PSYCHOLOGICAL ASPECTS OF CYBERCRIME PREVENTION

UDC: 004.056:[343.451+343.971]
DOI: https://doi.org/10.53486/tids2025.08

BARBĂNEAGRĂ OXANA
Academy of Economic Studies
oxana.barbaneagra@ase.md
ORCID ID: 0009-0008-2567-0170

Abstract. Cybercrime is any criminal activity using information devices and/or digital networks which exploit various information vulnerabilities, involving the criminal use of technologies, identity theft, data breaches, computer viruses, scams, and other malicious activities. A number of current publications demonstrate important psychological aspects that have become an integral part of cybercrime. The main goal of the research conducted is to determine the psychological mechanisms of cybercrime and use specific techniques to prevent it. The research was based on examining open Internet publications from experts and specialized companies. The study demonstrated that the basic psychological aspects of cybercrime are the primary motivations and psychological vulnerabilities of the victims. The first refers to the thirst for financial gain, the sense of power and control over victims, and ideological motivations. In their quest for illicit gains, cybercriminals typically target individuals and legal entities with valuable assets, using ransomware attacks, credit card theft, online banking fraud, large-scale money laundering operations, identity theft, phishing, and the creation of fraudulent websites. For some perpetrators, the feeling of power and control over their victims is important due to the anonymity offered by the online environment (which shields them from the fear of identification or retaliation) and the feeling of invincibility. Similarly, cyberbullying and online harassment can be used with the intention of hurting, humiliating or intimidating. Ideological motivations are related to political, extremist, or ethical hacking goals. In terms of victim vulnerability, we differentiate cybercrimes based on manipulation of human behavior, phishing attacks and deceptive techniques, exploiting cognitive biases, impulsiveness and the psychology of online addiction. This involves manipulative techniques with emotions such as fear, greed, curiosity, empathy, or excitement, as well as abuses based on trust and the building of false relationships. One of the solutions to the problems generated by cybercrime is the use of certain psychological techniques, which can be divided into three groups: deducing behavioral profile and risk assessment; undertaking awareness and education measures; carrying out psychological intervention and rehabilitation activities.

Keywords: psychology, cybercrime, motivation, technique, prevention.

JEL Classification: D91, G41, L86

INTRODUCTION

Cybercrime is a general term that is related to any illegal activity with the use of a computer, network, or digital device (Brush Kate, Cobb Michael, 2024), (Proofpoint).

The Council of Europe Convention on Cybercrime defines cybercrime "as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity, and availability and copyright infringements" (Brush Kate, Cobb Michael, 2024).

Cybercrimes have a certain diversity, with some specialists dividing their typology into the following categories (Brush Kate, Cobb Michael, 2024):

- Crimes in which the computing device is the target, whose purpose, for example, may be to gain access to the network;
- Crimes that use the computer as a weapon; for example, to carry out a denial-of-service attack;

- Crimes in which the computer is used as an accomplice; for example, when it comes to using it to store illegally obtained data.

Cybercrime can be further divided into four categories (Cybertalents):

1. *Individual cybercrimes*, which are related to the activity of individuals. Examples include phishing, spoofing, spam, cyberstalking, and others;

2. *Organizational cybercrime*, which primarily targets organizations and is usually committed by teams of criminals, including malware and denial of service attacks.

3. *Property cybercrimes*, which target property such as credit cards or intellectual property rights.

4. *Society cybercrimes* are the most dangerous form, as they include cyberterrorism.

The conducted research has uncovered important psychological aspects that can be considered as part of the motivation and mechanisms behind cybercrime.

In this context, expert Jonathan Reed (2025) states: "To truly understand cybersecurity is to understand the human mind — both as a weapon and as a shield. …At the core of every cyberattack is a human, driven not just by code but by complex motivations and psychological impulses. Cyber criminals aren't merely technologists. They are people with intentions, convictions, emotions and specific psychological profiles that drive their actions."

A cybercriminal is a person who applies their technological skills to carry out malicious acts and illegal activities in the form of cybercrimes. These criminals can be individuals or form teams (Cybertalents).

These criminals exploit security gaps and vulnerabilities discovered in cyber systems to gain entry into the target environment. These security breaches can take the form of weak authentication methods and passwords, but they can also arise from the lack or ineffectiveness of security models and policies (Cybertalents).

As expert Bhagat Singh Sharma (2023) states, cybercriminals are motivated by a variety of factors, such as financial gain, personal gratification, and even specific political or ideological beliefs. They also exhibit certain psychological traits, such as impulsivity, thrill-seeking, and lack of empathy, which can lead to a lack of concern for the consequences of their actions, including the harm they cause.

Understanding these psychological aspects of cybercrime can be an important component for developing preventive cybersecurity measures, which in turn can reduce the risk of individuals and companies becoming victims of cybercrime.

This article has two main purposes:

- To study the psychological aspects of cybercrime.
- To examine the analysis of behavioral patterns and address psychological issues in order to mitigate the risks associated with cybercrime.

MAIN CONTENT

1. Materials and Methods

The research was based on examining open Internet publications from experts and specialized companies. The conducted research has allowed us to outline the essence and basic psychological aspects of cybercrimes. Then, the psychological possibilities of developing strategies to identify cybercriminals and prevent their activity were studied. The research was completed by drawing up the related conclusions.

2. Results and Discussion

The first part of the study conducted was dedicated to examining the psychological aspects of cybercrimes.

Some experts say that one of the basic psychological foundations of cybercrime is the anonymity provided by activity in cyberspace, which can encourage some individuals to commit crimes that they would not dare in the physical world. Cybercriminals often assume that they can more easily avoid punishment for breaking the law online (Loughtec, 2024).

The expert Jonathan Reed (2025) states: "Many cyber criminals share distinct personality traits: an inclination for risk-taking, problem-solving prowess and an indifference to ethical boundaries. Furthermore, the physical and digital distance inherent in online crime can create a psychological disconnect, minimizing the moral weight of their actions. This environment enables cyber criminals to justify their behavior in ways they might not if they had to face their victims in person."

Opportunistic behavior is also possible. That is, in some cases cybercriminals take advantage of vulnerabilities and weaknesses in software, hardware, or networks without having a specific motive, but with the intention of exploiting the weaknesses for personal gain (Loughtec, 2024).

From a criminological perspective, the following theories can be highlighted to explain the motivation of cybercrimes (*Criminological…*, n.d.):

1. *Rational choice theory*. Individuals engage in cybercrime under the influence of the belief that it is a profitable and low-risk activity. That is, their actions are the result of weighing the potential benefits of committing the crime against the potential risks of being discovered and punished.

2. *Social learning theory*. Criminal behavior by some individuals is the result of observing the behavior of others, especially those close to them. It may also be influenced by the media's portrayal of hackers as charming and successful.

3. *Strain theory*. Individuals may engage in cybercrime when they are dealing with tensions or pressures in their lives, such as economic problems or social exclusion. In this case, criminal activities may become a way to relieve stress or gain a sense of power and control.

4. *Routine activities theory*. Cybercrimes can occur when three factors converge: a motivated perpetrator, a suitable target (e.g., a vulnerable computer system), and the absence of capable protectors (e.g., lack of effective cybersecurity measures).

5. *Self-control theory*. Individuals who commit cybercrimes often have low levels of self-control. This means that many of them are prone to acting impulsively and making decisions without considering the consequences.

Some experts have examined the psychological motivations of cybercriminals (Figure 1) **(**The Hackers Meetup, 2024), (Coretech, 2022), (Loughtec, 2024):

Figure 1. The main psychological motivations of cybercrimes

Sources: (The Hackers Meetup, 2024), (Coretech, 2022), (Loughtec, 2024)

➢ *Financial gain*. According to many experts, financial gain (obtaining economic profits) is the main motivation of cybercriminals, the difference being the methods of obtaining the funds.

This can include:

- Direct access to a bank or investment account, stealing the password of a financial site followed by transferring the assets to one of the criminals;
- Swindling an employee into making a money transfer using a specific technique;
- Carrying out a ransomware attack on the entire organization.

With the stated goal in mind, cybercriminals typically target individuals and businesses with valuable assets, carrying out ransomware attacks, credit card theft, online banking fraud, large-scale money laundering operations, identity theft, phishing, and the creation of fraudulent websites. Cybercriminals may also target an individual's private information or corporate data for theft and resale.

➢ *Recognition and achievement*. Some criminals are motivated by the sense of accomplishment (self-affirmation) that can come with breaking into an important system.

They may operate in groups or independently, but to some extent they crave recognition. By nature, most cybercriminals are competitive and love the challenge that their actions bring. They often encourage each other to carry out sophisticated cyberattacks.

➢ *The feeling of power and control over victims*. For some perpetrators, the feeling of power and control over their victims is important due to the anonymity offered by the online environment and the illusion of invincibility. Cyberbullying is often carried out with the intention of hurting, humiliating or intimidating.

➢ *Ideological motivations*. In this case, it is cybercrime committed with political, extremist, or ethical hacking goals. Typically, these crimes are organized by criminal groups that target entities that challenge their worldviews, often focusing on religious beliefs or geopolitical conflicts.

Cyberterrorism involves the use of technology to cripple a nation’s infrastructure or disrupt critical services. Driven by political or ideological agendas, cyberterrorists may launch attacks on government agencies, financial systems, or vital utilities to create chaos and instill fear.

Extremist groups use information technologies to impose and spread their ideology, recruit members, and conduct propaganda campaigns. Cyberspace has become a global terrain for these groups to radicalize individuals and incite violence.

A specific form of cybercrime committed under the impact of ideological factors is *ethical hacking*, also known as *hacktivism*, related to unauthorized access to computer systems with the intention of promoting social or political change.

Although criminals believe their motives are noble, the illegal methods used can cause substantial damage and create ethical issues.

Some cybercriminal groups use their hacking skills to attack large organizations. The motives are usually related to a cause, such as respecting human rights or alerting a large corporation to vulnerabilities in their system. They may also target groups whose ideologies do not align with their own. These groups may steal information and claim to practice free speech, but more often than not, these groups carry out DDoS (Distributed Denial of Service) attacks to overload a website with too much traffic and cause it to crash.

➢ *Patriotic considerations*. Patriotic sentiments are sometimes supported by funding and assistance from a particular state. “Patriots” use cybercrime methods to advance their nation’s own interests. Typically, this involves stealing information (including intellectual property), personally

identifiable information, and money to fund or advance espionage and exploitation causes. In this case, state-sponsored actors carry out malicious cyberattacks and claim that their cyberespionage activities are legitimate activities on behalf of the state.

➢ *Exploiting vulnerabilities*. This includes cybercrimes based on the manipulation of human behavior, phishing attacks and deception techniques, exploiting cognitive biases, impulsivity and the psychology of online addiction. In most cases, the addictive nature of the digital world and inherent human impulsivity are exploited. The Internet in the modern world offers instant gratification and escape from reality, leading to the development of online addictions. Individuals with a propensity for addiction may engage in cybercrime as a means of fueling their compulsive behaviors.

Some experts point to *the exploitation of the human factor through social engineering* (Reed, 2025).

As Jonathan Reed (2025) notes, the vulnerability of the human mind is one of the most powerful weapons in a cybercriminal's arsenal. Social engineering attacks, such as phishing, exploit non-technological human factors such as trust, fear, urgency, and curiosity, which have become alarmingly effective. A Verizon report notes that the human element was included in 68% of data breaches, highlighting the vulnerability of human interactions.

Phishing attacks focus on creating a sense of urgency, fear, or curiosity. Attackers manipulate users of information products into clicking on malicious links or revealing sensitive information. The success of these attacks depends on creating an illusion of trust and authority, taking advantage of innate human tendencies.

Impulsivity plays an important role in the conduct of cybercrime, as impulsive individuals are more likely to engage in risky behaviors without considering the potential consequences. Cybercriminals capitalize on impulsive behavior to exploit victims and gain unauthorized access to sensitive information. To do this, they use techniques of manipulating emotions such as fear, greed, curiosity, empathy or enthusiasm, as well as abuses based on trust and building false relationships.

Expert Nilesh Roy (2024) focuses attention on the psychological features of cybercrimes:

➢ *Cognitive biases and decision making* are systematic patterns of deviation from the norm or rationality in judgment (reasoning), which can affect both attackers and defenders. They can take the form of confirmation bias and risk assessment bias.

Confirmation biases occur in attackers, when they fall victim to biases manifested only by seeking information confirming pre-existing beliefs, which can lead them to underestimate a target's defenses or to ignore the potential consequences of their actions.

Risk assessment biases occur in both attackers and defenders, who may misjudge risks due to optimism (underestimating the possibility of negative outcomes) and anchoring (overly relying on the first piece of information encountered). These biases can lead to overconfidence in security measures or underestimating the capabilities of an attacker.

➢ *Social engineering* uses human psychology to gain unauthorized access to systems or information and can take one of the following forms:

– *Psychological manipulation* relies on exploiting victims' emotions, such as fear, greed, or curiosity. For example, by crafting persuasive messages, victims are persuaded to reveal sensitive information or click on malicious links;

– *The impact of social dynamics* by appealing to the perceived authority of the sender, the urgency of the message, or the familiarity of the source, to increase the effectiveness of the attacks.

➢ *Stress* can significantly influence decision-making, especially in high-stakes situations, such as responding to a cyber incident. This influence is twofold:

– *The impact on defenders* is manifested by the pressure on cybersecurity professionals, especially during active incidents. Stress can impair judgment, leading to hasty decisions that may not be optimal;

– *The impact on attackers* is exerted when engaging in prolonged or complex activities. Stress can lead to mistakes or deviations from the preliminary plan, which defenders can uncover if they are vigilant and adaptable.

The second part of the study focused on examining the importance of understanding the psychological aspects of cybercrime for developing effective prevention strategies.

By analyzing behavioral patterns and addressing psychological issues, proactive measures can be taken to mitigate the risks associated with cybercrime **(**The Hackers Meetup, 2024):

- Behavioral profiling and psychological risk assessment;
- Education and awareness;
- Psychological interventions and rehabilitation.

Behavioral profiling and psychological risk assessment tools are designed to assist in identifying potential cybercriminals and preventing their actions.

Authors Kitty Kioskli and Nineta Polemi (2020) report the following: "Psychological profiling (or just 'profiling') is broadly defined as the various techniques of identifying and analyzing behaviors performed in a crime. …Profiling assists the investigation by either selecting the offender from a pool of suspects or by providing the offender's description for future identification."

Psychological profiling involves examining the psychological factors that drive individuals to commit criminal acts. It aims to understand the complex motivations, personality traits, and behavioral patterns that contribute to a person becoming a cybercriminal. Psychological profiling draws on principles from psychology, criminology, and behavioral science to profile potential criminals and understand their actions in the digital realm. An important aspect of psychological profiling is examining the personality traits associated with cybercriminals. Research has identified traits such as narcissism, Machiavellianism, and psychopathy as prevalent among individuals involved in cybercrime. These traits can manifest themselves in actions such as manipulation, lack of empathy, and risk-taking, which are typical of participating in criminal cyber activities (Reynolds, 2024).

A psychological risk assessment is a tool designed to identify potential dangers and risks to the mental health and well-being of individuals and to take measures to minimize or eliminate them (Weidl, 2023).

In this context The Hackers Meetup (2024) mentions the following:

1. *Identifying potential cybercriminals*. Analyzing behavioral patterns (e.g., online activities, communication style, and history of previous cybercrime) can help experts detect individuals with a heightened propensity to engage in cybercriminal activities.

2. *Analyzing behavioral patterns*. Behavioral patterns can reveal clues to potential cyberbullying. They include excessive secrecy, exaggerated online activity, and a tendency to exploit or manipulate others.

3. *Assessing risk factors for cybercrimes*. Assessing risk factors related to a person's use of information technologies, personal and social circumstances, and motivations, contributes to understanding the likelihood of this individual's involvement in cybercrime and developing related prevention strategies.

In this context, we can talk about a special field of research known as *cyber forensic psychology* related to the application of psychological principles and techniques in the investigation of cybercrimes, which is extremely important for understanding the behaviors and motives of attackers, as well as for developing effective investigative strategies (Roy, 2024).

User behavior analytics has become an intersection of information technology and psychology. By analyzing behavioral patterns and detecting deviations, organizations can proactively identify potential threats. This approach is based on the principle that individuals, even in the digital environment, follow predictable patterns. Behavioral analytics can uncover abnormal behaviors, such as an unexpected attempt to access restricted files or logins at unusual times, signaling a potential security breach. The combination of psychology and technology allows for dynamic and adaptive security measures that detect threats early, even before they escalate into full-blown incidents (Reed, 2025).

Enhancing psychological education and promoting awareness about safe digital behavior are basic elements in preventing cybercrime.

These activities refer to the specific field called *cybersecurity psychology* which examines how people perceive, interact with, and respond to cyber threats, with the aim of researching the thought processes that guide their actions (Anders, 2023).

In other words, cyber psychology is the study of the psychological aspects of the interaction of human thought with information technology, with an emphasis on the Internet and digital environments. This field investigates how psychological principles influence both attackers and defenders (Roy, 2024).

In this area the complex of activities may contain (The Hackers Meetup, 2024):

1. *Psychological education for safer cyber behaviors*. By educating individuals about the psychological techniques used by cybercriminals, they become able to recognize and resist manipulation attempts. Promoting critical thinking skills and digital literacy can help individuals be informed, make informed decisions, and identify potential threats.

2. *Enhancing digital literacy*. Digital literacy programs aim to improve knowledge about online security, privacy protection, and responsible digital citizenship. Informing individuals about the risks of cybercrime allows them to take proactive steps to protect their online activity.

3. *Cybersecurity awareness programs in institutions* can help educate interested individuals about best practices, potential risks, and the importance of maintaining a secure online environment.

Psychological interventions and rehabilitation programs are designed to address the issues contributing to cybercrime, assisting individuals in the rehabilitation process and preventing relapse by:

1. *Understanding rehabilitation methods* focus on examining the psychological, behavioral, and social factors that determine a person's involvement in cybercrime, including therapy, counseling, skills development programs, and support networks geared toward positive behavior change.

2. *Addressing underlying psychological issues*. Many cybercriminals have specific psychological issues, such as low self-esteem, trauma, or feelings of helplessness. Psychological interventions aim to identify and address these issues, helping individuals develop healthier coping mechanisms and reducing the likelihood of recidivism.

3. *The role of therapy in cybercrime prevention*. Therapy plays an important role in preventing cybercrime by examining the root causes of criminal behavior. Individual and group therapy sessions can form a supportive environment in which individuals can vent their emotions, gain perspective on their actions, and develop strategies for better decision-making.

Jonathan Reed (2025) mentions the mental strength of cyber professionals.

Protecting against cyber threats, along with technical skills, requires resilience, ethical conviction, and a deep understanding of human behavior. Cyber professionals face constant psychological pressure, and mental resilience allows them to quickly plug gaps, restore security, and learn from incidents.

Creativity and adaptability are also mandatory for cybersecurity. As cybercriminals constantly refine their tactics, security professionals are forced to anticipate these moves and must innovate by developing new countermeasures before an attack occurs.

The aforementioned author also mentions the importance of ethics by virtue of the fact that cybersecurity professionals have access to sensitive data and important tools. In case of their improper use or negligence, substantial damage becomes possible. Implementing a solid code of ethics can create a psychological anchor, helping professionals navigate the moral complexities of their work, respecting the privacy and security of users.

Of great importance is the promotion of a *psychologically sound cybersecurity strategy*. An effective cybersecurity strategy is not only about blocking attacks, but also about adapting to human behavior. Therefore, security measures must be tailored to natural human tendencies. This will work best if users adhere to comprehensive security protocols (Reed, 2025).

Promoting a culture of psychological safety within a company can also encourage employees to be open to security concerns. When employees can freely discuss potential threats and even mistakes, they are able to identify risks early and a collective commitment to cybersecurity is formed within the company.

CONCLUSIONS

The conducted research has demonstrated that cybersecurity is not just a technical issue, but has fundamental human aspects. Psychology's role in cybersecurity is currently very broad, encompassing user behavior as well as attacker prediction and profiling. Its goal is to understand the goals, cognitive patterns, and emotional factors that drive cybercriminals to take action to combat and prevent cybercrime. The psychology of cybercriminals is complex, demonstrating a high adaptability to new technologies, the ability to use multiple tools and techniques to exploit weaknesses in software, networks, and human psychology. And the psychological motivation for illegal behavior is very diverse. Simultaneously, international practice has developed effective techniques designed to help prevent cybercrime. Modern cybersecurity strategies must combine technology and psychology to form effective protection that takes into account both the technical vulnerabilities of the system and human behavior. Combating cyber threats by professionals relies on their mental toughness, creativity, and ethical strength. Implementing behavioral analytics, incorporating the human perspective into cybersecurity strategies, and launching training programs based on psychological principles contribute to the formation of a more adaptive and robust defense system.

REFERENCES

1. Anders Larkin, 2023. The Importance of Teaching Cybersecurity Psychology to Employees. Available at: https://www.hooksecurity.co/blog/importance-of-teaching-cybersecurity-psychology. [Accessed 16.05.2025]
2. Brush Kate, Cobb Michael, 2024. What is cybercrime and how can you prevent it?. Available at: https://www.techtarget.com/searchsecurity/definition/cybercrime#:~:text=Cybercrime%20is%20any%20criminal%20activity,directly%20damage%20or%20disable%20them. [Accessed 10.05.2025]

3. Coretech, 2022. 6 Motivations of Cyber Criminals. Available at: https://www.coretech.us/blog/6-motivations-of-cyber-criminals. [Accessed 12.05.2025]
4. Criminological Explanations of Cybercrime. Available at: https://cod.pressbooks.pub/crimj1165/chapter/module-3/ [Accessed 14.05.2025]
5. Cybertalents. *What is Cybercrime? Types, Examples, and Prevention*. Available at: https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention [Accessed 12.05.2025]
6. Kioskli Kitty, Polemi Nineta, 2020. Available at: A Socio-Technical Approach to Cyber-Risk Assessment. https://core.ac.uk/download/586551524.pdf. [Accessed 15.05.2025]
7. Loughtec, 2024. Exploring the motives behind cybercrime. Available at: https://www.loughtec.com/exploring-the-motives-behind-cybercrime. [Accessed 13.05.2025]
8. Proofpoint. *What Is Cyber Crime?*. Available at: https://www.proofpoint.com/au/threat-reference/cyber-crime [Accessed 12.05.2025]
9. Reed Jonathan, 2025. *Hacking the mind: Why psychology matters to cybersecurity*. Available at: https://www.ibm.com/think/insights/hacking-the-mind-why-psychology-matters-to-cybersecurity [Accessed 08.04.2025].
10. Reynolds, A'shya Latrice, 2024. *Profiling Cybercriminals: Behavioral Analysis and Motivations Behind*
11. *Cybercrime Activities*. Available at: https://digitalcommons.odu.edu/cgi/viewcontent.cgi?params=/context/covacci-undergraduateresearch/article/1094/&path_info=COVA_Research_Paper____Profiling_Cybercriminals__Behavioral_Analysis_and_Motivations_Behind_Cybercrime_Activities.____3_.pdf. [Accessed 24.05.2025]
12. Roy Nilesh, 2024. *Cyber Psychology in CyberSecurity: A Comprehensive Analysis*. Available at: https://www.linkedin.com/pulse/cyber-psychology-cybersecurity-comprehensive-analysis-roy--5x5ac#:~:text=Cyber%20psychology%20is%20the%20study,influence%20both%20attackers%20and%20defenders. [Accessed 10.04.2025].
13. Sharma Bhagat Singh, 2023. *The psychology of cybercriminals: understanding the mind of a hacker*. Available at: https://www.linkedin.com/pulse/psychology-cybercriminals-understanding-mind-hacker-sharma [Accessed 10.04.2025].
14. The Hackers Meetup, 2024. *Understanding the Psychology Behind Cyber Crimes*. Available at: https://thehackersmeetup.medium.com/understanding-the-psychology-behind-cyber-crimes-235ab3360078 [Accessed 08.04.2025].
15. Weidl Christof, 2023. What to *Consider in a Psychological Risk Assessment, Who Should Conduct It, What it Brings, and Best*. Available at: https://www.lemin.ai/en/post/what-to-consider-in-a-psychological-risk-assessment-who-should-conduct-it-what-it-brings-and-best#:~:text=A%20psychological%20risk%20assessment%20(PBG)%20is%20an%20important%20tool%20for,to%20minimize%20or%20eliminate%20them. [Accessed 14.05.2025].