Psychological Manipulation Techniques in Cybercrime and Its Prevention Strategies

Yujia Li
School of Civil and Commercial Law, Southwest University of Political Science and Law, Chongqing, China

Keywords: Psychological Manipulation Techniques, Cybercrime, Prevention Strategies.

Abstract: In the field of cybercrime, "psychological manipulation technique" is the means that criminals pre-fer to use. It relies on the anonymity of the network environment and a wide range of information diffusion ability, the use of human weakness to carry out fraud, extortion and other criminal behaviour, the personal safety of individuals and social order caused a great threat. This project takes the psychological manipulation technology of cybercrime as the research object, through literature analysis, case analysis and other research methods, conducts in-depth research on the psychological manipulation technology of cybercrime, analyzes its application in various types of cybercrime, and reveals its difficulties and hazards in dealing with it. Then, countermeasures are formulated from the aspects of building a new firewall, three-dimensional innovation of judicial mechanism, establishment of cooperative governance system, improvement of technology and preventive measures, hoping to effectively prevent psychological manipulation technology in cybercrimes.

1 INTRODUCTION

1.1 Research Background and Significance

The psychological manipulation technique in cybercrime refers to that in virtual space, criminals induce the victims to produce wrong cognition or emotional response through elaborate psychological strategies and then carry out the criminal behavior. This technique is extremely covert and efficient. The background and significance of studying this technology is that on the one hand, it can help individuals crack the cognitive vulnerability, enable the public to independently identify the psychological manipulation logic of criminals, and build a cognitive immune system to resist this manipulation. On the other hand, it can help maintain social security and rebuild social trust. In addition, it can promote the interdisciplinary integration of law, psychology and other disciplines. The law will usher in a revolution. The traditional criminal law focuses on "behavior and result", while the research on psychological manipulation will promote "cognitive autonomy" as a new legal interest. In the application of psychology, the relevant defense strategies are directly transformed from some classical theories of Asch's conformity experiment and Mil-gram's obedience experiment, which will have practical value. In a word, in-depth study of psychological manipulation techniques in cybercrime is not only an urgent need to deal with real threats, but also an important measure to promote social progress (Zheng, 2024).

1.2 Overview of Research Status at Home and Abroad

Psychological manipulation techniques in cybercrime have been a hot issue that has attracted much attention in recent years. Scholars at home and abroad have carried out in-depth research on it from many angles such as psychology and criminology. Foreign research started earlier, especially in Europe and the United States, aiming at Internet fraud, social engineering attacks and other behaviors, put forward the theory of "social engineering", emphasizing how criminals exploit human psychological weaknesses (such as trust, fear, greed) to manipulate. Studies have shown that attackers can break through victims' psychological defenses in an average of 7 minutes by constructing false identities and faking urgent situations (Hadnett, 2021). For example, according to the Federal Bureau of Investigation (FBI), the economic loss of online fraud in 2022 exceeded $10 billion, with the majority of cases involving

Li, Y.
Psychological Manipulation Techniques in Cybercrime and Its Prevention Strategies.
DOI: 10.5220/0014393700004859

In *Proceedings of the 1st International Conference on Politics, Law, and Social Science (ICPLSS 2025)*, pages 593-599
ISBN: 978-989-758-785-6

psychological manipulation techniques, such as impersonating an authority to induce victims to transfer money. Recent empirical research further reveals that 73% of successful online scams involve emotional manipulation, specifically targeted attacks on loneliness and empathy (Sasse et al., 2022).

However, domestic research is more combined with localized cases, focusing on new fraud methods, such as "killing pig plates" and fake investment (Qin, 2024). A study by the Institute of Psychology of the Chinese Academy of Sciences shows that through emotional manipulation and false promises, criminals make their victims become so dependent in a short period of time that they lose their rational judgment. Overall, domestic and international research shows that the core of psychological manipulation techniques is to exploit human weaknesses, and the anonymity of the online environment and the speed of information dissemination further magnifies this harm.

1.3 Research Methods and Innovations

Combining theory and practice, this paper comprehensively discusses the operation mechanism and prevention strategy of psychological manipulation technology in cybercrime. This paper uses literature analysis to sort out the research results on cybercrime and psychological manipulation and summarizes the shortcomings and research gaps of existing theories. Using the case study method, the typical cybercrime cases in recent years (such as "killing pig plate", impersonating public security law fraud, etc.) are selected, and the psychological manipulation methods of criminals and their effects on different groups are deeply analyzed. The innovation points are mainly reflected in the following aspects: First, interdisciplinary, not limited to the field of law, but the deep integration of law and psychology. Second, it is old and new, and puts forward some innovative solutions, such as the establishment of cognitive speed bumps based on psychological principles and the empowerment of authority with science and technology.

2 PSYCHOLOGICAL MANIPULATION TECHNOLOGY IN CYBERCRIME

2.1 Psychological Manipulation Techniques Embody the Subjective Aspects of Crime

Criminal responsibility shall be borne for intentional crimes. The use of psychological manipulation technology in cybercrime not only reflects the technical ability of the perpetrator, but also reflects the intention or negligence of the subjective aspect. According to Article 14 of the Criminal Law of the People's Republic of China, an intentional crime is committed when a person knows that his or her actions will cause social harm and hopes or allows such results to occur, thus constituting a crime. And Article 15. A person who should have foreseen that his conduct might have consequences harmful to society, but failed to do so because of his negligence, or believed that such consequences could have been avoided because he had foreseen them, shall constitute a crime of negligence. Criminal responsibility for a negligent crime shall be borne only if it is prescribed by law. 14. According to this, the subjective aspects of crime include intent and negligence. In cybercrimes, the subjective aspect is usually intentional, especially in cases involving psychological manipulation techniques, where the perpetrator's subjective malice is more obvious. The intention of crime is composed of two factors: the cognitive factor (knowing) + they will factor (therefore committing).

2.1.1 Psychological Manipulation Technique Reflects the Intention of the Perpetrator

The actor must have certain professional knowledge to use psychological manipulation techniques. The behavior-result chain is as follows: the perpetrator carefully designs the psychological strategy -- the victim is induced to have false cognition -- the perpetrator uses this to commit the crime. In this process, the actor knows that his behavior is illegal and hopes or allows the harmful result to occur. For example, in a "phishing attack", the perpetrator creates a fake email or website address to trick the victim into clicking on it, providing their personal information or transferring money directly. This

behavior is a direct manifestation of the perpetrator's intent.

2.1.2 Psychological Manipulation Techniques Reflect the Illegal Purpose of the Actor

The perpetrator uses psychological manipulation technology in the process of cybercrime, usually to achieve the purpose of illegal possession, destruction, interference and so on. In addition to the well-known illegal acquisition of property, there are other illegal purposes. For example, in a social engineering attack, the perpetrator poses as a trusted third party in order to gain the victim's trust and gain access to confidential information. The perpetrator has a clear illegal purpose in the process of carrying out the psychological manipulation technique, which conforms to the subjective component of the crime.

2.1.3 Psychological Manipulation Techniques Enhance the Subjective Malignancy of Behavior

The use of psychological manipulation techniques not only reflects the intention of the actor but also enhances the subjective malignancy of the behavior. The perpetrator implements psychological manipulation technology and makes full use of the needs and psychological weaknesses of the victims to carry out network crimes. This behavior has a high concealment and causes greater psychological harm to the victims. Therefore, in judicial practice, the use of psychological manipulation technology can be regarded as an important basis for identifying the subjective malignant degree of the perpetrator.

2.2 The Application of Psychological Manipulation Technology

2.2.1 Psychological Manipulation Means in "Killing Pig Plate" Fraud

In the beginning, the perpetrator creates a personable, successful person who contacts and interacts with the victim frequently, shares his life experiences, and cares about the victim's emotions. Over time, the victim's trust in the perpetrator will grow. After a certain amount of affection and trust has accumulated, the criminal will get down to business. They will say that they are good at investing, that they have done certain things that are guaranteed to win, produce fake screenshots of profits, describe a bright future where they can easily make a lot of money, and ask their victims to put their savings into fake investment platforms without thinking about it until they lose all their money (Xu & Li, 2024). In addition, in this process, the criminals will also use the "push and pull technique" to control the emotions of the victims, sometimes enthusiastic and sometimes indifferent, so that the victims in emotional fluctuations, more and more want to get attention and recognition, so that more and more trapped.

2.2.2 Psychological Manipulation Means in the Fraud of Impersonating Public Prosecutors

In this type of fraud, criminals take advantage of people's fear and deference to legal authority. They will pose as police officers, other public prosecutors and government officials, tell the identity of the victims seriously, and then fabricate the alleged money laundering charges of the victims and forge relevant documents to create a tense and strict law enforcement atmosphere, causing the victims to panic and think that they are involved in some "big case" and must cooperate with the investigation (Supreme People's Court of the People's Republic of China, 2020). Later, the other party would use the secret of the case as an excuse to ask the victim not to contact the outside world and ask the victim to transfer the money into the so-called "safe account". Because of the fear of being punished by the law, the victims are panicked and often follow the instructions of the other party directly.

2.2.3 Psychological Manipulation on Social Platforms

The huge user base and the fast speed of information dissemination make social platforms a major disaster area for "psychological manipulation". Fraudsters take advantage of the social functions of social platforms to communicate with netizens under false names. In addition to emotional induction, they also spread fake lottery messages within the group, claiming that they are randomly selected and have a chance to win big prizes, provided that they pay certain fees and deposits (Li, 2023). They took advantage of the greed of some people and the false information that others in the group had "successfully claimed" to lure victims to transfer their money. In addition, they often make inflammatory remarks to incite users to antagonize each other, while they fish in the rough waters to spread malicious links or obtain personal information.

3 PSYCHOLOGICAL MANIPULATION IN EMAIL

Criminals often send a well-designed, deceptive email to the victim. Or posing as a bank or a well-known company, the victim is asked to open an account, fill out personal information, or make a transaction directly. The emails, often using official logos and fonts, mimic a normal letter format and can be confusing. Some are subject lines such as "urgent notice" or "important document", designed to create a sense of urgency that people will not open them. When users clicked on the link, they could be directed to a fake site, where data could be leaked or money stolen.

3.1 Increasingly Difficult to Deal with the Support of Science and Technology

The rise of artificial intelligence and big data technology has provided criminals with more accurate criminal tools. They use algorithms to dig deep into the vast amount of information about users on social media platforms. By analyzing users' posts, likes and comments, and browsing history, they can map out users' interests, hobbies, and financial status, and then pinpoint their psychological weaknesses. For example, in some online scams targeting specific consumer groups, criminals design seemingly high-end investment scams targeting people who are keen on luxury consumption based on big data analysis, taking high returns as the bait, and taking advantage of their desire to increase their wealth. Past studies using data mining techniques to analyze a large number of online fraud cases have clearly shown that psychological manipulation techniques have become more sophisticated with the help of technology, and the camouflage of criminal acts has become stronger, which is difficult to cope with traditional prevention methods (Huang, 2023).

3.2 Undermining the Social Trust System

The frequent success of psychological manipulation techniques of cyber crimes has dealt a heavy blow to the social trust system. The exposure of online fraud cases will trigger a chain reaction within the society. The victims not only suffer financial damage, but also leave an indelible psychological trauma. After witnessing these cases, people around them develop fear and distrust of the Internet environment. In terms of social networking, people are wary of strangers' active communication, and their normal social interaction is hindered. In the field of e-commerce, consumers have doubts about the security of online transactions, so many people reduce or even give up online shopping. This lack of social trust greatly reduces the advantages of convenience and efficiency of the network society, seriously affects the healthy development of the network ecology, and increases the cost of social operation.

3.3 Legal Supervision Is in Trouble

At present, there are many loopholes in the legal supervision of psychological manipulation techniques of cyber crimes. The transnational and virtual nature of cybercrime, coupled with the hidden characteristics of psychological manipulation techniques, make traditional laws unable to deal with such crimes. The legal systems of different countries and regions differ significantly in terms of the definition and jurisdiction of cybercrimes. In cross-border cybercrimes, criminals often take advantage of these legal differences to move between different jurisdictions and evade legal sanctions. For example, some online fraud groups set up their servers in countries with looser laws and regulations to defraud residents of other countries, making it extremely difficult for law enforcement departments to track down and arrest them. At the same time, for the specific identification standards of psychological manipulation techniques, the legal level has not yet formed a clear and unified standard, and the rules of evidence collection are not perfect. As a result, it is difficult for law enforcement departments to accurately determine criminal acts in the actual process of case handling, and the collected evidence may not be effectively used to charge crimes due to the lack of clear rule support, which seriously weakens the deterrent power of law against psychological manipulation technology of cyber crimes.

4 COUNTERMEASURES AGAINST PSYCHOLOGICAL MANIPULATION TECHNIQUES IN CYBER CRIMES

4.1 Build a New Firewall

4.1.1 Build Cognitive Speed Bumps

In his 2011 book Thinking: Fast and Slow, American cognitive psychologist Daniel Kahneman systematically proposed and popularized an important theory in psychology and cognitive science, the dual System theory. This theory reveals an important point, that is, human cognition and decision making depend on two different thinking systems, and there is a game between the intuitive system and the rational system when human beings make decisions. The cognitive dissonance theory, formally proposed by American social psychologist Leon Festinger in 1957, also shows that when an individual holds two or more contradictory mental cognitions at the same time, psychological tension and discomfort will result from the dissonance. The perpetrator will use this dissonance to force the victim to act and block rational thinking. Cybercriminals use interface design to create cognitive shortcuts that induce the user into an intuitive decision-making mode. For example, phishing websites deliberately imitate visual symbols used by authorities to trigger users' heuristic judgments. Therefore, Internet users need to establish "cognitive speed bumps" to activate the rational system. If a link pops up in a phishing email, for example, users may be able to avoid being tricked if they take the time to check the details. Cognitive speed bumps act like brake pads for the brain, and are effective against the elaborate mental traps laid by criminals. Internet users can set themselves a short cooling-off period, such as 12 hours. In this way, the psychology can temporarily enter the buffer period, there is enough time to think and decide whether to take action, and the emotions such as impulse blindness, panic and tension are blocked from the door of reason.

4.1.2 Empower Authoritative Certification with Science and Technology

The obedience experiment carried out by the famous American social psychologist Milgram in 1961-1963 overturned people's cognition that "evil comes from individual evil", emphasized the shaping power of situation and authority on behavior, and effectively proved that the authority symbol can make 65% of subjects carry out orders that violate morality. The "Internet police" certificates and "court" notices forged by criminals make use of this psychological mechanism. The solution lies in reshaping the authoritative authentication system and establishing a dynamic verification channel. A typical example is Singapore's digital signature system for government services, which is based on blockchain technology and has made authority symbols unforgeable, reducing impersonation crimes by 73%. It can be seen that science and technology are the key to building an authoritative authentication system. If more energy and funds can be invested in the technical research of authoritative certification, it will reduce the frequency of network crime cases.

4.1.3 Social Support Systems for Coordinated Defence

The American psychologist Solomon Asch conducted a conformity experiment from 1951 to 1956. At the heart of the experiment was the question of how group pressure affects individual judgment. The results showed that 75 percent of participants followed the group's wrong answer on at least one trial; About a third obeyed the group pressure and chose the wrong answer all the time. Cybercriminals falsify social credentials to create false consensus. To do this, a network of trusted social credentials is needed. The resilience theory also emphasizes the central role of social support in coping with stress. A complete and effective network neighborhood watch system can be established to trigger community early warning when an individual's network abnormal operation is detected. For example, the Bank of Japan implemented the "transfer community confirmation" system, which successfully blocked about 83% of acquaintance fraud through the cross-verification of three social contacts. This distributed trust network reconstructs "village protection" in the digital age.

4.1.4 Three-Dimensional Innovation of Judicial Mechanism

If possible, it may consider adding a new crime to Chapter 6 of the Criminal Law in the future, that is, the crime of illegal psychological manipulation. To clarify its objective requirements include: (1) the use of systematic psychological intervention techniques; (2) continuous implementation of cognitive distortion behavior; (3) the victim's ability to make autonomous decisions is impaired. The subjective element needs

to prove that the perpetrator has a direct intention to manipulate the will of others.

In terms of evidence rules, we can try to establish a "psychological trace identification" system, and authorize judicial identification institutions to conduct psychological analysis of chat records and behavior patterns with the assistance of psychological authority departments to confirm whether there are manipulative interaction characteristics (Ministry of Public Security of the People's Republic of China, 2019).

4.2 Design a Sentencing Gradient Model

In view of this possible new crime, it is suggested to divide the harmful consequences into three quantitative standards: the first is to cause serious mental disorders or suicide consequences, sentenced to more than five years of imprisonment; Secondary causes impairment of social function for more than three months and is sentenced to fixed-term imprisonment of not more than three years. If level three is potentially dangerous but does not cause substantial damage, he shall be sentenced to criminal detention or public surveillance(Supreme People's Court of the People's Republic of China, 2020). When sentencing, the degree of specialization of technical means should be comprehensively considered, and those who use psychological professional methods to implement manipulation means should be severely punished, reflecting the evaluation principle of "technological malice".

4.3 Innovate Judicial Identification Standards

It can also make innovations in judicial determination standards. It is suggested that the Supreme People's Court should issue a special judicial interpretation to clarify that the identification criteria of "psychological manipulation behavior" should meet both: (1) the behavior pattern conforms to the psychological manipulation theory model; (2) there is an obvious power dominance relationship; (3) cognitive dependence results. In terms of proof standards, the compound identification model of "dominant evidence + expert assistance" can be adopted, allowing the use of big data behavior analysis reports as evidence reinforcement.

4.4 Establish a Collaborative and Co-Governance System

First of all, we will establish an inter-departmental coordination mechanism to enable close cooperation among public security, judicial, cyberspace and financial departments. With their advantages in investigation, public security departments are responsible for investigating cases and arresting criminals. Judicial departments provide legal support to fight crimes and ensure fair and lawful trials; Internet and information departments use professional technology to help monitor cybercrime clues and track criminals' online movements; The financial sector plays a key role in the upward flow of funds, cooperating to intercept the flow of funds involved and prevent victims from suffering greater losses. All departments hold joint meetings regularly to discuss the difficulties in the process of case detection, share experience, formulate targeted coping strategies, and form joint forces in the fight (Feng, 2023). At the same time, the training of professional quality law enforcement personnel has been strengthened. We will organize special training on psychological manipulation techniques, invite psychological experts to interpret criminal psychology, and network security technicians to explain the latest means and tracking technology of cybercrimes. In addition, it will carry out international cooperation, participate in various activities of international law enforcement platforms, establish transnational cybercrime information databases, break geographical restrictions, and jointly crack down on cross-border cybercrimes.

4.5 Improve Technology and Preventive Measures

Increase investment in research and development of artificial intelligence, big data and other technologies in the field of anti-fraud, use artificial intelligence algorithms to monitor interactive information on social platforms, detect suspicious emotional induction, misleading information and other signs of psychological manipulation in a timely manner, and issue early warnings. For example, an intelligent monitoring system developed by a research and development team of anti-fraud technology, through the study and analysis of a large number of online transaction data, can send an alarm at the moment of abnormal transactions, and effectively intercept a number of online fraud cases (Zhang & Zheng, 2023). Strengthen the supervision of online platforms so that they can effectively fulfill their main responsibilities;

Strengthen the review of information on platforms, establish a strict content review mechanism, and filter out false and fraudulent information. Improve the real-name authentication system, strictly verify users' identities, and reduce the existence of fake accounts.

5 CONCLUSION

Psychological manipulation technology in cybercrime is the product of cognitive weaponization of criminal means in digital age. Its essence lies in using human weakness and cognitive deviation to carry out precise attack. This paper reveals the operation logic of psychological manipulation technology from an interdisciplinary perspective and puts forward a three-in-one comprehensive response framework of "spiritual resistance, legal regulation and technical defense". At the spiritual level, the construction of cognitive speed bumps and distributed trust network realizes the upgrade from individual defense to group immunity; At the legal level, "illegal psychological manipulation crime" is added and a three-level sentencing model is constructed, which breaks through the limitations of traditional criminal law on behavior characterization and harm quantification, and brings "cognitive autonomy" into the scope of legal interest protection. At the technical level, innovative means such as blockchain authentication and AI monitoring and early warning provide tool support for authority empowerment and risk interception. However, the improvement of the governance system still faces challenges from accelerating technology iteration and difficulties in cross-border forensics. Future research should further explore the application of neuroscience in judicial expertise and build a transnational collaboration mechanism. Only through the multi-dimensional cooperation of law, technology and psychology can we build a "digital Great Wall" to resist psychological manipulation technology in cybercrimes, and provide a solid guarantee for individual rights and interests and network ecological security.

REFERENCES

Feng, Z. X. 2023. *Governance of online pyramid selling from the perspective of multi-agent cooperation.* Master's Thesis, South China University of Technology.

Hadnett, C. 2021. The psychology of social engineering: A framework for understanding attacker strategies. *Journal of Cybersecurity* 7(2): 45-58.

Huang, L. 2023. *Translation report on Chapter 15 of Criminal Profiling*. Master's Thesis, Southwest University of Political Science and Law.

Li, X. W. 2023. *A psych-anthropological study on victims of telecom network fraud.* Master's Thesis, Anhui University.

Ministry of Public Security of the People's Republic of China. 2019. *Electronic Data Forensics Rules for Public Security Organs*. Article 14.

Qin, S. H. 2024. Ideological risks in live streaming and governance approaches. *Journal of Wuxi Institute of Commerce* 24(3): 79-85.

Sasse, M. A., Nurse, J. R., & Hodges, D. 2022. Emotional manipulation in cybercrime: A quantitative analysis of phishing attack patterns. *Computers & Security* 115: 102619.

Supreme People's Court of the People's Republic of China. 2020. *Interpretation on Several Issues Concerning the Application of Law in the Trial of Compensation for Moral Damage Cases (Revised 2020)*. Article 3.

Xu, W., & Li, R. H. 2024. Online deviant behavior: Integrative attribution and governance mechanisms. *Journal of Jiangsu Police Institute* 39(2): 65-74.

Zhang, C. Y., & Zheng, T. C. 2023. Normative identification of organized crime in cyberspace. *Journal of Railway Police College* 33(3): 33-40.

Zheng, W. J. 2024. *The influence of online "echo chambers" on ideological and political education for college students and countermeasure research.* Master's Thesis, North University of China.