Vlach, Jiří - Kudrlová, Kateřina - Paloušová, Viktorie
Kyberkriminalita v kriminologické perspektivě
Cybercrime from a Criminological Perspective
ISBN 978-80-7338-189-9

Summary

Today's society is virtually unimaginable without digital technologies. They permeate our everyday life as a simple matter of course: mobile phones, e-mails, social networks, online news and shopping, from smart homes to smart cities. Above all, they are being slowly, but surely joined by more and more connected devices, giving rise to the term "Internet of Things". The number of connected households has continued to grow, while the use of the internet has gradually penetrated all age groups.

Cyberspace thus means much more than mere virtual reality or a parallel world only accessible to the young or technically proficient. It's already become an integral part of everyday reality, though more its emanation than a separate part. Nevertheless, it has certain characteristics that significantly affect "movement" and communication within its framework compared to the real environment: in particular, constancy (someone is always online), limitlessness (the internet knows no boundaries) and the absence of physicality (nonverbal elements of communication). However, we must not overlook the specifics at social (especially social networks), technological (e.g. the specifics of cryptocurrencies), control (e.g. content regulation) and economic (including online trading or internet banking) level.

Nevertheless, the development of technology and cyberspace has progressed hand-in-hand with the advent of associated crime - cybercrime. This includes both "traditional crime in a new guise" and completely new forms of crime that are unthinkable without a virtual environment (typically malware). We can be content with its definition as crime using information and communication technologies, although a number of other, more expansive definitions can be found. On the other hand, there are various classifications, most often based on the Convention on Cybercrime or crime enabled or facilitated by the use of ICT, or typologies grouping certain offences (e.g. online sexual abuse, the black market, etc.). Although each has its advantages and disadvantages, following the findings of our analysis of criminal files (see below), we offer a different form of classification, namely virtual violence

(threats, denied access to social network accounts, defamation, etc.) and online financial crime (and others).

Whether we stick to data and reports published in the Czech Republic or look further around the world, a continuing upward trend in cybercrime is evident and its range is varied. It includes various criminal offences such as fraud, violating the confidentiality of private documents and other papers, damaging or threatening the operation of public benefit organisations, etc., but especially so - called computer crimes (Section 230-232 of the Criminal Code, formerly Section 257a of Act No. 140/1961 Coll., the Criminal Code). From the very beginning of their criminalisation, we have seen a rapid increase in detected attacks, not to mention considerable latency. Despite the increasing number of solved cases, the range of offences is far from covered, so the clearance rate in recent years has remained at around one third. The situation in terms of judicial statistics seems only slightly better, with the number of convicted offenders to those prosecuted wavering at over one half, and around three quarters to those accused.

Basic data on cybercrime can be found in statistics, especially a combination of police and judicial statistics, with the addition of summary data from the Czech Statistical Office. Attention is usually focused on computer crimes, due to the difficult, or virtually impossible separation of cybercrime, e.g. fraudulent conduct collectively classified under Section 209 of the Criminal Code.

Certain information on the extent of cybercrime in the Czech Republic can also be gleaned from other research projects studying the online environment, although these mainly focus on phenomena other than cybercrime, particularly cyberbullying, child sexual abuse, social networking and in recent years, fake news. The picture is complemented by various research projects (only marginally dealing with cybercrime) and ad hoc or regularly published reports by various institutions and organisations (e.g. National Cyber and Information Security Agency). Of course, professional literature also deals with the issue; in the Czech environment, the work of V. Smejkal, J. Kolouch, R. Polčák and T. Gřivna, or teams led by them, is particularly noteworthy. Finally, there are also a number of professional conferences and similar meetings, especially the annual Cyberspace conference in the Czech Republic.

The project and its implementation

The Institute of Criminology and Social Prevention (ICSP) responded to the growing importance of cybercrime with the research task "Identification and Assessment of Types and Trends of Crime Committed via the Internet (Cybercrime) or Other Social Networks". The subject was selected forms of cybercrime in the Czech Republic and public experience with these crimes. The project was aimed at acquiring, analysing and evaluating new information about the prevalence of selected forms of cybercrime, offenders and their criminal activities, together with the acquisition, analysis and evaluation of information on public awareness of potential threats in cyberspace, their own experiences with cybercrime in the role of victims or offenders and self-protection measures. This is the first research project in the Czech Republic examining cybercrime through an analysis of court files, which goes beyond case studies and published statistics and aims to obtain statistically processable data that can be compared over time.

The first step was a study of national and foreign professional literature and relevant official documents (see **Chyba! Nenalezen zdroj odkazů.**), including legislation and available case law. This was followed by an analysis of judicial and police statistics (for more details, see **Chyba! Nenalezen zdroj odkazů.**). We then approached the core part of the project - studying selected criminal files and analysing the findings. These became the basis for the focus of the questionnaire survey for the general internet population, or respectively a representative sample of internet users aged from 16-74, the results of which will be published separately. We supplemented this data by consulting with selected experts (police officer, two IT specialists, including an employee in critical infrastructure). Partial results of the project were continuously presented in print form, online and in person, especially in the form of conference presentations (for more details, see **Chyba! Nenalezen zdroj odkazů.** and **Chyba! Nenalezen zdroj odkazů.**).

For the analysis of criminal files, we selected proceedings in which an indictment was filed for the commission of a computer crime (in all cases this was unauthorised access to computer systems and information media pursuant to Section 230 of the Criminal Code, or in conjunction with another computer crime), which ended with a final verdict in 2015. We ultimately had 66 criminal files (out of a total of 71 cases) involving 68 accused. This number is on the threshold of statistically relevant data, but constitutes virtually the complete final (and enforceable) judicial agenda for 2015.

The analysis of criminal files took place by searching for and recording monitored variables on record sheets. Fifty items were monitored this way, primarily comprising basic data about the accused (and marginally on the victims), the crime itself and the course of criminal proceedings. Most data included the accused, i.e. offenders, as well as those whose prosecution ended with a verdict other than conviction. We monitored general data (e.g. the court that issued the decision on the merits of the case), information on the legal assessment of the offence (e.g. qualification, concurrence, etc.), the final decision in the case (including the sentence imposed), the course of criminal proceedings (especially the length of individual stages of proceedings), the accused (sociodemographic data, previous criminal activity, etc.), the offence as such (especially the manner it was conducted and the platform used, the offender's motivation, data on victims, the damages caused, etc.).

Selected results

The analysis of criminal files provided lots of interesting information, albeit subject to its limited indicative value in view of the low numbers and expected high latency. Computer crimes are usually decided by a district court; in about two thirds of cases, the offender acted in concurrence with another offence (mainly of a financial/economically motivated nature). In one quarter of cases, the court acquitted the defendant or discontinued proceedings; convicted offenders were most often sentenced to imprisonment, which was conditionally suspended.

Unconditionally convicted offenders included a group of younger recidivists (aged 24-35), against older first-time offenders (aged 41-58), who abused their job positions to gain unauthorised access to non-public information systems. On the other hand, for example, offenders sentenced to community service by the court committed acts of virtual violence (mostly for revenge or out of jealousy), at an age not exceeding 22 (the stated age corresponds to the moment criminal proceedings commenced in all cases).

In less serious cases, where there was no doubt of the facts, and the matter could therefore be decided by a single judge who issued an order of summary punishment, the vast majority of cases involved the manipulation of data (deletion, modification, insertion of third-party data). The offenders mostly attacked people from their immediate surroundings (80%), or in connection with their employment (colleagues, employers 21%).

An interesting category was the 27 proceedings involving offences without concurrence, where the court imposed a penalty solely for computer crime. In all cases, this was

unauthorised access to a computer system and information media (Section 230 of the Criminal Code, without distinction between the first and second paragraph). The court convicted 18 offenders, 14 of whom received a prison sentence (on average 6 months), which the court conditionally suspended. The proceedings lasted an average of 1.4 years, while pre-trial proceedings were usually a bit longer. In about one half of cases, the offenders abused access to information technology (physical access to, for example, a laptop or knowledge of someone else's password).

Criminal proceedings lasted an average of 1.5 years (74 days to almost 5.5 years); 90% of cases were completed within 2.5 years. Pre-trial proceedings took an average of 0.8 years (4 days to 3 years), and proceedings before the court 0.7 years (17 days to 4 years). The use of remedies probably played a role in this respect (they were duly used in about one quarter of cases), while concurrence with other criminal activity, for example, did not. The total length of proceedings correlates slightly more with the length of proceedings in court than with the length of pre-trial proceedings, with the duration of pre-trial proceedings prevailing in most cases resolved within 2 years.

In cases pending for more than 3 years (n = 7), offenders, with an average age of 43 and economically motivated interests with the exception of one case, abused their access to an information system, thus most often damaging their employer (and possibly the subjects of attacked personal data).

The most numerous group were accused under the age of 24, in the range of 17-58, with an average age of 34, almost half are under the age of 30. Approximately 40% of accused were in a marital or similar relationship at the time criminal proceedings commenced. Ten accused committed their offences in connection with their position as a public official, including five members of the Police of the Czech Republic. Of the total of 26 recidivists, there were only two with special recidivism involving computer crime (in both cases the misuse of someone else's e-mail and so-called m-payments using mobile phones and social networks).

One fifth of accused were women, half of whom were aged 35-49 (in the range of 19-56, with an average age of 38). Two thirds of them had a high school diploma or higher education (more than one half of accused men were less educated). Similarly, the court convicted two-thirds of accused women, the most frequent sentence being a suspended prison sentence. Thus, a smaller percentage of women were convicted than men, however, imposed sentences were on average longer. Compared to accused male recidivists (30%), female recidivists

accounted for about one third (approximately 13%) of accused women. While offences committed by accused men and women can be described as virtual violence in about one half of cases and financial crime in the other half, this ratio changes to (only) 30% virtual violence when looking at convicted female offenders.

Accused can also be divided into roughly half based on an age limit of 30; the younger half of accused had only basic education at the time of criminal proceedings. Compared to an approximately 50% share of recidivists in total crime in 2015, we only found one third of recidivists among younger accused, and only one fifth in the older category. Therefore, cybercrime seems to be the domain of first-time offenders. The court more often imposed a secondary sanction with the main sentence in the case of older offenders, usually prohibited activity.

Exactly one half of accused had at least a high school diploma (including one third of women), of whom one third had a university degree, while all university graduates had hitherto clean criminal records. Among less educated defendants, about one half had previous experience of crime.

In more than one third of cases, the accused were suspected of misusing access to ICT provided in connection with their employment or through the trust of the victims. In almost one fifth of cases, the accused were suspected of misusing another person's login data to various accounts (mainly social networks and e-mails, as well as internet banking). Similarly, they often found login data somewhere (e.g. stored on a computer, written on a piece of paper). The use of technical means was minimal. The weakest points of protection thus include physical security, as well as the protection of e-mails, profiles on Facebook and information systems accessible to employees. Of personal data, the most widely misused are passwords.

Offences can again be roughly divided in half into virtual violence and financial/economically motivated crime, where this division cuts across various different categories, including, gender, age and education. We find differences, for example, when taking into account the position of a public official (all but one pursued financial interests) or concurrence (in three quarters of cases the accused acted concurrently with financial interests, but only in half of virtual violence). More specifically, in 40% of cases, the offence was an attempt to improve the accused's financial situation and in 30% a consequence of a complicated relationship situation (other forms - such as a prank - were less common). For example, offenders posted

intimate photos of the victims, accessed their accounts on social networks and e-mails without authorisation, or contacted other people on their behalf, etc. We expect the merits of the classification into virtual violence and financial/economically motivated crime (and others) to be confirmed in the future and enable good research comprehension of this topic. This would be significantly helped, for example, by the inclusion of the online environment in publicly accessible registers of statistical data.

In one half of cases, access to ICT was misused for offences with financial interests. It's worth mentioning three type groups - mostly educated people without criminal records: members of the Police of the Czech Republic who abused access to police information systems; "resourceful women" who abused their position at work to resolve their poor financial situation; and "data moguls" who misused clients' personal data from their employer's information systems. Other groups with financial interests include "geeks" who abuse their ICT skills to access a specific device or information system, and "online thieves" who obtain login data to the various accounts of victims (from their immediate surroundings) through which they gained access to funds.

In contrast, in virtual violence (where the accused knew the victim in 90% of cases), we only find two type groups, namely "avengers" and "jealous people". Jilted avengers, younger men (on average 26 years old) without previous criminal records, harmed their former partners through slander, online attacks, misusing their social media accounts, etc. Jealous attacks targeted past and present partners and harmed them in the same way as avengers, but they also sought control of their victims. In both groups, offenders misused victims' passwords or devices that they learned or used during their relationship.

Both natural and legal persons were injured parties in proceedings. In three quarters of cases there was only one victim, with 2-5 individuals in the remainder, except for 4 criminal proceedings, where there were dozens to hundreds of victims. The offenders committed up to 782 attacks (partly unsuccessful) and in 40% of cases caused financial damage in the amount of CZK 1,200 to CZK 27 million. Non-pecuniary damages were reported in 70% of cases, but were only quantified in one case. In just under two thirds of cases, the accused knew the victims personally (in one third this was their current or former partner, one fifth were simply acquaintances and one tenth were relatives) and one third attacked their employer (current or former).

Accused in an employment or service relationship to the injured party were slightly older, averaging 38 (21-56) years of age. Among the 23 accused in this context, seven were civil servants (three social workers, four members of the Czech Police). Offences took many forms. For example, a social worker drew social benefits instead of deceased clients; a bank employee set up loans to her benefit using the personal data of fictitious persons (with the highest damages of CZK 27 million and longest sentence of 9.5 years in prison); a member of the Czech Police provided information on ongoing criminal proceedings for payment. In other cases, for example, there was the corruption of data in a company database or data transferred to competitors.

Recurring phenomena included e-mail attacks, from simply viewing the contents to their manipulation or taking over the identity of the mailbox owner (communicating on their behalf). E-mails contain a wide range of important information: e.g. the mailbox owner's contacts or part of their daily schedule, and especially the contents of the communication itself, often including login details for other applications, particularly social networks, or serving as the contact e-mail for restoring access. E-mails played a significant role in about one quarter of cases and included virtual violence (e.g. searching for infidelity or communicating on behalf of the victim) as well as financial interests (e.g. changing billing information or forwarding e-mails to competitors). As a rule, such actions were facilitated by the victims themselves, who did not sufficiently secure their passwords. These were simple (e.g. the name of the attacked institution), physically accessible (e.g. stored on a borrowed laptop), unchanged (misused by a former employee after the termination of their employment or a partner after a breakup), or easily recoverable for offenders (e.g. thanks to a simple security question).

As part of the project, we also examined the specific issue of cyber-grooming, establishing contact with children in the online environment for the purpose of their sexual abuse. Offenders contact the victim, maintain sexually oriented communication with them, build emotional addiction, lure intimate content from them (especially photos and videos to pornographic material) and then blackmail and threaten to obtain more such content, or force the victim to meet in person and engage in sexual activities of a physical nature. Such conduct has therefore been criminalised (among other things) since 2014 under the establishment of illegal contact with a child (Section 193b of the Criminal Code). The number of convicted cases (mostly first-time offenders and more often under the age of 30) has since increased to

45 convicted offenders in 2019, with their characteristics and modus operandi roughly corresponding to those presented in professional literature.

We also conducted three semi-structured interviews with selected experts (a member of the Police of the Czech Republic and two IT employees, including one involved in critical infrastructure). They all talked (on their own initiative) about ransomware, at least two of them agreed on other topics such as fraud in international trade, child pornography, infrastructure weaknesses (especially local network and server security), social engineering (in relation to, among other things, employees), data collection by large corporations, risks due to neglected updates, the use of cloud services and of course the topic of employees as a potential risk and the human factor in general (especially carelessness associated with login data): "*the biggest threat is from users in the local network*." They also mentioned the issue of detecting and sanctioning offences given the transnational nature of the internet and related phenomena such as difficult law enforcement or organised crime. They also focused more attention on cryptocurrencies and, to a lesser extent, fake news. In particular, they consistently recommended regularly updated protection/security software and education - to ensure typical and current cases receive appropriate publicity and training employees and ordinary users in the field of ICT security (with an emphasis on caution relating to login data).

The last part of the project is a questionnaire survey, which will be reported separately in 2021. This publication presents an outline of cybercrime research relevant to the Czech Republic, the methodology (selection of respondents and method of questioning) and individual areas covered by the questionnaire in more detail (self-protection by ICT users, the degree of their victimisation by selected phenomena and their experience in the role of offender, including consideration of activities and devices related to employment).

In conclusion, we reflect on some of the shortcomings or weaknesses of the ending project (e.g. narrowing the analysis of criminal files to computer crimes and their number), on findings that would perhaps deserve more attention (e.g. younger recidivists compared to older first-time offenders), our own considerations (e.g. the classification of cybercrime into financial/economically motivated crime and virtual violence) and, last but not least, the focus of any future project (especially the continuing analysis of criminal files).

Translated by: Presto