SOCIALIZATION & HUMAN DEVELOPMENT
International Scientific Journal

Review Article

UDK 159.922.8+159.923(=053.67)

PSYCHOLOGY OF DEVIANT FORMS OF ECONOMIC PERSONAL BEHAVIOR IN CYBERSPACE

Koval Hanna

Abstract

The goal of the research achieved by the author is the analysis of psychological features of deviant forms of economic behavior of an individual in cyberspace.

Methodology. To implement the problematic completeness of the research and obtain scientifically based and reliable results and general conclusions, a complex of theoretical methods was used: synthesis, logic and structure of the presentation, analysis and generalization, tools of scientific source studies. Linguistic methodology and the method of cognition were used to study the problematic issues of this work in the unity of their visual and factual perception, social content, legal and terminological form of representation. The systemic-structural approach made it possible to conceptually form, implement the theoretical foundations and model the complexity of the research discourse.

Results. It is shown that human crime and delinquency are related to both external factors (interaction with other types of crime, age, gender, material values, influence of peers) and internal factors that mediate criminal tendencies. It was concluded that the specifics of deviant forms of individual economic behavior in cyberspace have not yet been sufficiently studied, and attention is focused on more common types of cyber deviance. Instead, the actual problems are the peculiarities of the formation of economic cyber deviance; the detection of a tendency to this type of behavior; planning correctional and educational psychological work with deviants and victims of economic cybercrimes. An important problem is the difficulty of conducting research taking into account the key feature of cyberspace - anonymity.

Keywords*: cybercrime; fight against cybercrime, security; cyber deviance; online victimization.*

Relevance

Cybercrime is an inevitable companion of the globalization of information processes, a threat to the socio-humanitarian component of society's life. Cybercrimes are the most dynamic group of socially dangerous acts, as they become more common and dangerous every year. The growing number of cybercrimes in institutions and organizations, the continuous development of information technologies and new opportunities for "improving" the tools of their commission create economic threats to global information networks (Singh, Silakari, 2022).

Due to its anti-social nature and hidden identity, this type of crime has been convenient and easy for criminals, fraudsters, criminals and just network bullies from the very beginning. In addition to informational and psychological imbalance, which usually become a logical consequence of cyber violations, it makes sense to actualize the economic benefit/harm from such actions. After all, especially often such crimes in the space of network culture are committed with the pragmatic motive of illegal enrichment (Matveev, Nykytchenko, Stefanova, Khrypko, Ishchuk, Pasko, 2021).

The purpose of the study: to consider the psychological features of deviant forms of economic behavior of an individual in cyberspace.

Methodology

To implement the problematic completeness of the research and obtain scientifically based and reliable results and generally significant conclusions, the work uses a classic set of philosophical and worldview, general scientific methods: synthesis, logic and structure of the presentation, analysis and generalization of the problems of scientific sources.

Linguistic methodology and the method of cognition were used to study the problematic issues of this work in the unity of their visual and factual perception, social content, legal and terminological form of representation.

The systemic-structural approach made it possible to conceptually form, implement the theoretical foundations and model the complexity of the research discourse.

Results

A particular category of deviance that is becoming more common nowadays is cyber deviance, which is classified as a harmful activity that occurs in the digital realm (Jewkes, Yar, 2013; Graham, Smith, 2019; Yar, Steinmetz, 2019). It refers to cases of harmful behavior that are connected in one way or another to the computer and provoke a strong reaction from the media, politicians, academics and the public. This interpretation outlines two main characteristics of cybercrime, namely: the electronic environment and the impact associated with increased concern about cyber security.

The growth of cybercrime is due to the transformation of socio-economic systems, the transition to the digital economy and the virtual environment. There are three main groups of cybercriminals:

1. Cybercriminals who carry out criminal activities exclusively in cyberspace. Criminal groups formed under conditions of criminalization of cyberspace. Without criminogenic factors, such persons are less of a public danger than real criminals.

2. Cybercriminals who carry out criminal activities such as in cyberspace as well as in real life. Their psychology is generally criminal. However, the impact of the criminalization of cyberspace is negligible.

3. Persons who previously committed crimes not related to cyberspace, but subsequently committed cybercrimes. This group is formed by organized criminal communities that use the opportunities provided by the Internet. Advanced organizational

skills help such cyber criminals to use people with special knowledge to commit crimes. Their main efforts are aimed at maximizing profits and increasing their influence (Duff, 2008).

Depending on the motivation of criminal behavior, the following types of cybercriminals are distinguished.

- Type of interest: crimes aimed at obtaining specific items of value in cyberspace, for example, game items for their further sale.

- Bullying type: cyberbullying and cyberstalking. Crimes are characterized by threats of murder, suicide; possibly with elements of blackmail for not publishing certain personal content.

- Sexual type: characterized by the illegal distribution of pornographic materials for profit.

- Socially disorganizing type: crimes that violate social norms,
provided for by law and have a destructive effect on society.

- Ideologically or politically motivated type: a form of protest, political or ideological confrontation.

- Research type: the motivation of these crimes is the study of software and hardware components of electronic devices and their networks, the search for vulnerabilities, the possibility of their use and elimination.

Minors become victims of cybercriminals more often than adults. The most high-profile events related to cybercrime in recent years are the mass participation of teenagers in suicide groups. Group members receive a variety of self-harming tasks.

Psychological factors such as self-control, peer influence, materialistic values, impulsivity, and demographic factors such as age, gender, and education significantly independently and jointly predict Internet fraud trends among the youth. All variables jointly predict the tendency to commit Internet fraud. However, those young people who are more exposed to peer influence, prefer material values and are impulsive are more prone to online fraud.

Atwai & Holt, investigating the influence of peers on the behavior of Internet fraudsters, proved that communication with delinquent peers is an important factor in criminal behavior among young people (Atwai, 2011; Holt, 2011). A similar result was observed by Burton, Evans, Cullen & Olivares in the study of predictors of the reckless behavior of young people (Burton, Evans, Cullen, Olivares, 1999). The importance of their findings is that the older the youth, the more prone they are to online fraud.

Ideologically motivated economic criminals benefit from interactions with self-interested criminals and law-abiding actors who provide criminal resources in the form of knowledge, skills, and accomplices (Roberta, 2011). The reason for this is that the profile of economic offenders in cyberspace today is extremely diversified and it is becoming increasingly difficult to distinguish a common criminal from a typical economic offender such as an international terrorist or a domestic political extremist.

From a psychological point of view, the psychological explanation of crime can look as simple as "greed and dishonesty". Duffield & Grabosky point out that such an explanation is too simplistic (Duffield, Grabosky, 2001). According to them, not all dishonest people commit fraud.

Discussion

Until now, no scientist has been able to provide a psychological characteristic that serves as a valid and reliable marker, indicator, symbol or sign of an individual's propensity to commit fraud and cyberspace. As a result, there are numerous examples of attempts to distinguish between people who will commit fraud, or who are likely to commit fraud given the situation, from those who will not.

The main conclusions from the analysis of various risk factors for the economic form of cyber deviance turned out to be threefold.

First, online routines and activities play a significant role in both the diversity of different types of deviant behavior in cyberspace and polyvictimization. The theoretical premises of the theory of routine activity agree well with the relevant statements. The more active an individual is in cyberspace, the more exposed they are to potential criminals and other dangers, and the more likely they are to become victims. These statements are consistent with most existing research on online victimization (Leukfeldt, Yar, 2016).

Second, offline victimization matters. Prior cybercrime is a risk factor for a wide range of online victimization as well as online polyvictimization. This further confirms and complements the results of previous studies, which note that online and offline victims are not the same entirely separate groups of victims, and the online environment has expanded the environment of victimization among those who are already victims in real life (Choi, 2019; Ioannou, 2018; Mitchell, 2011; Oksanen, Keipi, 2013).

Thus, the accumulation of negative experiences in both offline and online contexts is assumed, where a person is not protected, even if the offender is physically absent. Such findings still raise further questions. For example, why does past experience of violent victimization increase victimization risk for so many different types of online victimization and polyvictimization? Is it just the accumulation of all kinds of negative experiences? Looking for an answer to them requires further comprehensive research.

Third, different types of cybercrime have different risk factors. Although offline victimization increased the risk of online victimization, the role of various socioeconomic factors was different in some cases compared to the risk factors for many forms of offline victimization. For example, those with better financial status may be at greater risk in part because they tend to be more active internet users (Statistics Finland, 2018), and therefore potentially more accessible to a wider range of economic cybercriminals. At the same time, the problem may also be that they have a larger "attack surface" or, in other words, have more devices at their disposal.

Conclusions

The chosen issue is so broad that it requires an outline of key issues to clarify the root causes, features, and development of a personality prone to deviant forms of economic behavior in cyberspace. It is appropriate to determine to what extent these parameters depend on the country of residence, level of education, type of employment, presence of victim experience in real life. The conditions and features of the formation of economic cyber deviance require attention; detection of a tendency to this type of behavior; planning correctional and educational psychological work with deviants and victims of economic cybercrime. An important problem is the difficulty of conducting research when referring to various theories and taking into account the key feature of cyberspace - anonymity.

Since the issues of deviant and delinquent behavior are at the intersection of the scientific interests of psychology and criminology, cyber security, and IT, it should be taken into account when planning a study to meet the needs of all areas.

References

Addae, J. H., Sun, X., Towey, D., Radenkovic, M. (2019) Exploring user behavioral data for adaptive cybersecurity. // User Model User-Adap Inter.. №29 (3). pp. 701–750.

Ahram, T., Karwowski. W. (2019).Advances in Human Factors in Cybersecurity. In: AHFE: international conference on applied human factors and ergonomics. // Springer, Washington D. C. pp. 66–96.

Anderson, R. (2006). The economics of information security. // Science, №314 (5799). PP. 610–613.

Anderson, R. (2001). Why information security is hard-an economic perspective // Proceedings of the 17th Annual Computer Security Applications Conference,. PP. 358–365.

Atwai, A. (2011). Youth cybercrime influenced by peers youth today. University of Liverpool. URL: http: // www. youthtoday. org / viewarticle. cfm? article id=4859

Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., Wollinger, G. R. (2018). Cyber-dependent crime victimization: The same risk for everyone? // Cyberpsychology, Behavior, and Social Networking, №21 (2). pp. 84–90.

Branley, D. B., Covey, J. (2017). Is exposure to online content depicting risky behavior related to viewers own risky behavior offline? // Computers in Human Behavior, №75. pp. 283–287.

Burton, V. S. Jr., Evans, T. D., Cullen, G. T., Olivares, K. M. (1999). Age, self-control, operationalization theories and adult criminality.//Journal of' qualitative criminology, № 10.pp. 213–239.

Choi, K., Cho, S., Lee J. R. (2019). Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. // Computers in Human Behavior, №100. pp. 1–10.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. // Feminist Media Studies, №18 (4). pp. 609–625.

Duff, A. (2008).The Normative Crisis of the Information Society. // Cyberpsychology: Journal of psychosocial research on cyberspace, №2 (1).

Duffield, G., Grabosky, P. (2001). The psychology of fraud, trends and issues in crime and criminal justice. // Australian Institute of Criminology, № 199. pp. 1–6.

Farrington, D. P. (2017). Integrated developmental and life-course theories of offending. New York, NY: Transaction Publishers. 280 p.

Graham, R. S., Smith, S. K. (2019). Cybercrime and digital deviance. New York, NY: Taylor and Francis; Routledge. URL: https: // www. taylorfrancis. com / books / mono / 10.4324 / 9781351238090 / cybercrime-digital-deviance-roderick-graham-shawn-smith

Hargittai, E. (2010). Digital variation in internet skills and uses among members of the «Net Generation». // Sociological Inquiry, №80 (1). pp. 92–113.

Harris, B. A., Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. // The British Journal of Criminology, № 59 (3). pp. 530–550.

Holt, T. J. (2011). Low self-control, deviant peer associations, and juvenile cybercrime. // American journal of criminal justice, URL: News. msu. edu / medial... / 06 / 963e40c7–08ff – 411d-af1-fe7563496f89. pdf

Ioannou, M., Synnott, J., Reynolds, A., Pearson, J. (2018). A comparison of online and offline grooming characteristics: An application of the victim roles model. // Computers in Human Behavior, № 85. pp. 291–297.

Jewkes, Y., Yar, M. (2013). Handbook of internet crime. London; New York, NY: Taylor and Francis; Routledge. URL: https: // books. google. ro / books?

Leukfeldt, E. R., Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. // Deviant Behavior, №37 (3), pp. 263–280.

Maimon, D., Louderback, E. R. (2019). Cyber-Dependent Crimes: An interdisciplinary review. // Ann Rev Criminol. № 2 (1). pp. 191–216.

Matveev, V., Nykytchenko, N., Stefanova, N., Khrypko, S., Ishchuk, A., Pasko, K. (2021). Cybercrime in the economic space: psychological motivation and semantic-terminological specifics // International journal of computer science and network security, №21 (8). PP. 203–211.

Mitchell, K. J., Finkelhor, D., Wolak, J., Ybarra M. L., Turner H. (2011).Youth internet victimization in a broader victimization context. // Journal of Adolescent Health, №48 (2). pp. 128–134.

Niels, P., Mavrommatis, P., Abu Rajab, M., Monrose, F. (2008). «All Your iFRAMEs Point to Us. // Proceedings of the 17th USENIX security symposium, 2008. PP. 1–15.

Oksanen, A., Keipi, T. (2013).Young people as victims of crime on the internet: A population-based study in Finland. // Vulnerable Children and Youth Studies, №8 (4). pp. 298–309.

Payne, B. K., Hadzhidimova, L. (2018). Cyber security and criminal justice programs in the United States: Exploring the intersections. // Int J Crim Justice Sci. № 13 (2). pp. 385–404.

Pfleeger, S. L., Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. // Comput Secur. № 31 (4). pp. 597–611.

Reyns, B. W., Fisher B. S., Bossler, A. M., Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization? // American Journal of Criminal Justice, №44 (1). pp. 63–82.

Roberta, B. (2011). Where political extremists and greedy criminals meet: A comparative study of financial crimes and criminal networks in the United States. // In A dissertation submitted to the Graduate Faculty in Criminal Justice in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York. URL: https: // www. ojp. gov / pdffiles1 / nij / grants / 234524. pdf

Shulman, E. P., Steinberg, L. D., Piquero, A. R. (2013). The age-crime curve in adolescence and early adulthood is not due to age differences in economic status. J. // Youth Adolesc, № 42. PP. 848–860.

Singh, S., Silakari, S. (2022). A survey of cyber-attack detection systems. international // Journal of computer science and network security, № 5. PP. 1–10.

Statistics Finland. Use of information and communications technology by individuals. (2018). URL: http: // www. stat. fi / til / sutivi / 2018 / sutivi_2018_2018–12–04_tie_001_en. html. Accessed 10th of March 2020.

Tilley N., Tseloni, A., Farrell, G. (2011). Income disparities of burglary risk: Security availability during the crime drop. // The British Journal of Criminology, №51 (2). pp. 296–313.

Yar M., Steinmetz, K. F. (2019). Cybercrime and Society. Thousand Oaks, CA: SAGE Publications, 368 p.

AUTHORS INFORMATION

Koval Hanna

D. S. in Psychology, Associate Professor, Department of Differential and Special Psycholog, I.I. Mechnikov National University of Odesa, Ukraine

0000-0003-0291-7501aankova68@gmail.com

Competing interests: Any competing interests were declared by author.

Disclaimer: The author declares that her opinions and views expressed in this manuscript are free of any impact of any organizations.

ABOUT THIS ARTICLE

Cite this article

Koval Hanna PSYCHOLOGY OF DEVIANT FORMS OF ECONOMIC PERSONAL BEHAVIOR IN CYBERSPACE 2023 Socialization & Human Development journal 1. DOI 10.37096/SHDISJ-23-1.1-0007

Submitted on 30 Jun 2023 / Revised 10 Sep 2023 / Approved 1 Nov 2023

Published: **20 Nov 2023**

DOI: 10.37096/SHDISJ-23-1.1-0007

Managing editor - *Nataliia Dembytska*.

RIGHTS AND PERMISSIONS