EÖTVÖS LORÁND UNIVERSITY

DOCTORAL SCHOOL OF LAW

DOCTORAL PROGRAMME OF CRIMINOLOGY

THE CAUSES OF CYBERCRIME AND OFFENDING – A CRIMINOLOGICAL STUDY OF CYBER-DEPENDENT CRIME IN HUNGARY

THESES OF THE DOCTORAL DISSERTATION

Árpád Varga

SUPERVISORS:

Dr. Katalin PARTI, assistant professor

Dr. Miklós LÉVAY, professor

LEADER OF THE DOCTORAL SCHOOL:

Dr. Marianna NAGY, professor

Budapest

2023

Tartalomjegyzék

1. Objectives of the doctoral thesis

The study of cybercrime is a new field of criminology, however the development of information technology started in the 1960s. The first significant cybercrimes were already well publicised in the 1980s and by the end of the 1990s they had become a visible phenomenon at the societal level, especially in the United States[1] , but the Council of Europe[2] and the OECD[3] had also started to map the field since the late 1980s. By the early 2000s, the first documents had been drawn up which laid the foundations for action against cybercrime in Europe, including Hungary.

Hungarian criminology, however, still deals only sporadically with cybercrime. Most of the works published since the early 2000s examine crime and victimisation, which affect a broader section of society. However, there is a distinct lack of research that examines cybercrime, that are IT skill-based and dependent on the knowledge of information systems. This area is referred to by Marleen W. Kranenbarg as computer-related crime as cyber-dependent crime[4], by Katalin Parti and Tibor Kiss as computer-related crime[5] and by David S. Wall as crimes that violate the integrity of computer systems[6].

Although more and more researchers investigate this area at international level, there is a lack of research in Hungary that would specifically analyse so-called malicious hacking, committed by black hat *hackers*.

The aim of this dissertation was therefore twofold: to provide an exploratory study summarising the general characteristics and situation of cyber-dependent crime in Hungary, and to identify the patterns and influences that play a role in becoming a cyber offender and the potential exit from offending.

The first task of the research required an exploratory quantitative desk research to identify the most significant cyber-dependent crimes in Hungary and to map the presence and typical patterns of cyber offenders. By reviewing 274 prosecutions initiated between 2013 and 2018

---

[1] Majid YAR: *Cybercrime and Society*, SAGE Publications Ltd, 2006. 28.
[2] Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime https://rm.coe.int/09000016804f1094
[3] *Computer related crime: analysis of legal policy*. Paris, Organisation for Economic Co-operation and Development, 1986.
[4] Marleen W. KRANENBARG: *Cyber-offenders versus traditional offenders: an empirical comparison*. Netherlands, Vrije Universiteit, 2018 (Doctoral dissertation) https://research.vu.nl/en/publications/cyber-offenders-versus-traditional-offenders-an-empirical-compari
[5] KISS Tibor – PARTI Katalin: Informatikai bűnözés. In: BORBÍRÓ Andrea – GÖNCZÖL Katalin – KEREZSI Klára – LÉVAY Miklós (szerk.): *Kriminológia*. Budapest, Wolters Kluwer, 2016. 491–517.
[6] David S. WALL (ed.): *Crime and the Internet: Cybercrimes and Cyberfears*. London, Routledge, 2001.

by the eight district prosecutors' offices in Budapest, the file research allowed me to map the presence, main characteristics and dynamics of cyber-depending offending.

The dissertation aimed to answer the following research questions:

1. What are the characteristics of cybercrime in Hungary?
2. Can we identify the characteristics of cyber-dependent crime in the files of the Budapest District Prosecutor's Offices?
3. Can we identify any suspects or perpetrators of the cybercrimes under investigation?
4. What information do we have about the perpetrators of cybercrimes and what IT skills do they have?
5. What problems arise in the investigation of cybercrime?

Answering the questions did not require a criminal law analysis, so the analysis of the files was specifically focused on the criminological characteristics of cyber-dependent crime and included the examination of Articles 375, 392, 394, 423 and 424 of Act C of 2012 on the Criminal Code (hereinafter: Criminal Code).

The other aim of the dissertation was to understand the characteristics of becoming a cyber offender, the characteristics of the offending career and the reasons for possible exit from offending by using the criminological theories. This required the selection of appropriate criminological theories and the synthesis of their components.

The testing of the theoretical framework required a semi-structured in-depth interview survey based on a snowball method due to the low number of available hackers already involved in IT offences. This qualitative method provided an opportunity to partially understand the life histories of the offending hackers, to explore their attitudes towards IT, their motivations and attitudes. The interview research took place between October 2021 and December 2022 and was conducted with a total of 11 self-reported hackers involved in at least some minor IT offences. This is further complemented by a re-analysis of two of my interviews with offending hackers in my 2014 Criminology Master's degree research paper[7]. Reasons for the low number

[7] VARGA Árpád: *Számítástechnikai bűnözés és elkövetők – A bűnelkövetővé válás okainak és jellemzőinek vizsgálata*. OTDK dolgozat. 2014. (kézirat).

of interviewees include the high level of distrust among hackers and the high latency in the field.[8]

The interview research aimed to answer the following research questions:

1. What are some examples of cybercrime in the Hungarian hacker community?
2. Are the scientific hacker definitions and typologies used in Hungary among hackers and to what extent do the respondents accept them?
3. Where are the boundaries between the legislative environment and the activities of hackers according to them?
4. Is there a correlation between family patterns, peer attitudes, norms of online communities and reward systems for hacking towards cybercrime? (Differential Association-Reinforcement theory)[9]
5. In the case of infringements committed or suspected to have been committed by the interviewees, did neutralisation factors arise (in particular denial of responsibility, denial of harm or reference to higher values)? (Neutralisation theory)[10]
6. Are the cyber offences in the Hungarian hacker community form an adolescence-limited period, or is there a trend towards a career in crime? If so, are there any exit points in the career (Life-course theory)?

2. The research methodology of the thesis

2.1. Methodology of the exploratory file research on cybercrime

The aim of this dissertation was to explore the most important characteristics and knowledge needs of Hungarian cybercrime. In order to develop a realistic picture of Hungarian cybercrime, it was necessary to review the registered crimes, to review the literature and, to a small extent, to identify anomalies in the prosecution of cybercrime.

---

[8] Alice HUTCHINGS – Thomas J. HOLT: Interviewing cybercrime offenders. *Journal of Qualitative Criminal Justice & Criminology*, 7:1, 2018. 75–94.
[9] Robert L. BURGESS – Ronald L. AKERS: A Differential Association-Reinforcement Theory of Criminal Behavior. *Social Problems*, 14:2, 1966. 128–147.
[10] Grasham M. SYKES – David MATZA: Techniques of Neutralization: A Theory of Delinquency, *American Sociological Review*, 22:6, 1957. 664–670.

The research includes an analysis of some of the cases launched between 2013 and 2018. The data collection was limited to Budapest, a decision motivated by the concentration of cases in Budapest as shown in the crime statistics and also the assumption that companies, firms, financial institutions and many website hosting providers involved in cybercrime have their headquarters in Budapest, so that the targets with a higher probability of cyber-dependent offences are located here. As a consequence, the aim of the exploratory research was to achieve a high number of such cases rather than representativeness. The selection of Budapest cases was also justified by the fact that the two most important offences included in the research from 2016 onwards (Article 423 and 424 of the Criminal Code), became the responsibility of the IX District Prosecutor's Office.

According to the agreement, files were made available by the Prosecutors Office between 2013 and 2018. The research involved the review of 274 cases prosecuted under the Articles of 375, 423, 424, 392 and 394 of the Criminal Code.

The primary focus of the research was to map offending behaviour and offender characteristics, so only a small part of the data on criminal procedure was included, while statistical data analysis was not an integral part of the research.

2.2.Methodology of the qualitative interview research

The dissertation also included an interview research of the Hungarian hacker community. This is explained by the fact that file research alone is not suitable for identifying the characteristics of Hungarian cyber offenders, so the use of alternative methods of insight was essential. The specific attitudes, outlook and life path of the hacker community required semi-structured in-depth interviews. The primary aim of the research was to map the pathways leading to offending behaviour, to understand the learning processes of hackers and to test the applicability of selected criminological theories on Hungarian cybercrime.

The input condition for the research was the commission of an act that the interviewee suspected or that could be considered a crime under the Criminal Code. The purpose of this criterion was to ensure that the research subjects were only persons who were presumed to have committed a criminal cyber offence in their lives.

The research used this criterion to explore the thoughts, life paths, major activities and dilemmas of hackers in the grey and black zones. The survey is primarily designed to explore

the motivations for hacking, life-course turning points, the process of learning and neutralisation. Due to the preferences of the interviewees, the focus of the research was largely but not exclusively on moral dilemmas around vulnerability testing.

In the selection process, emphasis was placed on self-definition of knowledge, so that participants themselves spoke about the extent of their knowledge and how it differed from the 'average user' level.

The most difficult part of the research was the recruitment. Based on international experience, it was planned to conduct at least 20 in-depth interviews. However, the participation in the hacker conference and the activity in online forums and chat rooms did not live up to expectations. It became clear from the contacts that the participants were reluctant to cooperate because of the perceived risk of prosecution. This attitude during the data collection period is consistent with the observation made by Hutchings and Holt.[11]

In order to increase the usefulness of the research, two interviews conducted along similar research questions for the 2014 National Student Research Conference were re-analysed, drawing on the practice once used by Jordan and Taylor[12] .

The survey included nine men and two women, the youngest respondent being 17 years old and the oldest 49 years old. The interviewee with the lowest level of education by age was a 17-year-old high school student, while several interviewees had the highest level of education, including a Master's degree.

3. Results of the dissertation

3.1. Results of the explanatory file research on cybercrime

The file research has painted a picture of Hungarian cybercrime in which – at least in Budapest – low-skilled cyber offences still predominate. The overwhelming majority of cases are dominated by cash withdrawals with stolen credit cards and online or offline payments with stolen credit cards. Moreover, the number of cases is nowadays rather small compared to the overall crime rate, and their modus operandi cannot be considered as offences requiring skills beyond the ordinary IT knowledge. Around two thirds of the cases investigated and detected

[11] HUTCHINGS–HOLT i.m.
[12] Tim JORDAN – Paul TAYLOR: A sociology of hackers. *The Editorial Board of The Sociological Review*, Oxford, 1998. 762–763.

under Article 423 of the Criminal Code are abuses involving password stealing or the use of a previously shared password. The remaining part of the cases had foreign connections where almost no information was available on the real situation of cyber-dependent crime in the country.

The result of the explanatory file research in case of Article 423 of the Criminal Code led to the following findings:

- In Hungary, the Budapest cases seem to be dominated by accessing and modifying email addresses and social media profiles.
- Around two thirds of these cases involve easy methods, in particular previous knowledge of passwords (e.g. during a relationship).
- Victims often give their login details to the offenders themselves.
- The reason for access is usually some kind of relationship or family problem, while to a lesser extent email addresses are used to prepare the commission of some other crime for financial gain.
- Access to the social media profile is preceded by access to the email account.
- The vast majority of known intrusions did not require any IT skills.
- Out of the 85 cases examined, only 16 (18.8%) clearly involve an offence requiring a higher level of IT knowledge, of which 11 cases are linked to vulnerability exploitation or DDoS attacks. Only three of these cases resulted in the perpetrator being prosecuted.
- There are also scattered examples of sophisticated cyber-dependent crime in Budapest, but their prevalence was not yet significant in the period under review.
- In cases where the perpetrator has IT skills, such as using software, zombie network or IP address masking to change the location of the access point, the number of successful investigations is negligible.
- The investigating authority can try to detect the offence by contacting the e-mail service providers and requesting data from the ISP, but the passage of time or the foreign access point makes it unlikely that the procedure will be successful.

The result of the explanatory file research in case of Article 375 of the Criminal Code led to the following findings:

- Based on the 174 cases examined, fraud detected by the investigating authority using information systems are not cyber-dependent offences, with a few exceptions.
- The number of offences that demonstrate skills beyond the average IT knowledge is also negligible.
- The detection success rate is high for cases where the offence does not involve any IT knowledge and is linked to the use of physically stolen credit cards or credit card data.
- For cyber-enabled crimes, there are a high number of cases where the victim provides the pin code themselves or the offender finds it next to the card.
- In some cases, offenders try to use the cards even in the absence of a pin code. This practice occurs when making online payments and purchases using paypass.
- Cases where credit card data has been accessed through online payments, purchases were made abroad or malicious software were used are signs of cyber-dependent crime.
- In such cases, however, there are not exhaustive data available to analyse the technological circumstances of the crimes.
- Based on the examples of phishing in the literature, the criminal activity in IT arises in cases where data is transferred and used abroad.
- In the case of fraud committed abroad, the investigative authorities have not been successful in any of the cases.
- In the cases investigated by the Budapest District Prosecutor's Offices between 2013 and 2018, there was only one where the offender may have had skills above the average user and was identified. In this case, the offender was considered a *script kiddie*.

It is important to note that the Kranenbarg grouping is still valid from a criminological point of view, but it does not coincide with the criminal law, because while intrusions and other breaches of information systems or data can be considered cyber-dependent offences, the vast majority of the perpetrators do not fall under the definition of a cyber offender. It is therefore worthwhile to judge the offences from a criminological point of view on the basis of the knowledge required to commit them and to distinguish cyber-dependent or cyber-enabled offences along these criteria.

Due to the low number of cases, in case of the Article 424, 392, and 394 of the Criminal Code, it was not possible to formulate well-founded conclusions with regard to the five research questions.

3.2. Results of the qualitative interview research

The analysis of the interview research revealed that the vast majority of hacking incidents are limited to juvenile offences, mainly focused on vulnerability disclosure, but there are also sporadic cases of more serious acts that pose a threat to society. For the majority, these offences have faded from young people's lives as their legal awareness has increased, their university education has improved and the ethical dilemmas of the hacker community have become clearer. In comparison, a smaller proportion of young people refrained from more serious offences, but sometimes, out of positive reinforcement and, for example, excitement, vigilantism or the desire to help, committed minor or major offences that were not brought to the attention of the authorities. The third type of life paths include those for whom pro-offending definitions and alternative understandings of the world of information technology, combined with the need to cope with the difficulties of private life, have contributed to a stronger and longer lasting offending. In this case, it can be seen that the length of a career depends on the individual's environment and opportunities. Legal prosperity, finding pathways to IT knowledge, arguments in favour of traditional IT careers and the positive aspects of a stable family environment may tip the scales towards a conform lifestyle.

In terms of life courses, it can also be seen that while Moffit's theory[13] generally distinguished between juvenile and lifelong offending, cyber-dependent offending involves a third life course, which is the group of episodic offenders. In their case, we can speak of two sub-groups: old-school hackers and 'swinging' hackers more interested in malicious hacking.

In case of the two groups with adult offending (episodic offenders and career offenders), it can be seen that positive reinforcement and neutralisation (especially the reference to higher values and denial of responsibility) increase the chances of offending. On the other hand, in this case the IT sector's paths to high incomes and prosperity make it more rewarding to choose legal routes, there is no need of a coherent offending career.

---

[13] Terrie E. MOFFITT: Adolescence-Limited and Life-Courses-Persistent Antisocial Behavior: A Developmental Taxonomy. *Psychological Review*, 100:4, 1993. 685–694.

In the case of career crime, however, it can be seen that financial cybercrime occurs when there are no positive experiences from society, such as family life, professional life or online relationships, that make law abiding lifestyle attractive. In such cases, delinquency is an alternative means of validation. Thus, for two interviewees, for example, alternative definitions, the normativity of data misuse and the exclusion from legal careers had a strong effect on reinforcing associations with delinquency. In contrast, the hacker who had a career as an offender as a young adult was driven towards a conventional career by the opening of legal avenues for success and the possibility of a stable family life, such as support from a relationship, even if the lack of prosecution for offending and the financial rewards helped him at this stage of his life.

In terms of social learning theory, it can be seen that differential-association, pro-criminal definitions and positive reinforcement also play an important role in the commission of cyber offences. However, these are not particularly stable and their effects are not always directly perceived by the individual. Thus, in a good number of cases, sometimes one narrative and sometimes another emerges from the confusing moral and ethical rules of the IT profession as a whole. This is most apparent in differential associations and definitions because the wealth of information available online and the ideas behind it often leaves the hacker community unable to define precisely the boundary between legally objectionable acts and the social good. Therefore, especially at a young age, the desire for knowledge, professionalism and curiosity also increase the acceptability of acts that are essentially punishable. Often, following supportive feedback and experiences of success, they may thus become attracted to actions that later lead to moral dilemmas, such as guilt.

The applicability of the analysis presented in this dissertation and the two theories examined in the context of the life course is therefore supported, but only in the case of cyber-dependent offenders. The good identification of the interviewees' life histories and the lengthy interviews, often including their views on their own IT environment, showed results consistent with the research in the literature and presented in the dissertation.

4. Publication list

VARGA Árpád: A számítógépes sütik és az adatgyűjtés problémája. In: Koltay András – Török Bernát (szerk.): Sajtószabadság és médiajog a 21. század elején. 4. kötet. Budapest, Wolters Kluwer, 2017. 233-263.

VARGA Árpád: Review of the Monograph on 'Information – Society – Security': Zsolt Haig: Információ – Társadalom – Biztonság. In: Marcel, Szabó – Petra, Lea Láncos – Réka, Varga (szerk.): Hungarian Yearbook of International Law and European Law 2016. The Hague, Hollandia, Eleven International Publishing, 2017. 741–743.

VARGA Árpád: Médiaértés a médiajog és a kriminológia határán: a digitális technológia kihívásai. In: Fazekas Marianna (szerk.): Jogi tanulmányok, Budapest, 2018. 439–450.

VARGA Árpád: Koltay András - Török Bernát (szerk.): Sajtószabadság és médiajog a 21. század elején 3. Recenzió. Magyar Jog, 65:3, 2018. 188–192.

VARGA Árpád: A kiskorúak online aktivitásának kriminológiai értelmezése, különös tekintettel az állam és a szülők szerepére. Belügyi Szemle, 66:12, 2018. 98–119.

VARGA Árpád: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. In Medias Res, 8:1, 2019. 145–167.

VARGA Árpád: Informatikai bűnözés egy ügyészségi aktakutatás tükrében. In: Kiss Tibor (szerk.): Kriminológiai Közlemények 80. 2020. 125–135.

VARGA Árpád: Az adathalászat általános jellemzői, trendjei és észlelési kérdései napjainkban. Infokommunikáció és Jog, 74, 2020. 14–20.

VARGA Árpád: Kiss Tibor – Parti Katalin – Prazsák Gergő: Cyberdeviancia. Könyvismertető. In Medias Res, 9:1, 2020. 184–187.

VARGA Árpád: Kriminológiai elméletek és informatikai bűnözés. In Medias Res, 1, 2021. 155–196.