УДК 1
DOI 10.21661/r-114276

Б.М. Ибраева

ТЕОРИЯ ЦИФРОВОЙ ПРЕСТУПНОСТИ

***Аннотация**: хакеры кажутся самыми мистическими личностями в современном мире. Там, где легальные меры не помогают, хакеры могут вмешаться. Однако не только хакеры, но и государственные служащие совершают киберпреступления, как только приходят к власти. Это просто совпадение или власти и хакеры имеют много общего? Эта статья попытается пролить свет на причины, побуждающие людей совершать цифровые преступления.*

***Ключевые слова**: хакеры, власть, теория кибернетических преступлений, кибератаки, белые воротнички, киберпреступления, мотивы, причины, цифровые преступления.*

B.M. Ibraeva

THEORY OF DIGITAL CRIME

***Abstract**: hackers seem to be the most mysterious people in the contemporary world. Where legal actions are helpless, hackers can intervene. However, not only hackers but state employees commit cybercrimes once they get power. Is it just a coincidence or authorities and hackers have lots of things in common? This article is trying to cast light on the reasons why digital crimes are committed.*

***Keywords**: hackers, authorities, power, cyber-attacks, motives, reasons, cybercrimes, theories of cyber-crime, digital crimes.*

Introduction

Digital crimes include crimes committed on the internet as well as all types of crimes, perpetrated in the sphere of information and telecommunications systems. In this regard, the subject of the offense is all information resources and technologies, whereas the purpose of this violation is criminal trespasses. In short, cybercrime regarding non-legal intervention in the work of computers, software and computer nets

as well as an unauthorized modification of any digital data refer to the legal categories, where the object of the crime is the information security, whereas the computer is the subject. If we consider cybercrime as a social occasion, it can be an exchange using email messages containing the information about a venue of a future crime as well as an arrangement of any criminally oriented data on a website.

The European Union Convention, signed in 2001, November 23, identified all types of offenses in the field of information and telecommunications systems [1]. There is an unauthorized access to digital data and illegal interception of information, impact on computer systems and intentional criminal damage, deletion, deterioration, change or block digital data. The list also includes unauthorized usage of special technical devices to commit a crime, forgery, and fraud, distribution of child pornography or information promoting racism as well as hatred and inciting violence against minority groups.

Theories of Crimes

Criminology states for some arguments why people commit any types of crimes. There is Societal or Macro-Level and Community Theories, considered by Howitt [2], Control Theory described by McGuire [3] as well as Routine Activities Theory initially proposed by Cohen and Felson [4]. There are also Deterrence Theory, Influence Socialization, and Individual one as well as Strain Theories by Merton and Agnew [5] and many Psychological Theories including personality, pedophiles, and other mental disorders. Last but not least, there is Terrorism and Political Theory rooted in Karl Marx's book in 1887 [6]. All of them observe criminal issue at various levels. Their purpose is to dig deeper the psychological aspects of committed crimes [7]. In other words, the theories mentioned above aim to find out why crimes occurred [8]. However, the best argument explaining the nature of cybercrime is the Routine Activities' Theory [9] rooted in a theory of human ecology, presented by Hawley [10], which pointed to three significant temporal constructs of community structure: rhythm, tempo, and timing. The research done by Hawley revealed many cases when people who did not seem like common criminals committed digital crimes [11]. Taking into account some cyber offenses committed without any desire to cause harm, but due to

a high level of curiosity, another interesting theory explaining the causes of cyber-criminal behavior is Learning Theory that can shed some light on hackers' attacks [7].

The Nature of Hackers

So, let's consider the biggest group of cybercrime representatives – hackers. Many psychologists hold an opinion that those whom the society had rejected were usually computer freaks. The criminologists claim that the reasons for antisocial existence could be numerous: from physical disability or imperfection to ugliness. If this so, the deprivation of human contact caused people addicted to the computer as the unique way of self-esteem and self-expression. However, this is mostly a logical fallacy because a contradictory statement is false – not every physically challenged person can become a hacker.

Probably Western psychologists have approached to the truth closer than their colleagues from other regions. Among their patients there have been enough people who were not adapted to the reality, experiencing enormous difficulty in the sphere of communication with surrounding people and having an inadequate reaction to everything happening around them. In one word, these are individuals who look like mental degenerates capable of programming pretty well. Moreover, in many cases, such patients have autism usually diagnosed when people isolate themselves from the society and completely lose an ability to form emotional attachments as well as build any communication with people. In particular, the percentage of autism fluctuates from four to fifteen cases for every 10,000 children. Furthermore, the major part of those kids is boys. Statistically, the U.S. sociologists register more than 400,000 autistics, 80% of whose are a brilliant according to their IQ rate.

Why Hackers Commit Cyber Crimes

A hacker does not desire to cause harm to anyone. All he or she wants is to attract other people's attention, compensating a lack of communication. Such an unconscious impulse people can interpret as a commitment to revenge on humanity for ignorance and isolation, even though it is not always true. So, this aspect of a hacker's motive entirely coincides with the routine mentioned above activities' theory which provides

many examples of totally unsuspecting people who committed crimes due to their insult and desire to revenge for it [11].

Of course, not all hackers are social outcasts. Some of them dream about cracking the Pentagon defenses in high school on a dare or due to the greatest interest and inquisitiveness. The mentioned above Leaning Theory indicates three core values of any hacker – technology, secrecy, and mystery. Every hacker cannot imagine his life without technology. He always tries to get to the bottom of everything, demonstrating a level of qualification in front of so-called «colleagues' [7].

White-Collar Crimes with regard of Strain and Space Transition Theories

One more impressive group of individuals regarding human nature, most at risk to commit digital and other crimes, are administrative professionals [7]. The computerization of working places fosters an interconnection between digital violations and those who perpetrates them. Very often state ministers have unlimited access to the internet on their totally outdated and decked out computers to facilitate their work. Moreover, white-collar workers' authorities are powerful enough to determine the fate of their fellow citizens.

Many theories have been analyzed to figure out the motives of state employees. Merton's Strain Theory resulted in providing the best clarification [7]. According to Merton, people who once enjoyed the financial success may commit crimes connected with fraud merely because they try to save and even increase their money [12]. Furthermore, reviewing the literature on the topic, we suddenly came across the Space-Transition Theory, promoted by Jaishankar in 2007 [13], which still require some more tests and research works. Nevertheless, this approach has a complicated explanation why a person behaves differently migrating from one environment to another. In particular, an ordinary person, who suddenly gets the position which allows deciding for or against other people, would probably use the cyberspace as a way to prove his dominant role. Furthermore, individuals, whose primary task is «to repress criminal behavior in reality tend to commit a crime in virtual space, which, otherwise, they would not engage in physical space, due to their status and position» [13].

Conclusion

To sum up, the human's brain is a complex organism, consisted of a lot of different neurons that hardly ever understand each other. As a result, the consciousness is a tip of the iceberg because the biggest part of thinking flows unconsciously. Therefore, the motives of many actions have been still a mystery. However, our attempt to connect the crime theories with the reasons why people become digital criminals let us hope that we succeeded in clarifying perhaps, the most unusual cases.

References

1. Cybercrime: Security & Surveillance. Retrieved 2016, from [Электронный ресурс]. – Режим доступа: https://cdt.org/insight/cybercrime/, 2011

2. Howitt, D. Community Theory. Legal and Criminological Psychology. – №14 (1). – P. 183–183. – doi:10.1348/135532508x377128, 2009

3. McGuire W.J. A Perspective Approach to Theory Construction. Personality and Social Psychology Review. – №8 (2). – P. 173–182. – doi:10.1207/s15327957pspr0802_11, 2004

4. Cohen L.E. Social change and crime rate trends: A routine activity approach / L.E. Cohen, M. Felson // American Sociological Review. – 1979. – №44. – P. 588–608.

5. Agnew R. Strain Theory. Encyclopedia of Social Problems. – doi:10.4135/9781412963930.n550

6. Karl Marx. Political Theorists in Context. – P. 217–236. – doi:10.4324/9780203402276_chapter_9

7. Taylor R.W. Digital crime and digital terrorism (3rd edition). Upper Saddle River, NJ: Pearson/Prentice Hall, 2006.

8. Kirwan G. Can Theories of Crime be applied to Cybercriminal Acts? In G. Kirwan, A. Power (Eds.) the Psychology of Cyber Crime: Concepts and Principles (P. 37–51). Hershey, PA: Information Science Reference. – doi:10.4018/978–1-61350–350–8. ch003, 2012

9. Leukfeldt E.R. Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis / E.R. Leukfeldt, M. Yar // Deviant Behavior. – №37 (3). – P. 263–280. – doi:10.1080/01639625.2015.1012409, 2016

10. Hawley A. Human Ecology: A Theory of Community Structure. – New York: Ronald Press, 1950.

11. Clarke R.V. «Situational» Crime Prevention: Theory and Practice. British Journal of Criminology, Delinquency and Deviant Social Behavior. – 1980. – №20. – P. 136–147.

12. Merton. General Strain Theory. Springer Reference. – doi: 10.1007/springer-reference_223303

13. Jaishankar K. Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology. – 2007. – №1. – P. 7–9.

Ибраева Баян Мукушевна – канд. филол. наук, профессор, заведующая кафедрой ЧУ Академия «Болашак», Республика Казахстан, Караганда.

Ibraeva Bayan Mukushevna – candidate of philological sciences, full professor, head of department PI «Bolashak» academy, Republic of Kazakhstan, Karaganda.
