CYBERCRIME – EMERGING ISSUE

Ivana Luknar, PhD[1]

Abstract: With the rise of social distancing, security of the Internet and online communication has become an essential issue and cybercrime an emerging challenge. Challenges inherent to cybercrime evolve just as quickly as the technology that creates those challenges. Therefore, it is recommended that more research be conducted for a better understanding of cybercrime and how rapidly-evolving technologies will alter the response of police in the future.

Keywords: cybersecurity, cybercrime, Internet

INTRODUCTION

In the world of mass contagion by coronavirus we are experiencing a lot of changes. Coronavirus spread across the world and forced people to stay at home. A general hypothesis is that coronavirus will push advanced technology and its adoption forward in almost every field of our existence including: E-government, medicine and healthcare, application of robotics, agriculture and food production, distance learning, etc. While the use of information technology (IT) appears to be the main tool to communicate and minimize the pandemic's impact of social distancing, the availability of Internet and online communication has become essential for any person, institution and even government. For sure, development of digital technology has produced many benefits to society, but it has also produced a wide range of cyber threats. Those threats can seriously harm and target individuals, industry, critical infrastructures and even governments. Parallel to the growth of the Internet, IT possibilities and increasing number of the users, the range of illegal cyber activities continues to grow. Considering all of the abovementioned aspects of the current situation brought about by coronavirus and technology development, it is not hard to predict cyber criminals as an emerging issue. The demand for cybersecurity evaluation has increased. Given the urgency of addressing these issues, purpose of this paper is to instigate worldwide governments to develop and reform digital strategies concerning cyber domain. First, the paper discusses the Internet and cybercrime by content analysis method. After that, the paper concludes by pointing out the need to improve understanding of cybercrime and offering recommendations to ensure better cybercrime prosecution in the future. This is also an overview of cybercrime, security and its problematic nature and difficulties of understanding it.

1 ivanaluknar@gmail.com

INTERNET

Undoubtedly, computer technology, and especially the Internet, has created a new space for people to interact and connect. Advanced technology and high-speed Internet connection has changed human social interaction worldwide and allowed for long distance fast connection and communication. Wide range of Internet usage for work, information and leisure (sharing photos and videos with friends, paying bills, searching, etc.) carries opportunity for nefarious individuals to exploit others using the Internet and advanced technology, resulting in cyber-victimization. The use of the Internet will continue to increase.

Table 1. World Internet usage statistics 2020 (Internet World Stats., March 3, 2020)

Internet Users 31 May 2020	Internet World %	Penetration Rate (% Pop.)	Growth 2000-2020	Internet World %
Africa	526,710,313	39.3 %	11,567 %	11.3 %
Asia	2,366,213,308	55.1 %	1,970 %	50.9 %
Europe	727,848,547	87.2 %	592 %	15.7 %
Latin America / Caribbean	453,702,292	68.9 %	2,411 %	10.0 %
Middle East	183,212,099	70.2 %	5,477 %	3.9 %
North America	348,908,868	94.6 %	223 %	7.5 %
Oceania / Australia	28,917,600	67.7 %	279 %	0.6 %
WORLD TOTAL	4,648,228,067	59.6 %	1,187 %	100.0 %

Many authors have written about the internet as powerful communication tool that has the potential to amplify and accelerate crime in a fraction of a second (Davis, 2012; Williams, 2008; Broadhurst, 2006; Humphrey & Schmalleger, 2012: 331). It goes beyond the concept of territoriality and functions independently of state borders. "The location of the offenders in relation to the scene of the crime is the characteristic of cybercrime that differentiates itself most from others… the criminal usually is not present at the [cyber] crime scene thus making apprehension difficult" (Speer, 2000: 260). The evolution of the Internet is a significant challenge. "While criminals may operate across jurisdictional boundaries, law enforcement cannot" (Finklea, 2013: 10), which results in the existence of jurisdictional struggles.

CYBERCRIME

There is no generally accepted definition of cybercrime (computer-related crime). Huge numbers of definitions have appeared, according to Furnell et al., "in part because the problem is dynamic and changes over time, and also because different sources have tended to assess things from differing perspectives (e.g. some may look particularly at external attacks and consequently exclude internal abuse, whereas others may focus upon malicious code threats and thereby omit other forms of attack)" (Furnell, Emm & Papadaki, 2015). For the purpose of this paper we have chosen some definitions of cybercrime:

- "crimes committed at a distance, with significant difficulties concerning the determination of the place of perpetration of such an offence, carried out by electronic means, in a digital sphere" (Pradillo, 2011: 364)

- "any crime that is facilitated or committed using a computer, network, or hardware device" (Gordon & Ford, 2006: 14)
- "any unauthorized, or deviant, or illegal activity over the Internet that involves a computer as the tool to commit the activity and a computer as the target of that activity" (Moitra, 2005).

Mainly, cybercrimes are traditional crimes, but facilitated in an electronic environment. That is why cybercrimes can look similar to traditional types of offending. Technology has allowed criminals to expand their scope with more pathways thus making crime more complex, while anonymous nature and indirect involvement reduce the probability of cybercrime punishment. Cybercrimes imply the use of computer technology to perform or facilitate the commission of unlawful acts, and also crimes against computers, networks and systems. So, computer can be both the tool and the target of an offense. Broadhurst has summarized the wide scope of cybercrime in this way:

- "Interference with lawful use of a computer. Cyber-vandalism and terrorism; denial of service; insertion of viruses, worms and other malicious code.
- Dissemination of offensive materials. Pornography/child pornography; online gaming/betting; racist content; treasonous or sacrilegious content.
- Threatening communications. Extortion; cyber-stalking.
- Forgery/counterfeiting. ID theft; IP offences; software, CD, DVD piracy, copyright breaches, etc.
- Fraud. Payment card fraud and e-funds transfer fraud; theft of internet and telephone services; auction house and catalogue fraud; consumer fraud and direct sales (e.g. virtual "snake oils"); online securities fraud.
- Other. Illegal interception of communications; commercial/corporate espionage; communications in furtherance of criminal conspiracies; electronic money laundering" (Broadhurst, 2006: 413).

Davis mentioned three components of cybercrime: "1) a computer with which the action is perpetrated; 2) a victim computer; and 3) an intermediary network" (Davis, 2012: 273). Parker (Parker in: Humphrey & Schmalleger, 2012: 335) has identified seven different types of cyber criminals: 1) pranksters, 2) hucksters, 3) malicious hackers, 4) personal problem solvers, 5) career criminals, 6) extreme advocates, and 7) malcontents, addicts, irrational and incompetent people.

Cybercrime has evolved from the typical computer crime of the past to other more complex computer offense forms and will continue to change as malicious users become more technology-savvy and gain easier access to computers. For sure, cybercrime has changed from simple variations of existing categories of crime to more complex forms.

Today, a good deal of uncertainty exists in addressing crimes with a cyber-component. A lot of issues have complicated cybercrime investigations. Bossler and Holt mentioned some of them: "the lack of a standard definition for cybercrime; little public outcry in comparison to traditional forms of crime; difficulty in investigating an invisible crime; an inability to acquire and maintain the required technologies needed to investigate these offenses due to resources; difficulty in training and retaining officers; and gaining managerial and line officer support for investigating these forms of crime" (Bossler & Holt, 2012: 167). They also indicate that police and prosecutors do not have enough knowledge and the resources needed to adequately investigate and prosecute cybercrime (Bossler & Holt, 2012). Computer-related crime cannot be investigated or prosecuted based on common law. Since many cybercrimes lack a visual element, users of the internet, computers and other forms of advance technology may not see responding to cybercrime as "real" police work. All of the above mentioned issues have contributed to a deficiency in reliable statistics and significant underreporting of cybercrime, which further makes assessing the actual prevalence of computer crime more difficult.

RECOMMENDATIONS

Recommendations for measures that can be taken to ensure multilevel defense against cybercrime:

- Consciousness use of the internet – "People have to have a common understanding of what to do to protect themselves, and why, know what to do" (Levi, 2017b: 15) and who to contact in case of cyber offense against them and their property. Generally refers to raising public awareness and knowledge of cybercrime through different campaigns. "Public awareness campaigns are an important component in policing cybercrime as they inform the public on existing threats, while providing knowledge on how they can protect themselves online" (Koziarski & Lee, 2020: 205).

- Conscious implementation of new digital technology in our work and lives (systematic control, planning, set rules, consideration of cause and effects) – Fast growing and increasing dependence on technology as well as complex nature of cyber space and cybercrime have created worldwide concern about how to deal with fast changes and issues, secure cyber space and combat cybercrime.

- International monitoring, juridical cooperation - Cybercrime issue is a challenge for both domestic and international law enforcement. Many authors agree that law enforcement responses and prevention strategies to cybercrime are often ineffective (Holt, Lee, Liggett, Holt & Bossler, 2019; Lee et al., 2019; Willits & Nowacki, 2016). Where those laws that concerns key aspects of information security and information assurance intersect in transnational cases maybe harmonized or conflict-ridden. Levi suggest to "reconsider some of the overlaps that exist between online and offline crimes, and think through the ways in which online is transformative either for levels and organisation of crime commission or for the balance between disruption (another ambiguous term) and the traditional detection, investigation and prosecution processes that constitute a criminal justice response" (Levi, 2017a: 15). Indisputably, both juridical and technical coordination between nations is essential for effective transnational law enforcement when we speak about cybercrime.

- Multilevel transnational cooperation – Discussing cybersecurity and cybercrime and international exchange of experiences: conferences, summits, workshops, congresses, conventions and other mechanisms, in many ways rise awareness about the cybercrime issues. Relations among nations concerning cybersecurity are mostly adjusted through treaty obligations such us: European Convention on Cybercrime, the United Nations (UN) Convention against transnational organized crime and The National Cybersecurity Framework Manual of 2012. Budapest Convention (The **Convention on Cybercrime** of the Council of Europe - CETS No.185) adopted in November 2001 and supplemented by a **Protocol on Xenophobia and Racism** committed through computer systems „remains the most relevant international instrument – the "gold standard" – on cybercrime" (Council of Europe, June 23, 2019). It was the first instrument that served as a guideline against cybercrime and a framework for international cooperation between 65 signatories (until today) to this treaty "on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation" (Council of Europe, November 23, 2001). The United Nations (UN) Convention against transnational organized crime indirectly deals with cyber-crime when carried out by criminal networks in relation to serious crime. Above mentioned instruments are designed to address rights and collaborations between countries regarding cyber activity. Those conventions provide examples of greater law harmonization. Because they have effectively established a complex network of activities, regulations and treaty obligations between convention signatories and fewer opportunities for

transnational criminals to exploit jurisdictional and legal loopholes between nations. "Convention signatories also are required to harmonize their internal domestic laws to allow for broad coverage of improper activity and consonance with the laws of other countries with which they must collaborate. Countries that have not signed on to the convention's requirements may need more ad hoc solutions to transnational collaboration, although bilateral treaty obligations between major technological nations fill some of those gaps" (Losavio, Pastukov, Polyakova, et al., 2019: 2).

- Reducing the dark number - When a crime occurs, willingness of the individuals who are victimized to report it is crucial in effective crime control because police can only intervene and a response by the justice system can be expected if cybercrime is officially noted. There are many reasons why "cybercrimes are less likely to be reported" (Graham, Kulig & Cullen, 2020: 11). "Experimental results show that people perceive a computer crime to be more serious when the data is more sensitive, the offender is motivated by financial gain, the amount of loss is high, and a large number of records are affected—in roughly that order. If sentencing reflected public perceptions, a crime with these features would be punished more harshly than a crime in which these factors are less true" (Graves, Acquisti & Anderson, 2019: 347). Cross, in her case study of online fraud, finds inability and frustration of victims to lodge a complaint because the uncertainty of who and where to report an offense to (Cross, 2019: 9, 36). Also, "a failure to improve law enforcement responses to cybercrime may negatively impact their institutional legitimacy as reliable regulators of cybercrime" (Koziarski, & Lee, 2020: 199). Studies on willingness to report crime to the police "find that legal cynicism is negatively correlated with perceptions of procedural justice and positively correlated with procedural injustice. Surprisingly, however, their models reveal cynicism to be significantly and positively related to reporting and beliefs about arrests – a counterintuitive finding" (Graham, Kulig & Cullen, 2020: 11). "Dark numbers" of cybercrime present a serious problem that cannot be alleviated by prosecution allowing offenders to continue breaking the law. Reporting and notification of cybercrime is also essential for monitoring cybersecurity and defense both at the state and international levels.

- Law enforcement responses - The concept of jurisdiction which refers to cybercrime is particularly challenging and problematic. As Crowther noticed, most cyber activity should not involve the military at all, but "militaries should be able to range anywhere throughout cyberspace to complete appropriate missions" (Crowther, 2017, 74). "It is quintessential for law enforcement to be effectively trained on what they have the capacity to do, given their contextual circumstances, as it may have the capacity to improve officers' perceptions. For agencies that have limited resources allocated for cybercrime, this may include speaking to victims, taking reports, and passing along information to other agencies that have greater cybercrime resourcing" (Koziarski, & Lee, 2020: 205).

- Improve cybercrime policing - "There is scope for a more dynamic, structured and response-focused approach to guidance, warnings and awareness-raising, and the police can play a collaborative role in arrangements to provide that advice before and after individuals become victims" (Levi et al., 2017b: 16). The focus is to improve cybercrime policing through updating and evaluating traditional police approaches, developing new, more efficient ways that could assist and improve cybercrime policing. Some authors encourage the emergence of "evidence-based policing (EBP)" (Sherman, 2013: 385; Koziarski & Lee, 2020: 199) and the use of "triple T" strategy: 1) targeting, 2) testing and 3) tracking (Sherman, 2013: 383-385) to develop and improve factors associated with policing wide range of crimes. Collecting and using digital evidence has produced notable benefits in the criminal justice system. "There are also jurisdictional challenges related to cybercrime and digital evidence as the Internet is boundless, and enables offenders to affect victims well beyond their physical reach. Investigators may recognize that an act occurred, but be unaware of the location of the offender relative to their jurisdictional boundaries due to the virtual nature of the offense" (Holt, Clevenger & Navarro, 2020: 94). Because many cybercrimes transcend multiple geographic locations, it is often

unclear which agency should respond. Police all over world struggle with addressing cybercrime and deciding on how to conduct adequate police investigations because of their ability / inability to acquire the necessary technology and knowledge, difficulties to retaining officers who possess the appropriate skills to deal with cybercrime, as well as insufficient training.

- - Dedicated well-trained police personnel - There is some tension regarding the question as to whether all police officers generally should be responsible for investigating cybercrimes and digital evidence or these investigations should be reserved for a smaller group of specialists. Some authors have suggested training all cadets during their time at the academy in order to facilitate their subsequent efforts to address the issue of cybercrime (Holt, Clevenger & Navarro, 2020: 100; Nowacki & Willits, 2020; Bossler & Holt, 2012: 168) or "employing specialist civilian staff" (Levi, Doig, Gundur et al., 2017b: 16). Nowacki and Willits consider dedicated personnel as "one of the most common law enforcement responses to cybercrime" (Nowacki & Willits, 2020: 73). Holt suggests the establishment of specialized cybercrime policing units with skills necessary to address cyber offenses and which tend to have higher levels of training to deal with these offenses (Holt, 2018).

CONCLUSION

As information-technology power grows exponentially, the majority of future crimes will contain a cyber-component. Widespread use of the Web and technological innovations indicates that cybercrime will become a more and more common issue with the time, and especially after worldwide changes designed to prevent coronavirus spreading when states across the world closed their borders and reduced social life to minimum. This new worldwide reality caused by coronavirus enhanced the reliance on IT communications and their security. Police and law regulations are experiencing a challenging era dealing with crime with cyber-components. This paper is an invitation to governments, IT experts and criminologists to increase awareness of the increased prevalence of digital devices as components of crimes and criminal investigations by applying their knowledge and skills to the improvement of cybercrime prevention and prosecution.

REFERENCES

1. Bossler, M. A. & Holt J. T. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management* 35 (1), 165-181.
2. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management* 29 (3), 408-433.
3. Council of Europe (2001, November 23). *Convention on Cybercrime, Details of Treaty No.185*, Budapest. Accessed on June 23, 2020. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
4. Council of Europe (2019, June 23). *Cybercrime Convention Committee (T-CY), Preparation of the2nd Additional Protocol to the Budapest Convention on Cybercrime*. Accessed on June 21, 2020. https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff
5. Cross, C. (2019). Oh we can't actually do anything about that': the problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice, Online*, 1-18. Accessed on June28,2020. https://eprints.qut.edu.au/127517/1/CCJ_Jurisdiction_online_fraud_accepted_CROSS.pdf

6. Crowther G. A. (2017). The Cyber Domain. *The Cyber Defense Review* 2 (3), 63-78.

7. Davis, T. J. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal of Police Strategies & Management*, 35 (2), 272-284.

8. Finklea, M. K. (2013, January 17). *The interplay of borders, turf, cyberspace and jurisdiction: Issues confronting US law enforcement*. Congressional Research Service Report for Congress, Washington DC: Congressional Research Service. Accessed on July 3, 2020. https://fas.org/sgp/crs/misc/R41927.pdf

9. Furnell, S., Emm, D. & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. *Computer Fraud and Security 10*, 5-12.

10. Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1), 13-20.

11. Graham, A., Kulig, T.C, & Cullen, T. F. (2020). Willingness to report crime to the police. Traditional crime, cybercrime and procedural justice. *Policing: An International Journal* 43(1), 1-16.

12. Graves, T. J., Acquisti, A. & Anderson, R. (2019). Criminology perception versus punishment in cybercrime. *Journal of Criminal Law & Criminology*, 109 (2), 313-363.

13. Holt, J.T., Clevenger, S., & Navarro, J. (2020). Exploring digital evidence recognition among officers and troopers in a sample of a state police force. *Policing: An International Journal*, 43 (1), 91-103.

14. Holt, T.J. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *The ANNALS of the American Academy of Political and Social Science 679*, 140-157.

15. Holt, T.J., Lee, J.R., Liggett, R., Holt, K.M. and Bossler, A. (2019). Examining perceptions of online harassment among constables in England and Wales. *International Journal of Cybersecurity Intelligence and Cybercrime*, 2(1), 24-39.

16. Humphrey, A. J., & Schmalleger, F. (2012). *Deviant Behavior*, 2nd ed., Canada: Jones & Bartlett Learning.

17. Internet World Stats (2020, March 3). Internet Usage Statistics. The Internet Big Picture. World Internet Users and 2020 Population Stats. Accessed on June 21, 2020. https://www.internetworldstats.com/stats.htm

18. Koziarski, J., & Lee J. R. (2020). Connecting evidence-based policing and cybercrime. *Policing: An International Journal*, 43(1), 198-211. DOI 10.1108/PIJPSM-07-2019-0107

19. Levi, M. (2017a) Assessing trends, scale and nature of economic cybercrimes: overview and issues. *Crime, Law and Social Change* 67(1), 3-20. Accessed on July 1, 2020. http://orca.cf.ac.uk/95719/3/Assessing%20trends%20final%20published.pdf

20. Levi, M., Doig, A., Gundur, R. et al. (2 more authors) (2017b). Cyberfraud and the implications for effective risk-based responses: themes from UK research. *Crime, Law and Social Change*, 67 (1), 77-96. Accessed on July 3, 2020. http://eprints.whiterose.ac.uk/144360/8/Levi%2C%20Doig%2C%20Gundur%2C%20Wall%20and%20Williams%20%282017%29%20Cyberfraud%20and%20the%20implications%20for%20effective%20risk-based%20responses%20-%20themes%20from%20UK%20research.pdf

21. Losavio, M.M., Pastukov, P., Polyakova, S., et al. (2019). *The juridical spheres for digital forensics and electronic evidence in the insecure electronic world*, WIREs Forensic Sci. 1:e1337. Accessed on June 15, 2020. https://doi.org/10.1002/wfs2.1337

22. Moitra, S. (2005). Developing policies for cybercrime", *European Journal of Crime, Criminal Law and Criminal Justice*, 13 (3), 435-464.

23. Pradillo, J. C. O. (2011). Fighting against Cybercrime in Europe: The Admissibility of Remote Searches in Spain. *European Journal of Crime, Criminal Law & Criminal Justice* 19(4), 363-395. DOI: 10.1163/157181711X587800.

24. Speer, D. (2000). Redefining borders: The challenges of cybercrime. *Crime, Law and Social Change 34*, 259-273.

25. Williams, K. (2008). Using Tittle's control balance theory to understand computer crime and deviance. *International Review of Law Computers & Technology*, 22(1-2), 145-155.

26. Willits, D. & Nowacki, J. (2016). The use of specialized cybercrime policing units: an organization analysis. *Criminal Justice Studies*, 29 (2), 105-124.