financial platforms and use them to cause damage by an operation on the information system (e.g. by making a bank transfer), then they are committing information system fraud under Section 375(1) of the Hungarian Criminal Code. Suppose they obtain credit card data without authorisation and use the information system to cause damage (e.g. purchase in an online shop using the credit card). In that case, they may be liable for the fraudulent use of an electronic cash substitute payment instrument as defined in paragraph 5. When distinguishing between the different types of fraud, it should be noted that fraud committed by using an information system involves directly using it to cause material damage, whereas fraud always involves defrauding a natural person (Mezei, 2020; Ambrus, 2022).

C. Mobile viruses and ransomware

Malware designed for mobile devices has been with us for almost a decade and has evolved considerably. The first significant threat in the last decade was malware, whose main purpose was to show victims as many advertisements as possible and install (and then launch) the advertised applications silently. In some cases, aggressively displaying pop-up ads and delaying the execution of user commands can render the device unusable. With proper vigilance, these threats can be filtered out by the average user, which - in the longer term - has led to malware designed for mobile devices also starting to evolve, incorporating increasingly complex features that are capable of deception. With the rise of mobile banking, it has become clear that the battle to obtain valuable data is set to take on a new dimension. Programmes disguised as mobile apps appeared that collected relevant data, such as personal and financial information, without the user's knowledge and then transmitted it based on pre-written commands. However, the early Trojan malware, which in retrospect seemed relatively simple, was slowly being replaced by programs with more complex designs and functionality. The Cabassous malware, and later Flubot, which exploited the successful mechanism of action of Cabassous, received considerable press coverage across Europe.

Cabassous, followed by Flubot, was released in Spain and Portugal between December 2020 and January 2021 and swept the continent in just over six months. The malware was complex, but in hindsight, it is relatively easy to reconstruct why it was so successful. Users received a short text message from a domestic number, but one they needed to recognise. The SMS contained a brief text message informing them that information on the delivery of the package/mail they had ordered was available via a link, also included in the text. Most people, unsuspecting that online ordering and related parcel delivery services were becoming commonplace due to the prevalence of COVID-19 at the time, click on the embedded link, which redirected the user to a page that used the branding of a parcel delivery company identified in the text. The apparent query about the parcel's delivery status required the user to install a data package. The malware was installed on the device, in many cases, despite the device's warning, i.e. with the user's active involvement, where it began to collect and transmit data relevant to the offenders on the device based on pre-written scripts. This included the contents of the contacts list (phonebook), a list of applications installed on the device, text messages, and similar text content.

The primary targets of the malware were so-called financial or crypto service-related apps, whose presence in the app list clearly indicates that the user is conducting financial or other transactions on the device, meaning that sensitive financial data can be obtained from the device. When accessing such apps, the malware used the so-called overlay function to "generate" an app that is identical or similar to the open app, where the user could enter login details. Since the malware transmitted all data in real time to a C2 server and had access to text messages, it could even transmit the two-factor authentication (2FA) code (received via SMS) to the perpetrators. This allowed the attackers to log in in real time and record transfers or other transactions on behalf of the user.

The malware spread by exploiting privileges over text messaging functions, using directory information sent to the C2 server to send text messages from infected devices only to caller numbers that were not in the directory or call log of the device. Thus, in many cases, in addition to unauthorised financial transactions being recorded, other losses were incurred due to the charges for text messages sent without the users' knowledge. Flubot caused the most significant damage in Spain and Finland, where millions of Android devices were infected. The considerable threat prompted Europol EC3 (Europol Cyber Crime Center) to launch a joint operation involving 11 countries, including Hungary. Major infrastructures linked to the malware were shut down during the operation in June 2022 (Europol, 2022c).

In addition, ransomware viruses remain a particular threat, increasingly exploiting the growing prevalence of teleworking and the technical features that make it possible. These malicious programs work by encrypting files or even entire data files stored on the infected information system, making them inaccessible to the victim and demanding extremely high ransoms, up to millions of dollars, in exchange for the recovery code that unencrypts them. The software may also set a payment deadline, after which the data is permanently inaccessible. It is almost impossible to identify the perpetrators because the ransom is usually requested in cryptocurrency, payment of which does not guarantee that the encryption will be decrypted (For more about this, see Custers et al., 2020).

With the emergence of the pandemic, attacks targeting healthcare-related institutions (e.g. hospitals, clinics, social care homes) have also become more frequent. By scanning various networks, perpetrators can gain important information about insecure remote desktop access (RDP) applications and constantly monitor for disclosed virtual private network (VPN) vulnerabilities.

LockBit has become widely known as the world's most widespread and malicious ransomware by 2022, causing billions of euros in damage. The program is backed by the LockBit ransomware hacker group, who follow the ransomware-as-a-service business model (Europol, 2023a), which means that a core team creates the malware and runs its website while licensing and selling its code to affiliates launching attacks. LockBit has a worldwide presence, with hundreds of affiliates recruited to carry out ransomware attacks using LockBit's tools and infrastructure. Ransom payments were split between the LockBit core team and affiliates, who received, on average, three-quarters of the ransom payments collected. The ransomware group is notorious for experimenting with new methods to force its victims to pay ransoms. Triple extortion is one such method, which involves encrypting the victim's data and threatening to leak it. It also includes DDoS attacks as a further step in the pressure (Europol, 2024a).

Recent law enforcement operations and the leak of ransomware source codes (such as Conti, LockBit, and HelloKitty) have caused a fragmentation of active ransomware groups and the emergence of new variants. The leaked codes, coupled with the rapid advancement of AI tools, are likely to accelerate the development of new ransomware variants. These conditions provide both the incentive and opportunity for ransomware groups to splinter and rebrand. This not only hinders investigations and attribution but also allows them to exploit the ensuing chaos to capture a larger share of the criminal market (Europol, 2024b).

Cyber awareness and and resilience is key to preventing cyber attacks. The official website of the Hungarian Police provides an excellent example of crime prevention advice, including detailed guidance on topics such as the FluBot, ransomware, and ransom emails (Gyaraki, 2022).

According to Article 423 of the Criminal Code, these cyber attacks are punishable in the case of criminal offences of the information system or data breach, unauthorised circumvention or breach of a measure ensuring the protection of an information system (typical hacker attacks), unauthorised obstruction of the operation of an information system (DDoS attacks) and various unauthorised manipulation of data, alteration, deletion or rendering inaccessible of data (malware and ransomware attacks) (Mezei, 2020).

As technology continues to evolve, there is growing concern that large language models (LLMs), such as the better-known ChatGPT, can be used for criminal purposes and are being developed specifically for this purpose. An anonymous developer, who went by the name of last/laste, has created WormGPT, which is a doppelganger of ChatGPT but could be used to help cyber criminals. The hacker chatbot has no technical limitations that prevent it from answering questions about illegal activity and helping to carry out cyber attacks, unlike traditional LLMs such as ChatGPT. For example, it allows users to obtain sensitive data through social engineering, typically from employees of large companies. To create WormGPT, they used the relatively outdated, open-source 2021 large GPT-J language model as a platform and trained it with materials related to malware development.

Another malicious LLM became available later, in July 2023. The author promotes his product FraudGPT on several dark web forums and Telegram channels. FraudGPT is described as a tool that can create undetectable malware, write malicious code, search for vulnerabilities and security holes, create phishing pages, and learn hacking techniques (Erzberger, 2023).

Today, cybercrime has become a service-based business model. Tools and programs for launching various attacks can be used as a service or even purchased on the online forums of the dark web. Executing cyber-attacks has become more accessible due to the easy access to the knowledge, programs, and even the ready-made infrastructure needed to commit the crime. Because of this, both EU and national legislation now define preparatory acts as separate crimes—for example, the Hungarian Criminal Code. The criminal offence of circumvention of an information system protection measure under Section 424 of the Hungarian Criminal Code criminalises the creation, transfer, disclosure, acquisition or distribution of a password or computer program necessary for or facilitating the commission of an information system offence as well as the provision to another person of organisational knowledge relating to the creation of a password or computer program (Mezei, 2020).

Generative AI has yet to leave the field of cybersecurity and ethical hacking untouched. For example, HackerGPT is available to help cybersecurity experts quickly assess potential risks, and PentestGPT helps experts find vulnerabilities in information systems faster and more efficiently to fix them faster (penetration testing).

DarkGPT promises to be an easy-to-use tool that anyone just starting in the OSINT world can easily try. According to its creator, it is best suited for detecting leaked usernames and passwords. Various tools based on ChatGPT have already been created for the cybersecurity community, some of which we have covered: OSINVGPT, PentestGPT, WormGPT, BurpGPT and HackerGPT, and DarkGPT now complements this (Lee, 2024).

D. Cryptocurrencies

Cryptocurrencies remain popular, especially for users of dark web marketplaces that offer illegal goods and services. To ensure anonymity, the so-called privacy coins, such as Monero, dash or Zcash, are the most popular among these circles, as they offer a high level of privacy and almost complete protection of the user's data due to their operating mechanism. Criminals also use mixers, swap services and other methods to launder their illicit proceeds in Bitcoin and other traceable crypto assets quickly and efficiently. This is also helped by the existence of cryptocurrency exchanges that are less cooperative with the authorities, as well as service providers with weak know-your-customer (KYC) protocols, which do not have meaningful information about the true identity of their customers. At the same time, the role of cryptocurrencies is growing, not only as a means of payment but also in relation to investment fraud. These scams typically advertise services and platforms that are more lucrative than other trading or investment opportunities, but these platforms are typically deceptive, meaning that customers do not actually have control over the amount of money invested and that the payment of profits from cryptocurrencies is misleadingly linked to the payment of non-existent commissions and other fees or taxes.

Directive (EU) 2015/849 of the European Parliament and of the Council, as amended by Directive (EU) 2018/843 of the European Parliament and of the Council, introduced the concept of virtual currency and included providers of virtual currency to fiat currency conversion services and custodian wallet providers among the entities subject to anti-money laundering and counter-terrorist financing requirements under EU law (Wahl, 2021). Recent international developments, in particular within the Financial Action Task Force (FATF) framework, now call for the regulation of additional categories of virtual currency service providers not yet covered and for a broadening of the current definition of virtual currency. Therefore, at the end of May 2023, the EU adopted new legislation on cryptocurrencies.

To make it more difficult for criminals to circumvent anti-money laundering rules through cryptocurrencies, the European Parliament and the Council adopted Regulation 2023/1113 on data accompanying funds transfers and certain transfers of crypto assets and amending Directive (EU) 2015/849. EU lawmakers have recognised that certain crypto asset transfers are associated with particularly high-risk factors for money laundering, terrorist financing and other criminal offences, particularly transfers related to products, transactions or technologies aimed at enhancing anonymity, including encrypted wallets and mixers (mixers, tumblers).

The Regulation revises and extends the scope of Regulation 2015/847 with regard to cryptocurrency asset transfers to ensure financial transparency and provide the EU with a stable framework for the exchange of cryptocurrency assets in line with international standards. Regulation (EU) 2015/847 was adopted to ensure the uniform application across the EU of the requirements imposed by the FATF on providers of electronic funds transfers, in particular, the requirement for payment service providers to accompany transfers of funds with information on the payer and payee. Following the new amendments, virtual asset providers should ensure that transfers of virtual assets are accompanied by information on the originators and beneficiaries of those transfers, irrespective of the transfer amount. In addition, the virtual asset service providers should collect, store and share the information with their counterparties at the other end of the virtual asset transfer and make it available to the competent authorities upon request. The new regulation will apply from 30 December 2024 (Pingen, 2023).

The European Parliament and the Council have adopted new rules - Regulation 2023/1114 on Markets in Crypto Assets (MiCA). The MiCA proposal was first tabled on 24 September 2020 and is part of the EU's wider digital finance package, which aims to develop a European approach to foster technological progress and ensure financial stability and consumer protection.

The MiCA Regulation aims to protect investors and preserve financial stability while encouraging innovation and promoting the attractiveness of the crypto asset sector. The MiCA will also protect consumers from some of the risks associated with investing in cryptocurrency assets, for example by imposing stricter requirements on cryptocurrency asset providers and holding them liable if they lose investors' cryptocurrency assets, helping consumers to avoid fraudulent schemes. Issuers of stablecoin will be required to hold sufficient liquid reserves in a 1:1 ratio and partly in the form of deposits. Overall, stablecoins will be supervised by the European Banking Authority (EBA), and the issuer's presence in the EU will be a prerequisite for any issuance. The MiCA will not cover non-fungible tokens (NFTs) unless they fall under existing categories of cryptocurrencies. The MiCA Regulation will apply from 30 December 2024. Notwithstanding this, several provisions will apply earlier (Pingen, 2023).

D. Cybersecurity and cyber resilience

Cybercriminals often target financial institutions. If successful, their attacks can have serious consequences, as they can gain access to large amounts of sensitive financial and personal data, so it is important to focus on security and prevention. To harmonise the protection against cyber-attacks, the European Commission has therefore prepared a single set of rules, Regulation (EU) 2022/2554 on Digital Operational Resilience in the Financial Sector (DORA Regulation), which entered into force on 16 January 2023 and will apply from 17 January 2025.

The legislation ensures that financial institutions within the EU are effectively protected against cyber threats and ICT risks. The DORA Regulation will apply to a broader range of financial institutions than previous regulations, including traditional financial sector players, banks, insurance companies, investment firms, payment service providers, fintech companies and cryptoasset providers. It also covers third-party ICT service providers that provide services to these financial institutions (such as cloud platforms or data analytics services).

Unlike previous regulations, which focused on specific aspects of ICT risk or particular types of financial institutions, DORA covers all aspects of digital operational resilience. It applies to a broader range of organisations involved in financial services.

The primary objective of the DORA Regulation is to increase the financial sector's operational resilience to ICT-related disruptions and threats. This includes measures to prevent, mitigate, respond to and recover from such disruptions. Examples include ICT risk management, rigorous and mandatory incident reporting to competent authorities, digital operational resilience testing through vulnerability and penetration testing, scenario-based testing to simulate different operational disruptions, third-party risk management, and managerial accountability. The DORA regulation requires regular threat-led penetration testing (TLPT), a framework that mimics the tactics, methods and procedures of real threat actors considered to be the source of an actual cyber threat and that performs controlled, tailored, intelligence-led testing of a financial institution's critical edge systems. Financial institutions must conduct TLPT at least every three years. However, more frequent testing may be required depending on the institution's risk assessment and the nature of the threats. Suppose there are significant changes within the organisation, such as major IT infrastructure changes, mergers or major cyber security incidents. In that case, additional TLPT may be required to ensure no new vulnerabilities are introduced. Institutions are encouraged to use their experience from the TLPT to improve their cyber security posture continuously, address vulnerabilities promptly and reassess their defences as new threats emerge.

By bringing together different requirements in a single piece of legislation, the DORA regulation will ensure consistency and coherence in the financial sector, which needed to be more cohesive under previous laws. It gives supervisory authorities stronger powers to monitor compliance, conduct audits and impose sanctions in case of non-compliance.

The Regulation establishes a regulatory framework for digital resilience, requiring all businesses to ensure that they can withstand, respond to and recover from all types of ICT-related disruptions and threats. These requirements are common to all EU Member States. The main objective is to prevent and mitigate cyber threats. The regulation is a significant step towards strengthening the financial sector's protection against digital threats and ensuring confidence and continuity in the financial system in the face of growing cyber risks (Horváth, 2022).

In addition, as part of the EU legislative package, Directive (EU) 2022/2555 on measures to ensure a high uniform level of cybersecurity across the EU (NIS2 Directive) aims to increase the cyber resilience and incident response capacity of public and private actors operating and providing services in critical sectors. This will reduce the risks of cyber threats, attacks and cybercrime and minimise the economic and social damage caused by disruptions and attacks. The NIS2 Directive is an improved version of the previous NIS Directive (EU) 2016/1148, as since it entered into force, significant progress has been made in increasing the EU's cyber resilience, and new challenges have been faced. The new rules will ensure a uniform level of cybersecurity across the EU, responding to the evolving threat landscape and considering the digital transformation accelerated by the COVID-19 crisis. In light of this crisis, for example, a specific amendment to the Cybersecurity Directive was to extend its scope to more specific elements of the healthcare sector, such as organisations carrying out research and development activities related to pharmaceuticals.

The amended Directive aims to harmonise the cybersecurity requirements and implement cybersecurity measures in different Member States. To this end, it sets minimum standards for the regulatory framework and establishes mechanisms for effective cooperation between the competent authorities in each Member State. It updates the list of sectors and activities subject to cybersecurity obligations and provides for remedies and sanctions to ensure implementation. In Hungary, compliance with the requirements of the NIS2 Directive is regulated by Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision, but this regulation will be replaced by Act LXIX of 2024 on the cybersecurity of Hungary from 2025.

The NIS2 Directive broadens the scope and covers more sectors and types of organisations than its predecessor. Critical sectors include energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, digital infrastructure, public administration and space. The legislation also covers organisations operating in high-risk sectors such as postal and courier services, waste management and, manufacturing certain critical products, etc. The Directive sets out more stringent security requirements for companies and organisations. The NIS2 Directive requires organisations to implement more comprehensive risk management measures, which include specific provisions on supply chain security, incident response and business continuity. Organisations need to assess and manage the risks associated with their supply chain, including third- and fourth-party suppliers. This approach recognises the interconnected nature of modern digital ecosystems and aims to mitigate the risks arising from supply chain vulnerabilities. The new legislation introduces stricter and more detailed reporting requirements for significant incidents. Organisations must report incidents within 24 hours of detection, provide initial information, and then produce a detailed report within 72 hours. The NIS2 Directive applies to medium and large companies, i.e. those with at least 50 employees or at least €10 million in annual turnover, and the size rules do not apply to providers of electronic communications, trust, DNS, top-level domain name registry or domain name registration services (Koolen et al., 2024; Boeken, 2024).

In addition, the Council of the EU adopted Directive (EU) 2022/2557 on enhancing the resilience of Critical Organizations (CER Directive). EU Member States are required to identify, following a risk assessment, critical organisations that provide services that are essential for the maintenance of vital functions for society, economic activities, public health and safety or the environment, and cases where an event would have a significant disruptive impact on these essential services, including where national systems ensuring the rule of law would be affected. This covers organisations operating in various sectors, such as energy, banking, financial market infrastructures (but some parts of it do not apply to these), health, water and sanitation, digital infrastructure, central government-level public administrations, spacecraft operations and food. These rules will apply from 18 October 2024. Entities identified as critical entities under the CER Directive are also subject to the cybersecurity obligations of the NIS2 Directive.

In a further regulatory step, the European Commission published proposals for a third Payment Services Directive (PSD3 Directive) and a new Payment Services Regulation (PSR Regulation) on 28 June 2023, completing the Commission's review of the second Payment Services Directive (PSD2 Directive). The review of PSD2 started in 2022, involving regulators, market participants and external experts. The evaluation has shown that the interpretation of the PSD2 Directive is not uniform and that differences in interpretation and application of the Directive by Member States create difficulties. Therefore, several amendments for payment services are proposed to be laid down in a directly applicable regulation. The rules on market access, authorisation and supervision of payment service providers and institutions will continue to be laid down in a Directive.

Building on its predecessor, the PSD2 Directive, which, among other things, made it mandatory to introduce strong customer authentication for online and credit card transactions, the PSD3 Directive introduces several key changes and improvements to enhance security, promote competition and strengthen consumer rights in the rapidly evolving digital payments environment. It would extend the scope of strong customer authentication and require it for more types of transactions, including mobile wallet enrolment. It introduces enhanced measures to prevent fraud, such as requiring banks to check that account names match the IBAN account number provided and to monitor transactions more closely. Furthermore, in case of failure to check IBAN/name and, victims of spoofing fraud (where the fraudster impersonates the customer as an employee of the bank) will be able to claim compensation from their payment service provider. The PSD3 Directive simplifies data-sharing processes and ensures that consumers have control over who has access to their financial information. This reduces the risk of data breaches and unauthorised access.

III. Summary

Cybercrime has become increasingly sophisticated and complex in recent years. One of the most striking trends is the increasing number of ransomware attacks. Critical infrastructure sectors, such as healthcare and finance, are particularly vulnerable and have suffered significant disruption. Supply chain attacks have also become more common, highlighting the targeting of third-party suppliers to penetrate larger organisations. Highly publicised incidents such as the SolarWinds attack have highlighted the vulnerability of supply chains and encouraged companies to increase their security measures.

Phishing and social engineering attacks have also become increasingly sophisticated, with attackers crafting personalised and persuasive messages to lure users into revealing sensitive information. BEC scams have led to significant financial losses. The emergence of AI in cybercrime has further increased the threat. Cybercriminals are increasingly exploiting AI and machine learning to automate attacks, making them more efficient and more challenging to detect. Phishing attacks using AI-personalised messages have also become more successful. In the case of cryptocurrencies, cybercriminals take advantage of the popularity of decentralised financial platforms.

In response to the growing threats, the EU has introduced more robust cybersecurity legal frameworks, such as the DORA Regulation, the NIS2 Directive and the CER Directive, and has proposed a package of legislation on payment services that is still to be adopted.

The DORA Regulation represents a significant step forward from previous regulations, as it provides a more comprehensive, consistent and integrated approach to ensuring the digital resilience of the financial sector. Its broader scope, detailed requirements and emphasis on governance, third-party risk management, incident reporting, resilience testing and information sharing differentiate it from the previous regulatory framework. It addresses the complexity of modern ICT risks more robustly.

The NIS2 Directive is a comprehensive update of EU cybersecurity legislation that addresses the limitations of the original NIS Directive and adapts to the increased digitalisation and complexity of today's cyber threats. By broadening the scope, imposing stricter requirements, increasing incident reporting, introducing personal liability, focusing on supply chain security and strengthening sanctions, the Directive aims to significantly improve the EU's cybersecurity resilience. Organisations within the EU must be prepared to comply with these new regulations to avoid significant penalties and ensure protection against cyber threats. Supporting the NIS2 Directive, the CER Directive will further strengthen the cyber resilience of services essential to society and the economy.

The PSD3 Directive and PSR Regulation are a step forward in the fight against cybercrime, with comprehensive measures to enhance security, reduce fraud and protect consumers in the rapidly evolving digital payments environment. Furthermore, the trend towards stricter regulatory measures is complemented by increased international and domestic cooperation and information exchange between law enforcement agencies and organisations responsible for cybersecurity.

References

ALKHALIL, Z., HEWAGE, C., NAWAF, L., KHAN, I. (2021). Phishing Attacks: A Recent

BOEKEN, J. (2024). From compliance to security, responsibility beyond law. Computer Law & Security Review, 52. 1–5.

BULLETPROOF (2022). Annual Cyber Security Industry Report 2022. Bulletproof.co.uk.

CHIKÁN, A., GELEI, A. (2005). Supply chains and their management. Harvard Business Manager, 35–44.

Comprehensive Study and a New Anatomy. Frontiers in Computer Science, 3. 1–23. AMBRUS, I. (2022). Digitalisation and Criminal Law, Wolters Kluwer [in Hungarian].

CUSTERS, B., OERLEMANS, J.-J., POOL R. (2020). Laundering the profits of ransomware: Money laundering methods for vouchers and cryptocurrencies. European Journal of Crime, Criminal Law and Criminal Justice, 121–152.

ERZBERGER, A. (2023). WormGPT and FraudGPT - The Rise of Malicious LLMs, https://shorturl.at/LBerg

EUROPOL (2022a). Takedown of SMS-based FluBot spyware infecting Android phones. https://t.ly/lv09z

EUROPOL (2022b). Facing reality? Law enforcement and the challenge of deepfakes. Europol Innovation Lab observatory report. https://t.ly/cos33

EUROPOL (2022c). Takedown of SMS-based FluBot spyware infecting Android phones. https://t.ly/o8fbR

EUROPOL (2023a). Cyber-attacks: the Apex of Crime-as-a-Service. https://t.ly/KdJOX

EUROPOL (2023c): Online Fraud Schemes: A Web of Deceit. https://t.ly/JjFL4

EUROPOL (2024a): Law enforcement to disrupt world's biggest ransomware operation. https://rb.gy/w73d4m

Europol (2024b): Internet Organised Crime Threat Assessment (IOCTA).

EUROPOL (2021). Internet Organised Crime Threat Assessment (IOCTA). https://bitly.cx/7GsCf

EUROPOL (2023b). Internet Organised Crime Threat Assessment (IOCTA). https://rb.gy/r8a7pd

EUROSTAT (2023): 22% of EU enterprises had ICT security incidents, 14 February 2023.

EUROSTAT: ICT security measures taken by vast majority of enterprises in the EU, 13 January 2020.

GYARAKI, Réka: The role of security awareness, or questions about cybersecurity. Magyar Rendészet, 2022/2. (in Hungarian)

HORVÁTH, K. (2022). DORA Regulation - new EU cybersecurity regulation for the financial sector". fintechzone. https://shorturl.at/qSYe9 [in Hungarian].

IACONO, L., HICKMAN, J., MUNIZ, C. (2022). The rise of vishing and smishing attacks. The Monitor, 21. https://shorturl.at/pZEAo

IBM SECURITY (2022). Cost of a Data Breach Report 2022. https://shorturl.at/5028m

KOOLEN, C., WUYTS, K., JOOSEN, W., VALSKE, P. (2024). From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models. Computer Law & Security Review, 52.

LEE, G. (2024). Enhanced OSINT with DarkGPT, an AI tool to detect leaked databases.

ME, G. (2023). OSINT in the Intelligence era. Edizioni Themis.

MEZEI, K. (2020). Current challenges of cybercrime in criminal law. L'Harmattan - TK JTI (in Hungarian).

NAGY, T. (2018). Business E-mail Compromise, or the attacks related to credit transfers. Belügyi Szemle (in Hungarian).

OLADIMEJI, S., KERNER, S. M. (2023). SolarWinds hack explained: Everything you need to know. TechTager. https://shorturl.at/jD6Un.

PINGEN, A. (2023). New Rules for Crypto-Assets in the EU. eucrim, 2/2023.

Security Daily Review. https://shorturl.at/EI2KO.

SECURITY STAFF (2022). Email cyberattacks increased 48% in first half of 2022. Security Magazine.

VANDEZANDE, N. (2024). Cybersecurity in the EU: How the NIS2 directive stacks up against its predecessor. Computer Law & Security Law Review, 52.

WAHL, T. (2021). AML Package IV: EU Traceability of Funds Legislation to Be Extended to Crypto-Assets. eucrim, 3/2021.

© Mezei Kitti – Nagy Tamás

MTA Law Working Papers

Kiadó: Társadalomtudományi Kutatóközpont (MTA Kiválósági Kutatóhely

Székhely: 1097 Budapest, Tóth Kálmán utca 4.

Felelős kiadó: Boda Zsolt főigazgató

Felelős szerkesztő: Kecskés Gábor

Szerkesztőség: Hoffmann Tamás, Lux Ágnes, Mezei Kitti

Honlap: http://jog.tk.mta.hu/mtalwp

E-mail: mta.law-wp@tk.mta.hu

ISSN 2064-4515