Cybersecurity and Cybercrime in Hungary During the COVID-19 Pandemic

KITTI MEZEI & CSABA KRASZNAY

Abstract In March 2020, the whole world was hit by home office in one fell swoop, without the right IT tools and knowledge to work remotely. Deploying remote access and cloud-based services was nowhere near as easy, neither from a technical nor human point of view.The first warning sign that the digital switchover due to COVID-19 could have cybersecurity implications is perhaps best followed through the Spring 2020 calvary of the Zoom application. In 2021, Hungarian users could also find out about the security of endpoints from direct events that caused a lot of press coverage. The safe operation of education systems is a major administrative and technical challenge for the operators of individual institutions. In addition to mass phishing attacks, targeted spear-phishing attacks have also occurred, particularly taking advantage of the uncertainty caused by the coronavirus epidemic and the large number of people working from home. The first and most crucial issue is the emergence of certain applications of artificial intelligence in cybercrime. The second important question is how the perpetrators have suddenly improved their operational planning and operational security for committing cybercrime. The third concern relates to cooperation between states.

Keywords: • COVID-19 • cybersecurity • cybercrime • deepfake • fake news • online fraud • phishing malware • distance learning

CORRESPONDENCE ADDRESS: Kitti Mezei, Ph.D., Research Fellow, Centre for Social Sciences, Institute for Legal Studies, 1097 Budapest, Tóth Kálmán u. 2-4, Hungary; Assistant Professor, Budapest University of Technology and Economics, Faculty of Economic and Social Sciences, Department of Business Law, 1117 Budapest, Magyar Tudósok körútja 2, Hungary; Postdoctoral Researcher, University of Public Services, Institute of Cybersecurity, 1083 Budapest, Ludovika tér 1, Hungary, e-mail: mezei.kitti@tk.hu. Csaba Krasznay, Ph.D., Director, Associate Professor, University of Public Services, Institute of Cybersecurity, 1083 Budapest, Ludovika tér 1, Hungary, e-mail: krasznay.csaba@uni-nke.hu.

https://doi.org/10.4335/2022.2.15 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

1 COVID-19 pandemic and cybersecurity

According to a meme often shared by IT professionals recently, the main source of digital transformation for companies was neither the CEO nor the IT manager but COVID-19 (High 2021). It would be difficult to argue with the reality of this, as the relevant data proves it. For example, according to WeAreSocial's summary, between January 2020 and January 2021, the number of Internet users increased by 7.3%, equals 316 million people, the number of social media users by 13.2%, equals 490 million people. Meanwhile, the world's total population grew by only 1%, equal to 81 million people (Kemp, 2021). The relevant figures esteeming Hungary's digital transformation in the European Union's Digital Economy and Society Index (DESI) 2021 show similar results, such as the stagnant 64% to 70% of eGovernment users and the number of corporate users of cloud services rose from 11% to 17%, which is still well below the European average (European Commission, 2021a).

So, there is no question that our subjective feeling that IT surrounds us is completely correct. Whether it is our work, learning, or communication, digital tools and services are unavoidable. And what is unavoidable, if it is not used properly or used inappropriately or with malicious intentions, it can lead to serious social problems.

This is faithfully reflected in the trends related to cybercrime, which clearly show that organised crime groups have adapted to the digital transition of potential victims and have developed crime patterns that can maximise their benefits in acts against individuals and organisations that have just latched on online services. These trends are perfectly highlighted in Europol's annual Internet Organized Crime Threat Assessment (IOCTA) 2021 report, which makes it easy to point to global and domestic challenges.

2 The home office posed cybersecurity challenges

In March 2020, the whole world was hit by home office in one fell swoop, without the right IT tools and knowledge to work remotely. No wonder there has been a drastic increase in the demand for web conferencing applications through which meetings could be conducted and after which everyone learned the name Zoom or Microsoft Teams. After that, creating secure access to enterprise resources soon became a serious need, leading to increased use of cloud services and the use of virtual private networks (VPNs) on a daily basis. In this connection, the information security specialists of the companies have gained short-term experience that the user endpoints (smartphones, tablets, laptops) very often do not even meet the basic security requirements. Then, as a final blow, it also had to be realised that there is no telecommuting without IT infrastructure that is resilient to cyber threats (Europol, 2021).

The first warning sign that the digital switchover due to COVID-19 could have cybersecurity implications is perhaps best followed through the Spring 2020 calvary of

the Zoom application. The first security problems of the solution, which suddenly became very popular, were highlighted by researchers in mid-March, followed by more and more news almost daily. Without wishing to be exhaustive, the following announcements followed one another:

- **March 30**
  The world is getting to know the phenomenon of zoombombing when unauthorised people enter video conferencing due to a software authentication error.
  It also turns out that Zoom is sending user data to Facebook.
- **April 1**
  Researchers point out that Zoom uses inappropriate end-to-end encryption.
- **April 2**
  It turns out that by exploiting a software error, passwords stored in Windows used to make calls could be stolen.
  Unauthorised access to other users' cloud-stored Zoom data is achieved.
- **April 3**
  Zoom-related phishing pages appear in bulk.
  Analyses show that the company is using an inappropriate encryption algorithm.
  Due to increased user demands, the company is starting to use new cloud servers located in China, which means several calls important to national security are going through this country.
- **April 6**
  Illegally recorded Zoom conversations are appearing on YouTube.
- **April 7**
  Zoom gets banned by several government agencies.

After that, Zoom spent a total of 3 months improving the security of its service, setting an example for its competitors. Since then, there have been no major security concerns about online conferencing services. We can even attribute a number of exemplary privacy measures to them, such as blurring the room image in the camera and replacing it with a virtual background.

Deploying remote access and cloud-based services was nowhere near as easy, neither from a technical nor human point of view. According to the perspective of information security, this meant that the company had to be „opened up" to the world, to the Internet. There was a serious fear that the range of people accessing corporate information and the path of the information that escaped would become uncontrollable. While technical best practices are, of course, given to implement secure remote access, unfortunately, cybercriminals have begun to exploit the flaws of these solutions. For example, as mentioned in the IOCTA 2021 report, gangs that spread ransomware actively exploit vulnerabilities in VPN solutions and Microsoft Remote Desktop Protocol (RDP) to distribute malicious code. It should also be mentioned that according to HaveIBeenPwnd.com's records, there are more than 11.6 billion leaked, traceable user

accounts and passwords on the Internet, while hundreds of millions more access are being traded on the darknet.

In 2021, Hungarian users could also find out about the security of endpoints from direct events that caused a lot of press coverage. One such attack, which affected almost everyone, could be linked to malicious code called FluBot. During the infection, the victim first received an SMS that his or her package was arriving, but he or she would need to download an app to track it. After installation, the application had access to the data stored on the victim's phone, including the phone numbers. It collected the contacts and automatically transmitted the phishing SMS to them. For the infection, the victim had to actively click on the attached links and permission requests, so in general, the biggest threat lurking at the endpoints is the user itself, which raises the question of how much risk companies take regarding their complete security when allowing remote access to individually owned devices (National Cyber Security Center, 2021). Another such event is the revelation of Pegasus spyware developed by the NSO Group. Although this has only been used in a targeted manner against properly selected individuals, the case points out that an endpoint device and the data stored on it can be accessed remotely without the victim having to click on anything (Marczak, 2021).

The availability of infrastructures and, incidentally, organisational data assets are being tested by extortion-type attacks, in particular, ransomware and Distributed Denial of Service (DDoS) attacks with extortionist aim. Although these types of attacks are not new, their numbers have increased significantly during COVID-19. The modus operandi has changed, making it virtually impossible for most organisations to defend against them. An example of both cases occurred in Hungary. In April 2021, the most prominent car parts retailer, Unix Auto, fell victim to ransomware, and in November 2021, MediaMarkt's online sales became impossible due to similar reasons. In the first case, the infrastructure was Hungarian; in the second case, the international centre became the target, which also affected the Hungarian operation. Most Hungarian media service providers got to know about the DDoS attacks in the autumn of 2021, when their websites became inaccessible for hours.

3 Distance learning and cybersecurity

In March 2020, Hungarian public education was switched to absence digital education in one day. Tertiary education had two weeks. According to the data of the Hungarian Central Statistical Office in 2019, this meant 1.8 million users in Hungary, most of whom have never experienced learning via the Internet before (Hungarian Central Statistical Office, 2019). Of course, no actor in education was prepared for this rapid shift, as although many good practices were widespread and excellent foreign examples were available, their profound adaptation was not encouraged by legislation or the National Core Curriculum. Legally, nor the IT infrastructure was ready to accommodate this nearly two million people, and the state-developed e-Kréta system got able to serve the digital

needs of public education only roughly a year after the outbreak of the pandemic (Hoffman, 2021: 150), meanwhile taking classes via the Internet continued using foreigner services (Microsoft Teams, Google Meet, Zoom).

The review of 1488/2016. (IX. 2.) Government Decree on the Establishment of a Secure Internet Service for Children, on Conscious and Value-Creating Internet Use and on Hungary's Digital Child Protection Strategy shows the unpreparedness of the Hungarian education system to distance learning, which is safe and considers data protection. The detailed strategy issued on the basis of the government decree shows exactly what affairs the legislator planned to solve by 2020. It contains a number of important issues, which, although, could have contributed to overcoming some of the sub-problems, however, the document does not specifically address the concepts of distance and absence learning or the digital agenda. There is no trace of increasing the security of computer use at home or even improving the privacy and information security skills of educators in the toolkit. There is only one measure in the text, the implementation of which might have been useful at the time of the declaration of the state of danger: „Preparation and dissemination of information on child protection rules according to the Act CVIII of 2001 on Electronic Commerce and on Information Society Services and consumer protection law enforcement in relation to online commerce, furthermore up-to-date information on online child protection legislation, defensive options and media literacy programs on the website of each public education institution theorem" (Hungary's Digital Child Protection Strategy, 2016).

It is a feature of the digital work schedule that students, teachers, educators typically communicate with each other through their own device on a platform managed by an external service provider, sharing data and information that are considered personal. It can be seen that there are serious concerns about a situation where a minor child joins an online classroom via video, while his or her living space is visible in the background, all on a platform that the teacher has registered for free, thus approving the terms and conditions that the service provider is clearly designed to make the most of the data passing through the platform. From a privacy perspective, it is also a questionable practice for a teacher to request a video from a child to prove that he or she has completed a physical education class, who shares this with their teacher through a cloud provider. By storing the video, data processing takes place in an environment where data protection regulations are not clear. Since most educators decided to pass the curriculum at their own discretion during the first period of absence education, there were some particularly bad practices, such as requiring a child under the age of 13 to register on Facebook with a teacher's expectation. Not only did the parents' previous educational goals have to be violated, but also the social network's own rules of use.

The safe operation of education systems is a major administrative and technical challenge for the operators of individual institutions. Many elementary and high schools do not have a document regulating IT security, as a result of which the processes for operating an IT

system are not defined. Instructors who operate school IT systems often only on a part-time or class reductive basis are required to ensure that the infrastructure is operational and to assist the school administration involved. The optimal solution in this situation is to outsource the operation of IT specialist systems, thus using a centralised service where the operational tasks are performed by qualified professionals. In case of systems where external service is not available, they try to provide a solution by building their own system, the long-term safe operation of which can be risky for them.

In tertiary education, in most cases, there is a company-level IT background available to support teaching and research work, which is operated either by a central organisational unit or by independent IT staff in each organisational unit. The vast majority of tertiary educational institutions have IT security regulations, and although they are not subject to uniform content regulations, most of them show the spirit of Act L of 2013 on electronic information security. When purchasing systems, the supplier also provides some training so that operators know and are able to operate them to some extent. Many institutions have contracts that provide professional support beyond the general operational tasks.

In light of all this, it is not surprising that the number of cybercrimes has risen significantly as children have been at home and used more digital devices than before, and educational institutions have been forced to maintain educational infrastructure without adequate resources (Coman and Mihai, 2021: 4). The IOCTA 2021 report, for instance, identifies the education sector as one of the main targets of ransomware attacks. Unfortunately, however, the drastic increase in sexual abuse of children highlights the particular problems of using the Internet for students' entire lives. Europol warns that online grooming has grown sharply on children's favourite social networks and gaming platforms, while the spread of children's own images is also a matter of serious concern. Both adults and children are at risk of online sexual extortion (sextortion), but the latter is particularly. In this case, the perpetrator wheedles him- or herself into the trust of the child (e.g., pretends to be a juvenile and befriends the child, shows him or her sexually explicit material to reduce his or her sexuality-related inhibitions), and exploits his or her vulnerability (Powell and Nicola, 2017: 122-124). The perpetrator does this in order to access sexually explicit images or videos of the child, which is eventually followed by a blackmail phase, when he or she is forcing, extorts his victim to do a sexual favour for him or her or to send additional compromising images or videos of him- or herself. If the victim does not comply with the request, the extortionist threatens to share the recording he or she already has (for example, through social media) and puts the victim under his or her control (Europol, 2014: 30). Without complete social isolation due to COVID-19, these two trends would presumably be less significant.

4 The COVID-19 pandemic and cybercrime

The COVID-19 virus crisis has been exploited in the online sphere and has become a major "bait" for offenders. The emergence of a crisis always brings new circumstances that provide an ideal environment for cybercriminals. For example, when Italian citizens could apply for coronavirus benefits, some hackers attacked Italy's social security website, causing a one-day shutdown.

During a pandemic, there is an alarming increase in the number of cyber-attacks against healthcare organisations. These threats have affected hospitals (for example, in the Czech Republic, a healthcare facility carrying out testing was paralysed by a ransomware virus), the World Health Organisation (WHO), whose servers have been hacked, and even companies at the forefront of vaccine development, as well as the European Medicines Agency (Palicz, Bencsik and Szócska, 2021: 84-85.). The healthcare sector lags far behind in cybersecurity, with a lack of digital skills among staff, outdated software and inadequate regulation and enforcement (Chigada, Madzinga, 2021).

In addition, perpetrators often target mobile devices, for example, to develop – or manipulate –apps that appear to track the spread of the coronavirus. In reality, the application infects the device with malware and collects personal data, credit card information, etc. (Collier et al., 2020: 5).

5 Phishing and malware

In parallel with the emergence of the coronavirus epidemic, phishing has also been on the rise. COVID Internet domain registrations have recently increased significantly, in many cases created for phishing. The fake websites appear to be real sites of real organisations but are used to distribute malware. Several COVID-19 phishing campaigns have been identified, attempting to exploit people's fear of the virus and trick them into opening malicious attachments, even on behalf of local or international health organisations (the WHO or the National Surgeon General). For example, COVID-19 phishing packages (e.g. infected programs disguised as a map showing the spread of the virus) are already available on the darknet. The subjects of these phishing emails include analyses of specific industries and official advice from health authorities on the coronavirus epidemic, as well as counterfeit products. The email attachments include ransomware, remote access Trojans and keystroke recorders installed on unwary users' computers and mobile phones (Guirakhoo, 2020).

As the number of infected people has increased, scams have emerged in which people are contacted on behalf of local hospitals claiming to have been infected. In other cases, attempts are being made to deceive people by using the digital COVID certificate issued by the European Union. The perpetrators also use malicious content hidden in the attachment in these cases.

The weakest link in cybersecurity is the human being. In most cases, the victim is behind every successful attack, so perpetrators often prefer social engineering attacks such as phishing to technical solutions.

According to Google, in March 2020, fraudsters sent 18 million phishing emails per day to Gmail users on COVID-19. In April, the tech company blocked more than 100 million phishing emails per day, nearly a fifth of which were related to the COVID-19 virus scam (Tidy, 2020). Emerging technologies such as artificial intelligence can make cyber-attacks more effective. Perpetrators can use it to develop malware, increase the effectiveness of ransomware or more targeted social engineering attacks, and circumvent image recognition and voice recognition, among other things. Europol is already calling for so-called "AI-as-a-service", or AI as a service, which could already be used for malicious purposes. (Cerulus, 2021 and see more Caldwell et al., 2020: 1–14).

Malicious programs and hacker attacks may constitute a criminal offence according to the Hungarian Act C of 2012 on the Criminal Code (hereinafter referred as to Criminal Code). The Hungarian Criminal Code in Section 423 contains the offence of breach of information system or data, which covers conducts criminalised under international and EU legislation (Budapest Convention on Cybercrime and Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems). According to Subsection (1), any person who gains unauthorised entry to an information system by compromising or defrauding the integrity of the technical means designed to protect the information system or overrides or infringes his or her user privileges is guilty of a misdemeanour punishable by imprisonment not exceeding two years. If it is committed intentionally by unauthorised access, for example, by a person who does not have access to the system (so-called hacking) or by exceeding or violating the limits of his/her access rights by remaining inside (for example, by using the password of another colleague who has access to the system in his/her capacity as an employee). Notably, the offence must be committed by breaching or circumventing a technical measure that provides protection (this means that the information system must have active protection, such as a password or other means of protection, for the offence to be established). The offence does not constitute a purpose, and therefore it is not a condition of the crime that it is committed for gain, damage or similar purposes. Nor is it a requirement that the offender subsequently performs any operation on the data stored in the information system or even interfere with the system's functioning. Therefore, unauthorised access is a criminal offence in itself (mere hacking). If this is followed by further unauthorised operations, such as deleting data or making it inaccessible, one of the following paragraphs is already triggered and merges into the more serious paragraphs of breach of information system or data. It is possible to cause damage to information systems in various ways. For example, someone who gains unauthorised access to the system could send a command to delete files necessary for the operation or a system shutdown. These cases are governed by Section 423 Subsection (2) point a) of the

Criminal Code, which provides that anyone who disrupts the use of the information system unlawfully or by way of breaching his or her user privileges is guilty of a felony punishable by imprisonment not exceeding three years.

Unauthorised interference with the operation of an information system or interference in breach of the limits of its lawfulness is also punishable under this offence. For example, it is not necessary for the offender to have access to the information system in question, as it is sufficient to interfere with its proper functioning in any way, regardless of the duration and extent of the interference, such as launching a DDoS attack, which results in the website of a bank or other service provider being rendered inaccessible.

According to Subsection (2) point b), anyone who alters or deletes, or renders inaccessible without permission, or by way of breaching his user privileges, data in the information system is guilty of a felony punishable by imprisonment not exceeding three years.

In addition, various manipulations of data in the information system are also prohibited: if data in the information system is altered, deleted or made inaccessible without authorisation or in violation of its authorisation (for example, as in the cases mentioned above, by infecting the system with malware, such as the trend in recent years to use ransomware, (Wall, 2021) or by further manipulation of data following unauthorised access).

An aggravated offence may be established and punishable for imprisonment between one to five years for a felony if the acts defined in Subsection (2) involve a substantial number of information systems, but the law does not define what constitutes a significant number, so it is for judges to develop a practice in this regard. An excellent example of an aggravated case is DDoS attacks. The attacker attempts to connect to the attacked computer by using hundreds or thousands of users' information systems controlled remotely by the attacker. Many data requests and transmissions are sent at once paralyses the attacked information system, which may exhaust the notion of a significant number of information systems.

In the other aggravated case, the penalty shall be imprisonment between two to eight years if the criminal offence is committed against works of public concern. Among the interpretative provisions, the Criminal Code defines in Section 459, point 21, by way of example, what constitutes as works of public concern: utilities, public transport establishments, electronic communications networks, logistics, financial and IT hubs and operations necessary for the performance of the tasks of universal postal service providers carried out in the public interest (e.g. financial institutions) and plants producing war materials, military items, energy or basic materials destined for industrial use. The problem with this is that the notions of critical infrastructure and works of public concern as used in the EU law (Directive 2013/40/EU on attacks against information systems) do not overlap, so the qualification of the offence can be controversial, especially in the case

of cyber-attacks on institutions of social welfare, public health. This is also important to draw attention to because, since 2017, Hungary has also introduced an electronic health system. All personal data and institutional care documents are stored electronically, thus increasing the risk of possible cyber-attacks.

In the case of spyware, the offence of illicit access to data [Section 422 (1) (e) and (d) of the Criminal Code] may arise if the data or the content of communications handled in the information system are secretly intercepted to obtain unauthorised knowledge of personal data, private secrets, trade secrets or business secrets, and the intercepted data are recorded by technical means.

In the context of the collection of bank card data and personal data, fraud (Section 375 of the Criminal Code) and misuse of personal data (Section 219 of the Criminal Code) are typically committed using the information system. According to Section 219 Subsection (1), a person who, by violating a provision laid down in an Act or a binding legal act of the European Union on the protection or processing of personal data and for gain or causing significant harm to interests, a) processes personal data in an unauthorised manner or in deviation from the purpose of processing is guilty of a misdemeanour and shall be punished by imprisonment for up to one year.

In cases when unknown persons create a fake profile on the social media site using the user's name and photos are considered criminal cases. Through this pseudo-profile, the perpetrator identifies the real friends of the impersonated user and sends messages and posts messages on behalf of the user. The aim is often to discredit the person concerned, tarnishing their reputation in the eyes of others, and this can result in significant damage to their interests. It is also possible that the personal data of others is used to commit crimes, for example, to defraud unsuspecting users of money or credit card details through a fake profile on social and online dating sites (romantic fraud) or e-commerce platforms.

6 Online fraud

In addition to mass phishing attacks, targeted spear-phishing attacks have also occurred, particularly taking advantage of the uncertainty caused by the coronavirus epidemic and the large number of people working from home. These emails are created in both content and form so that their unique features do not arouse suspicion. The attack is always preceded by a study of the intended targets (e.g. a preliminary assessment of their workplace, behaviour, and organisational structure). The perpetrators often pose as company executives or employees, business partners – business email compromise or CEO fraud – and send an email to the person responsible for the finances (e.g. a financial controller or accountant) asking them to carry out an urgent bank transaction. This step may be followed by further emails or even phone calls to confirm the need for the transaction by presenting themselves, for example, as a trusted business partner or lawyer. It is also common to hack into a company's mail system and gain access to valuable

information (e.g. who the targeted company has a supplier or other contractual relationships with, address lists, business correspondence, etc.) that may facilitate a targeted attack. As highlighted by the FBI's report, these attacks are highly costly, which estimates they caused 360 million dollars in 2016 and $675 million dollars in 2017 (U.S. Department of Justice, 2018, p. 36). These cases typically fall within the traditional offence of fraud. According to Section 373 of the Criminal Code, it is committed for illicit gain by defrauding a natural person and causing financial damage.

Taking advantage of the shortage of goods and the general fear, several online trading platforms have been set up to sell sought-after products such as sanitary masks, hand sanitisers and tests. However, customers never receive the products after paying the bill, and the fake online store operators disappear with the money. Such cases have also occurred in Hungary, where criminals have accessed the e-mail account of a person unknown to them without authorisation and then used the e-mail account by changing the password. They used the email account to register on an Internet portal and advertised respiratory protection masks, taking advantage of the epidemic situation. The perpetrators gave bank account numbers to the persons who had signed up for the advertisement, to which the victims transferred the money but did not send the ordered mouth masks because they did not have them. They applied for advertisements from different parts of the country (Prosecutor's Office of Hungary, 2021 and see more about online fraud cases: Wan Fei Ma, McKinnon, 2021; Murrar, 2021, and Buil-Gil, Zeng, 2021).

The person is liable for breach of information system or data (Section 423 of Criminal Code) because he did not have the right to use the e-mail account. He logged in and even changed the password by circumventing the technical measure. They are also liable for traditional fraud because they misled natural persons and caused them harm. In this case, the person does not cause damage through an operation using an information system and therefore cannot be held liable for fraud utilising an information system. For example, suppose you access your online banking account and make an unauthorised transfer or purchase using the obtained credit card details. In that case, you are committing fraud using the information system, as the central element of the offence is the information system and not the misrepresentation or fraud of the natural person.

In addition, a new series of frauds has emerged in Hungary that exploited the growing popularity of home delivery in the wake of the epidemic and restrictive measures. SMS messages were sent on behalf of courier services in response to the increase in online shopping. Unlike emails, SMS only shows a phone number, with no sender address to check (smishing). In all cases, the SMS requesting us to track your parcel contains a link that appears to take you to a known courier service when opened. Here, the unsuspecting user is asked to download and install an application to track their parcel, which is malware (such as the FluBot above) and collects data on the mobile phone, mainly bank IDs, cryptocurrency or credit card details.

In the UK, there have been cases of smishing that followed government announcements such as COVID-19 promising financial assistance and directing the public to a fake government website requesting bank card details. In another case, parents were targeted and promised help with free school meals but were also asked for bank details in return (Lalliea et al., 2021).

In parallel with the emergence of new security measures (e.g. strong identification systems, two-factor authentication, which banks are obliged to use), criminals are also trying to circumvent this through so-called SIM-swapping. Through social engineering or phishing, they obtain personal data and then block the old SIM card on behalf of the victim at the mobile phone service provider and request a new one to access various bank or other user accounts (Europol, 2020: 44–46).

Similar cases have been reported in Hungary. Victims were attracted by an advertisement for a house for sale at an excellent price in one such case. The advertiser informed them by telephone that the discounted price was because he needed money urgently because of family circumstances. He also indicated that the relative would soon show the apartment to other interested parties. Only one photo had been uploaded to the ad site but promised to send more pictures and a video by e-mail. The victims requested to receive the images through a service for sending large files, but the advertiser offered other free software for this purpose. The victims had no idea that the software could be misused on their computers. The software allowed the advertiser to establish a remote desktop connection between the computers. He then waited for the victims to log into their Internet bank account. This alone is not enough, because the only way to access the bank account is through two-factor identification, i.e. to enter and access the bank account after entering the code received in the SMS, in addition to the bank ID, and to do this, the perpetrator had to have control of their phone. The mobile phone provider said that an unknown person had initiated the exchange of SIM cards belonging to the victim couple's company subscription at one of their shops. The unknown person in charge claimed that they had been stolen and asked for the original cards to be blocked. The victims' phones then went silent. In addition, the unknown person presented a forged signature of the victims' company. The money in the victims' bank accounts was then accessed via the Internet banking service, and the nearly 85 000 euro was converted into bitcoin after repeated transfers (Horváth, 2020).

If the perpetrators obtain only the Internet banking login data and use them to cause damage using a transaction in the information system (e.g. by making a bank transfer), then the offence of fraudulent misuse of data by using the information system is committed under Section 375 Subsection (1), the offence of information system fraud. According to this Subsection, any person who, for unlawful financial gain, introduces data into an information system, or alters or deletes data processed therein, or renders data inaccessible, or otherwise interferes with the functioning of the information system, and thereby causes damage, is guilty of a felony punishable by imprisonment not exceeding

three years. The offence is an important complement to the traditional offence of fraud (Section 373 of the Criminal Code) because it covers fraudulent conduct that causes damage to property by direct use of the information system, and therefore does not involve the deception of a natural person, which is essential to establish fraud.

If they obtain credit card data without authorisation and use the information system to cause damage (e.g. purchasing 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 Subsection (5). This offence has no offence form - as is typical for other offences against property - and the basic cases cover damage ranging from one forint to five million forints. According to this Subsection, any person who causes damage by using a counterfeit or forged, or unlawfully obtained electronic payment instrument, or by accepting payment with such payment instrument shall be punishable.

Nemzeti Média- és Hírközlési Hatóság (National Media and Infocommunications Authority) (hereinafter referred as to NMHH) has been monitoring the practices of service providers with SIM card swapping in such cases. There have been cases of abuse that have caused considerable financial damage based on access to victims' bank confirmation SMSs. To keep our data and assets safe, a simple authorisation is no longer enough when it comes to changing our SIM cards. The NMHH has asked Telekom, Telenor and Vodafone to introduce new procedures after monitoring their practices. The telecoms authority and the operators expect tightened measures to reduce this type of abuse significantly. We can expect to see checks on the SIM card is replaced, delayed activation of the new card, requiring authentication in case of authorisation, but also sending verification codes and information SMS (NMHH, 2021 and see more about SMS-swapping: ENISA, 2021).

7 Deepfake and fake news

Finally, the rise of deepfake technology is worth mentioning, which is relatively new and poses an increasingly serious challenge to society. In the case of deepfake, an algorithm can replace the facial image in a video recording of a person with the facial image of another person, which can be deceptive to anyone. In addition to the harm caused to the individual (see revenge porn or content generated by artificial intelligence used for fraud), deepfake can contribute to disinformation (Whyte, 2020), distort democratic decision-making, and manipulate the electoral process, eroding public trust exacerbating divisions in society (Kirchengast, 2020). Protection against the coronavirus can also be hampered by fake news (e.g. content shared on social media, posts about the virus and vaccines). Therefore, new criminal conduct (Article 337 of the Criminal Code) has been added to the offence of fearmongering. According to Subsection (2), a person who, during the period of a special legal order and in front of a large audience, states or disseminates any untrue fact or any misrepresented true fact that is capable of hindering or preventing the efficiency of protection is guilty of a felony and shall be punished by imprisonment for

one to five years. The Hungarian Government introduced a state of emergency due to the coronavirus pandemic. There are increasing cases when people publish a piece of writings on the Internet that could impede the effectiveness of the protection against the coronavirus. These give rise to suspicion of the abovementioned criminal offence. Disinformation is still a major issue in the COVID-19 public debate. As a result, many have chosen not to believe in the scientific data, acknowledge COVID-related health risks and/or be vaccinated against the disease (European Commission, 2021b).

8 Summary

One of the key characteristics of cybercrime is its rapid adaptation. With the attacker infrastructure, know-how and billions of potential victims constantly available, it is a matter of finding the right theme to base an attack. The rapid digitalisation resulting from COVID-19 has created an unprecedented opportunity for criminal groups to use existing techniques to target a common theme. We saw familiar patterns in a coronavirus costume in the first pandemic period. But the phase from autumn 2020 onwards has brought frightening new developments, the rapid effects of which have already been felt through the evolution of ransomware or attacks on supply chains. But its long-term consequences are still to be seen.

The first and most crucial issue is the emergence of certain applications of artificial intelligence in cybercrime. The involvement of deepfake in online fraud is already a sign that AI is a technology available to anyone, but when will the most prominent groups start to exploit it to 'train' algorithms from stolen data? Remember, a criminal organisation is not hampered by data protection rules such as GDPR. They can get more accurate profiles and organisational information with the right knowledge than the best data analytics firms. And based on what they know about defensive solutions, they may develop attack algorithms that even the most sophisticated organisation is defenceless against.

The second important question is how the perpetrators have suddenly improved their operational planning and operational security for committing cybercrime. Although the link between intelligence agencies and criminal groups has existed since states have been conducting covert operations, and cyberspace operations are no exception, history teaches us that the most dangerous mix is when trained intelligence operatives turn to crime. This is evidenced by the Mexican drug war, where one of the most dangerous groups, Los Zetas, was founded by former secret service agents or the Islamic State terrorist organisation, in which former Iraqi intelligence agents were actively involved. Given that the high-profile cybercrimes of 2021 were committed in ways previously only used in state cyber operations, it is feared that intelligence knowledge has been transferred to these groups.

The third concern relates to cooperation between states. The ability to fight cybercrime is diminishing from North to South, the willingness from West to East, as a practising

investigator once put it. Unfortunately, this is borne out by the facts, as Russia and China did not participate in the October 2021 meeting held by President Biden to prevent the spread of ransomware. However, the answer to a question about Russia's absence suggested that the two governments had begun cooperating (The White House, 2021). Given the abundance of perceived state operations at the beginning of the COVID-19 period, it is questionable how genuine this willingness to cooperate is and how it can be sustained in emergency situations. Without cooperation, cyberspace peace cannot be achieved, and joint responses to the issues raised earlier cannot be provided.

Acknowledgment:

The research was supported by the Ministry of Innovation and Technology NRDI Office within the framework of the FK_21 Young Researcher Excellence Program (138965) and the Artificial Intelligence National Laboratory Program.

References:

Buil-Gil, D. & Zeng, Y. (2021) Meeting you was a fake: investigating the increase in romance fraud during COVID-19, *Journal of Financial Crime*, 29(2), pp. 460-475, https://doi.org/10.1108/JFC-02-2021-0042.

Caldwell, M., Andrews, J.T.A., Tanay, T. & Griffin, L.D. (2021) AI-enabled future crime, *Crime Science*, 9(14), https://doi.org/10.1186/s40163-020-00123-8.

Cerulus, L. (2021) One group that's embraced AI: Criminals, *Politico*, available at: https://www.politico.eu/article/artificial-intelligence-criminals/ (January 15, 2022).

Chigada, J. & Madzinga, R. (2021) Cyberattacks and threats during COVID-19: A systematic literature review, *South African Journal of Information Management*, 23(1), pp. 1-11, https://doi.org/10.4102/sajim.v23i1.1277.

Collier, B., Jones, R., Horgan, S. & Shepherd, L. (2020) The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations, *The Scottish Institute for Policing Research*, (1), pp. 1-18.

Coman, I. & Mihai, J.-C. (2021) The Impact of COVID-19 on Cybercrime and Cyberthreaths, *European Law Enforcement Research Bulletin*, SCE 5, pp. 61-67, available at: https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/489 (January 15, 2022).

ENISA (2021) *Countering SIM-Swapping: Overview and good practices to reduce the impact of SIM-Swapping Attacks* (Athens: ENISA).

European Commission (2021a) *Fighting disinformation*, available at: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation_en (January 15, 2022).

European Commission (2021b) *The Digital Economy and Society Index (DESI)* (11), available at: https://digital-strategy.ec.europa.eu/en/policies/desi (January 15, 2022).

Europol (2014) *Internet Organised Crime Threat Assesment (IOCTA)*, available at: https://www.europol.europa.eu/publications-events/main-reports/iocta-report (January 15, 2022).

Europol (2021) *Internet Organised Crime Threat Assesment (IOCTA)*, available at: https://www.europol.europa.eu/publications-events/main-reports/iocta-report (January 15, 2022).

High, P. (2020) Who Led Your Digital Transformation? Your CIO Or COVID-19?, *Forbes* (May 26, 2020), available at: https://www.forbes.com/sites/peterhigh/2020/05/26/who-led-your-digital-transformation-your-cio-or-covid-19/ (January 15, 2022).

Hoffman, I. (2021) Cybersecurity and public administration in the time of corona(virus) – in the light of the recent Hungarian challenges, *Cybersecurity and Law*, 3(1), pp. 145-158.

Horváth, Cs. L. (2021) A Hungarian family's bank account was zeroed out in a criminal fraud, *24.hu*, available at: https://bit.ly/3eRqr8H (January 15, 2022).

Hungarian Central Statistical Office (2019) Educational data, 2019/2020 (preliminary data), *Statisztikai Tükör*, available at: www.ksh.hu (January 15, 2022).

Kemp, S. (2021) Digital 2021: Global Overview Report, *DataReportal*, available at: https://datareportal.com/reports/digital-2021-global-overview-report (January 15, 2022).

Kirchengast, T. (2020) Deepfakes and image manipulation: criminalisation and control, *Information & Communications Technology Law*, 29(3), pp. 308-323, https://doi.org/10.1080/13600834.2020.1794615.

Lalliea, H. S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C. & Bellekens, X. (2021) Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, *Computers & Security*, 105, pp. 1-13, https://doi.org/10.1016/j.cose.2021.102248.

Marczak, B., Scott-Railton, J., Razzak, B.A., Al-Jizawi, N., Anstis, S., Berdan, K. & Deibert R. (2021) NSO Group iMessage Zero-Click Exploit Captured in the Wild, *The Citizen Lab*, available at: https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/ (January 15, 2022).

Murrar, F. (2021) Fraud schemes during COVID-19: a comparison from FATF countries, *Journal of Financial Crime*, 29(2), pp. 533-540, https://doi.org/10.1108/JFC-09-2021-0203.

National Cyber Security Center (2021) *Alert on sms messages related to the distribution of malicious code that misuse the name of parcel service providers*, available at: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-csomagkuldo-szolgaltatok-nevevel-visszaelo-malware-terjesztessel-osszefuggo-sms-uzenetekkel-kapcsolatban/ (January 15, 2022).

NMHH (2021) "*SIM card replacement made safer*", available at: https://nmhh.hu/cikk/223395/NMHH_biztonsagosabba_valt_a_SIMkartyak_csereje (January 15, 2022).

Palicz, T., Bencsik, B. & Szócska, M. (2021) Kiberbiztonság a koronavírus idején – a COVID-19 nemzetbiztonsági aspektusai [Cybersecurity in the age of the coronavirus - national security aspects of COVID-19], *Scientia et Securitas*, 2(1), pp. 84-85.

Prosecutor's Office of Hungary (2020) *The court arrested the fraudsters who sold masks* (April 3, 2020), available at: https://ugyeszseg.hu/a-birosag-letartoztatta-a-szajmaszkokkal-uzletelo-csalokat/ (January 15, 2022).

The White House (2021) *Background Press Call on the Virtual Counter-Ransomware Initiative Meeting*, available at: https://www.whitehouse.gov/briefing-room/press-briefings/2021/10/13/background-press-call-on-the-virtual-counter-ransomware-initiative-meeting/ (January 15, 2022).

Tidy, J. (2020) Google blocking 18m coronavirus scam emails every day, *BBC News*, available at: https://www.bbc.com/news/technology-52319093 (January 15, 2022).

U.S. Department of Justice (2018) *Report of the Attorney General's Cyber Digital Task Force* (Washington: DoJ).

Wall, D. (2021) The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending, *European Law Enforcement Research Bulletin*, SCE 5, Special Conference Edition Nr. 5, pp. 45-60.

Wan Fei Ma, K. & McKinnon, T. (2021) COVID-19 and cyber fraud: emerging threats during the pandemic, *Journal of Financial Crime*, 29(2), pp. 433-446, https://doi.org/10.1108/JFC-01-2021-0016.

Whyte, C. (2020) Deepfake news: AI-enabled disinformation as a multi-level public policy challenge, *Journal of Cyber Policy*, 5(2), pp. 199-217, https://doi.org/10.1080/23738871.2020.1797135.