How to cite this article:
Shabanzadeh, M., & Shakouri, F. (2026). Examining and Analyzing the Dimensions of Digital Crimes from the Perspective of the Mental Element. *Journal of Historical Research, Law and Policy, 4*(3), 1-13. https://doi.org/10.61838/jhrlp.227

Article history:
Original Research

Dates:
Submission Date: 12 November 2025
Revision Date: 07 February 2026
Acceptance Date: 14 February 2026
Publication Date: 01 May 2026

Examining and Analyzing the Dimensions of Digital Crimes from the Perspective of the Mental Element

1. Mehdi. Shabanzadeh[1*]: Department of Law, Bu.C., Islamic Azad University, Bushehr, Iran
2. Farzin. Shakouri[2]: Department of Law, Bu.C., Islamic Azad University, Bushehr, Iran

*corresponding author's email: Mehdishabanzadeh@iaubushehr.ac.ir

ABSTRACT

With the expansion of information and communication technologies and the formation of cyberspace, digital crimes have become one of the most complex social, economic, and security threats. Unlike traditional crimes, these offenses lack a physical nature and encompass a wide range of victims and harms. The present study aims to analyze the psychological dimensions of digital crimes, focusing on offenders' motivations, cognitive capacities, and social and deceptive skills. The research adopts a descriptive–analytical method based on library and documentary studies, and the data have been collected from domestic and international scholarly articles, specialized books, laws, and transnational documents. The findings indicate that economic, social, psychological, and political motivations; cognitive capacities such as risk analysis and strategic planning; and social skills and deceptive techniques play a decisive role in the success of digital crimes. These dimensions interact with one another, and without a comprehensive analysis of them, preventive and punitive policies will remain ineffective. Based on the findings, the development of psychological frameworks, reform of criminal laws, design of cybercriminal behavior analysis systems, and expansion of interdisciplinary research—particularly in response to emerging technologies such as artificial intelligence and the metaverse—are essential for effective prevention and mitigation of the harms caused by digital crimes.

Keywords: *Digital crimes, mental element, criminal motivations, cognitive capacity, social skills, deception, criminal policy, cyber prevention*

Introduction

With the rapid expansion of information and communication technologies and the growing penetration of cyberspace into all aspects of social, economic, and cultural life, human life has undergone fundamental transformations. Cyberspace, by enabling information exchange and real-time interactions, has created unprecedented opportunities for socio-economic development; however, it has simultaneously provided a conducive environment for the commission of digital and cyber crimes (1, 2). Unlike traditional crimes, digital crimes lack a physical nature and are not confined to place and time; these characteristics have expanded the scope of victims and increased the severity of harms, thereby making analysis and prevention more complex. Recent research indicates that understanding cybercriminal behavior without considering offenders' psychological and cognitive dimensions is incomplete. The mental element of crime encompasses motivations, intent, cognitive skills, and offenders' social capacities, and it determines target selection, modus operandi, and the success or failure of

© 2026 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

the offense (3, 4). In other words, analyzing offenders' motivations and psychological characteristics is a prerequisite for designing effective preventive policies and criminal justice responses (5).

Despite the enactment of numerous laws and regulations in Iran and globally to counter cyber and digital crimes, ambiguities persist regarding the precise definition of digital crimes, the scope of criminal liability, and the psychological analysis of offender conduct (6, 7). This scientific and legal gap means that many preventive and punitive measures cannot fully achieve the necessary effectiveness. Moreover, emerging technologies such as artificial intelligence and the metaverse have created new capacities for offending and have further intensified the psychological and cognitive complexity of digital crimes (8). These technologies have not only complicated the tools used to commit offenses, but have also made the analysis of offender behavior and the prediction of their activities more difficult.

In light of these developments, examining the psychological dimensions of digital crimes—including motivations, cognitive processes, social skills, and deception techniques—is essential. A precise understanding of these dimensions can contribute to the formulation of effective criminal policy, the design of efficient laws, the enhancement of user education, and the development of psychology-informed prevention mechanisms (9). Such analysis also enables the identification of differences between professional and amateur offenders and supports the construction of predictive models and preventive intervention strategies.

Given the importance of the mental element in the commission of digital crimes and the complexities introduced by modern technologies, the present study seeks to answer the following question: What are the psychological dimensions of digital crimes, and how do these dimensions influence the motivations, behaviors, and methods of cyber offenders? This study aims, through an in-depth analysis of domestic and international sources and with a focus on offenders' psychological and cognitive dimensions, to identify existing gaps in preventive policies and legal frameworks in Iran and elsewhere, and to propose scientific and practical solutions for addressing digital crimes.

Research Background

Research on digital and cyber crimes has expanded substantially over the past two decades due to the growth of information and communication technologies. Early studies mainly focused on defining cyber crimes, identifying their manifestations, and clarifying the need for criminalization, with the aim of establishing an adequate legal framework to address digital offending. At this stage, the psychological and cognitive dimensions of offenders received comparatively limited attention.

In Iran, Aliverdinia and Anvari, using a descriptive–documentary approach, defined the concept of cyber crimes and examined their instances (1). Their findings indicated that public education, digital ethics, and active user participation play a key role in preventing cyber crimes, and that purely punitive responses cannot achieve sufficient effectiveness. This study further suggested that the absence of psychological analysis of offenders constitutes one of the major barriers to designing effective preventive policies. With respect to criminal liability, Razavi Fard and Mousavi, through an analysis of the Iranian legal framework on computer crimes, highlighted the importance of criminal liability for both natural and legal persons in cyberspace (2). Their work emphasizes that without understanding the mental element of crime, criminal liability remains incomplete and ineffective. Zolfaghari and Tavangar, focusing on criminal policy in computer crimes, identified two main categories of digital crime: traditional offenses committed through computer tools, and emerging offenses directed against data and information systems

(10). They argued that conceptual ambiguity in defining computer crime is among the core challenges of Iran's criminal policy and that psychological analysis of offender behavior has been overlooked in legislative design.

Contemporary international research has also addressed the psychological dimensions of digital crimes. Bullée demonstrated that social engineering and sophisticated cyberattacks are designed around victims' cognitive and affective triggers, and that analyzing the psychological behavior of both victims and offenders is essential to understanding successful offending (11). Rogers and Rowe likewise maintain that psychological profiling of cyber offenders—encompassing motivations, personality characteristics, and decision-making patterns in digital environments—is a prerequisite for designing effective prevention and punishment policies (12, 13).

With the emergence of technologies such as artificial intelligence and the metaverse, digital crimes have become more complex, making psychological analysis of offenders even more necessary. Saleh-Nejad Behrastaghi and Soufi have shown that artificial intelligence functions both as an instrument for committing cyber crimes and as a tool for combating them; accordingly, understanding offenders' psychological and cognitive profiles is vital for developing defensive frameworks (14). In addition, Abouzari, in examining crime in the metaverse, proposed the creation of an independent branch termed "meta criminal law" and underscored the need to attend to offenders' psychological and cognitive complexities (15).

In comparative and theoretical scholarship, Biglari's analysis of the mental element in the international crime of genocide in jurisprudence and international law suggests that, in some crimes, the mental element alone can ground criminal responsibility; this insight can be instructive for conceptualizing digital crimes that may lack a tangible material outcome (16). Moreover, Arabie Ayask identified the ineffectiveness of existing laws, difficulties of proof, and weak international cooperation as major barriers to effective cybercrime control, emphasizing the need for legal reform and specialized training (17). Recent studies also indicate that the psychological dimensions of digital crime include economic, social, psychological, and political motivations, and that these dimensions combine with offenders' cognitive and social skills to determine whether the criminal act succeeds or fails (3, 18). This body of evidence suggests that many criminal policies and preventive measures will remain ineffective if they do not incorporate psychological analysis of offenders, and thus cannot fully ensure the security of users and organizations.

Despite legal and research advancements, comprehensive analysis of the psychological dimensions of digital crimes in Iran and globally remains limited. In particular, the combined examination of motivations, cognitive skills, and offenders' social capacities has been less frequently addressed, and this gap impedes the formulation of preventive policy and the drafting of effective laws. The present study, by analyzing the psychological dimensions of digital crimes, identifying offenders' motivations, cognitive processes, and social skills, and proposing preventive strategies, seeks to address this scientific gap and to provide an evidence-informed framework for criminal policy and effective prevention.

Theoretical Foundations

The concept of digital and cyber crimes

Digital or cyber crimes refer to criminal behaviors committed through digital tools, networks, and online environments, and they can generate extensive financial, social, and psychological harms (19). These crimes include data theft, phishing, system hacking, AI-enabled cyberattacks, and misuse of social networks (6). Unlike

traditional crimes, which are often materially manifested, digital crimes lack a physical nature and are frequently accompanied by psychological and cognitive complexities; accordingly, their analysis and prevention require a precise understanding of offenders' motivational and behavioral drivers (20).

The mental element in digital criminology

The mental element of crime includes intent, motivation, cognition, and offenders' psychological skills, and it plays a decisive role in the success or failure of digital offending (21). Research indicates that cyber offenders' motivations may be economic, social, psychological, or political (16). For example, phishing and social engineering attacks are commonly executed by exploiting victims' psychological vulnerabilities and by inducing false trust or a sense of urgency. Understanding offenders' motivations and psychological characteristics is thus a prerequisite for designing preventive policies, criminal regulations, and effective countermeasures. Domestic studies suggest that, although Iran's legal framework on computer crimes anticipates criminal liability for natural and legal persons, psychological analysis of offender behavior has received limited attention (7).

Cognitive dimensions and offender decision-making

The cognitive dimension of the mental element includes the capacity for analysis, planning, predicting victim behavior, and assessing risk. Findings indicate that cyber offenders draw on advanced cognitive skills to analyze their own conduct and victims' reactions and to design strategies for committing offenses (22).

• Risk-analysis-based decision-making: Many digital crimes are committed only when offenders anticipate a high likelihood of success. The ability to identify system vulnerabilities and analyze victim behavior constitutes a core component of the cognitive dimension (23).

• Strategic planning and anticipation: Complex offenses such as ransomware attacks require multi-stage planning and anticipation of victim responses. This cognitive capacity reduces the risk of failure and increases the effectiveness of criminal conduct (24).

• Learning and dynamic adaptation: Cyber offenders learn from their own prior experiences and those of others and adjust their strategies dynamically. This learning process forms a complex cognitive dimension that can make offending more efficient and, in some respects, more predictable (25).

Social skills and deception methods

A third psychological dimension concerns social skills and deception techniques. The success of digital crimes requires the capacity to gain victims' trust, manipulate emotions, and exploit personal information.

• Social engineering: Successful cyberattacks are often executed through psychological and social techniques. Creating urgency or fear can push victims toward erroneous actions (26).

• Interaction capacity in digital environments: By analyzing user behavior on social networks, offenders collect the information necessary to design personalized attacks. This complex social skill increases the probability of successful offending (27).

• Flexibility and adaptation: Successful offenders can adapt their deception methods to shifts in the cyber environment and to victim responses. This flexibility heightens the importance of education and preventive policies (28).

Emerging technologies and psychological complexities

The emergence of technologies such as artificial intelligence and the metaverse has made the psychological dimensions of digital crimes more complex. Artificial intelligence can operate both as an instrument for committing offenses and as a tool for combating crime; therefore, psychological and cognitive analysis of offenders in this context is of critical importance (15).

Based on theoretical and empirical evidence, the psychological dimensions of digital crimes can be organized around three main axes: motivations, cognitive skills, and social/deceptive capacities. Analyzing these dimensions is a prerequisite for designing effective criminal policy, preventive measures, and user protection. The theoretical foundations presented here provide an appropriate scientific framework for analyzing cyber offender behavior in the present study and establish a basis for examining the interaction between the mental element and the commission of digital crimes.

Methodology

The present study is a descriptive–analytical research project conducted to analyze the psychological dimensions of digital crimes. The descriptive–analytical approach enables the identification, categorization, and analysis of cyber offenders' characteristics, psychological factors, and motivations, and it facilitates a precise understanding of the relationships between the mental element and offender behavior in digital environments. The study population consists of scholarly studies, books, domestic and international articles, laws and regulations related to computer crimes, transnational documents, and illustrative case materials that address the psychological dimensions of such crimes. The sample was selected non-randomly through purposive selection of credible sources to ensure comprehensive coverage of both the theoretical and practical dimensions of the topic.

Research data were collected through library and documentary methods. The sources include domestic and international scholarly articles, specialized books in criminal law and criminology, research reports, Iranian laws, and transnational documents such as the Budapest Convention and the Arab Convention on Combating Information Technology Offences. In addition, relevant international publications on criminal psychology and cyber offender behavior were analyzed. Data analysis was conducted using content analysis. Under this method, scholarly texts and legal documents were coded for concepts related to the mental element, motivations, skills, and cyber offender behavior. A comparative analysis between Iranian law and transnational instruments was also conducted to identify similarities and differences in the treatment of the psychological dimensions of crime and criminal responsibility across different criminal policy frameworks.

Research Findings

The analysis of library-based and documentary sources indicates that the mental element constitutes the central component in the commission of digital crimes. Offenders' decision-making, target selection, modus operandi, and the level of criminal success are strongly influenced by three core psychological dimensions: motivations, cognitive capacities, and social/deceptive skills. These dimensions do not operate independently; rather, through their interaction, they shape the success or failure of digital offending.

1. Motivations of Cyber Offenders

Motivations form the core of the mental element of crime and determine why an individual engages in offending. The findings show that cyber offenders' motivations are layered and hybrid, often combining economic, social, psychological, and political factors.

Economic motivation: A substantial share of digital crimes is committed with the aim of financial gain. This category includes phishing, ransomware, online fraud, and unauthorized access to bank accounts. A comparative reading aligned with Razavi Fard and Mousavi indicates that, in Iran as well, economic motivation constitutes the primary driver of a large proportion of cyber offenses, and preventive policies that neglect this factor are unlikely to be effective (2). Moreover, when economic motivation is combined with offenders' high cognitive capability, attacks become more sophisticated and more difficult to detect.

Social/identity motivation: Some individuals engage in cyber offending to gain prestige or visibility on social networks. A comparative analysis consistent with Aliverdinia and Anvari suggests that, in Iran, activities such as the disclosure of confidential information or unauthorized penetration of others' systems may be undertaken to attract attention and secure social identity (1). These motivations activate not only the psychological dimension but also offenders' cognitive and social dimensions, because achieving social goals often requires planning and analyzing victim behavior.

Psychological/emotional motivation: Some cyber offenses arise from emotional needs such as power-seeking, entertainment, or revenge. These motivations are frequently associated with high complexity and extensive use of social engineering, as offenders employ psychological techniques to trigger victims' emotions (11).

Political/ideological motivation: Organized attacks aimed at disrupting political stability, infiltrating governmental systems, or disseminating ideological messages typically require advanced planning and cognitive analysis. The reviewed sources suggest that such motivations influence not only the offender's tolerance for risk, but also the selection of tools and methods used in committing the offense (28).

The findings further indicate that many cyber offenses involve mixed motivations, and prevention strategies premised solely on economic drivers are insufficient. A multi-dimensional approach that also accounts for social, psychological, and political motivations is required for preventive and criminal justice measures to be effective. The classification of cyber offenders' motivations and their behavioral implications is presented in Table 1.

Table 1. Classification of Cyber Offenders' Motivations and Behavioral Implications

Type of Motivation	Examples of Digital Crimes	Predominant Psychological Features	Influence on Modus Operandi	Implication for Criminal Policy
Economic	Phishing, ransomware, online fraud	Profit orientation, high risk analysis	Targeted and sophisticated attacks	Emphasis on financial deterrence
Social/Identity	Demonstrative hacking, data disclosure	Need for visibility, prestige-seeking	Media-oriented and symbolic attacks	Cultural and educational prevention
Psychological/Emotional	Cyber harassment, digital revenge	Anger, sensation-seeking, control needs	Reliance on social engineering	Psychological interventions
Political/Ideological	Infiltration of governmental systems	Ideological commitment, goal-directedness	Multi-stage planning	National security and structural prevention

The analysis suggests that many cyber offenses result from the synergistic combination of economic, social, and psychological motivations—meaning that a single attack may generate financial benefits, enhance offender status, and provoke an emotional response in the victim. In addition, there appears to be a direct relationship between

motivation type and the level of offense complexity; for example, political and ideological motivations tend to lead to multi-stage planning and increased attack complexity, whereas purely economic motivation is more often associated with targeted, lower-complexity attacks. Practically, this implies that criminal policy and preventive frameworks cannot be effective if they focus on only one motivational class; instead, they require layered and flexible strategies capable of addressing the full spectrum of potential motivations. Accordingly, motivations are not merely initial drivers of offending; they function as the entry point of the digital crime cycle and activate other capacities and skills.

2. Cognitive Capacities: The Core of Decision-Making and Behavioral Analysis in Digital Crimes

A key dimension of the mental element in digital crimes is offenders' cognitive capacity. These capacities include risk analysis, prediction of victim behavior, strategic planning, and learning from past experience, and they constitute the primary distinction between professional and amateur offenders. International research indicates that many successful cyberattacks would fail without systematic risk assessment, precise targeting, and strategic planning (12).

Risk-analysis-based decision-making: The findings indicate that professional cyber offenders, prior to acting, carefully assess both technical vulnerabilities and likely victim behaviors. This risk analysis includes identifying software weaknesses, evaluating users' awareness, and predicting victim reactions. In other words, digital crime success is unlikely without deep knowledge of the environment and the victim. A comparative reading aligned with domestic discussions underscores that high-cognition offenders may circumvent existing legal and technical controls, which further supports the need to analyze offenders' cognitive behavior in prevention design (2).

Strategic planning and reaction forecasting: Complex attacks such as ransomware, infiltration of organizational networks, and AI-enabled attacks require multi-stage planning. This planning includes identifying targets, selecting appropriate timing, designing entry pathways, and forecasting victim responses. Such cognitive capability reduces failure probability and increases attack effectiveness, implying that preventive policies must be designed to specifically disrupt these skills (7).

Learning and dynamic adaptation: The analysis indicates that offenders learn from past mistakes and from other offenders' experiences and dynamically revise their strategies. This learning includes adopting more advanced tools, altering tactics, and customizing attacks for each target. This finding suggests that digital crime extends beyond technical competence and that behavioral understanding and environmental cognition are critical to its success (13). Table 2 compares the cognitive capacities of professional and amateur offenders.

Table 2. Comparison of Cognitive Capacities Between Amateur and Professional Offenders

Cognitive Component	Amateur Offender	Professional Offender
Risk analysis	Minimal and intuitive	Systematic and data-driven
Planning	Single-stage	Multi-stage
Forecasting victim response	Weak	Accurate and experience-based
Learning from failure	Limited	Dynamic and adaptive
Use of emerging technology	Low	High (AI, automated tools)

This table indicates that cognitive capacity is the primary factor distinguishing professional offenders from amateurs. Criminal policy should incorporate mechanisms to differentiate levels of cognitive skill and offense severity. Offenders' cognitive capacity plays a pivotal role in decision-making, predicting victim behavior, and successfully committing digital crimes. Professional offenders increase their probability of success and minimize

the risk of failure by systematically analyzing risk, identifying system vulnerabilities, and forecasting victim responses. Moreover, the ability to learn from past experiences and adapt dynamically to environmental change makes digital crime more fluid and complex, such that static prevention measures are unlikely to remain effective. In this sense, cognitive capacity functions as the engine of the criminal cycle: motivations, without accurate cognition and planning, are unlikely to yield successful outcomes. Overall, the cognitive analysis suggests that cognitive capacity is the decisive differentiator between professional and amateur offenders and a key prerequisite for success in complex digital offenses.

3. Social Skills and Deceptive Techniques: The Human Dimension of Digital Crime Success

The third dimension of the mental element concerns social skills and deception methods, which are decisive for success in digital crimes. This dimension includes building victim trust, manipulating emotions, and exploiting personal and social information. Research evidence indicates that many successful attacks depend not only on technical skills but also on offenders' mastery of human behavior and victim psychology (11).

Social engineering and exploitation of psychological vulnerabilities: Phishing attacks, misuse of social networks, and engineered emails exemplify the use of psychological principles to deceive victims. Studies indicate that emotional triggers such as fear, urgency, and financial temptation can compel victims into erroneous actions. A comparative reading consistent with domestic scholarship suggests that analyzing the mental element is essential for designing preventive policies and user training (16, 29).

Interaction capacity and social network analysis: To design successful attacks, cyber offenders study user behavior in social networks and the digital environment. The collection of information such as interests, relationships, and online activity enables personalized attacks and increases the effectiveness of deception methods. Comparative alignment with Yekrangi and Morsi indicates that, even under stringent legal controls, offenders' high social competence can reduce the effectiveness of punitive responses (6).

Social flexibility and adaptive behavior: Successful digital offending requires the ability to adapt deception methods to a dynamic environment and to victim responses. For example, a phishing template that succeeds in one organization may fail in another; a successful offender is one who rapidly adapts to new conditions. These findings emphasize the need for dynamic preventive policies and continuous user training and indicate that static approaches and fixed instructions are unlikely to be sufficiently effective (27).

The combined analysis of cognitive dimensions and social skills indicates that the success of digital crimes depends not only on technical knowledge but also on victim-behavior analysis, forecasting capacity, and dynamic learning. Domestic and international evidence suggests that without a precise understanding of the mental element and its interaction with cognitive and social capacities, preventive policies and criminal justice responses will remain partial and ineffective (12, 13). In other words, successful digital offending depends on the interaction between motivations, cognitive capacities, and social/deceptive skills, and any legal or educational effort that does not comprehensively analyze these dimensions cannot ensure the security of users and organizations. Table 3 presents offenders' social skills and deception techniques.

Table 3. Offenders' Social Skills and Deception Techniques

Social Skill	Technique Used	Victim Vulnerability	Preventive Implication
Trust-building	Spoofed emails, impersonation	Institutional trust	Digital literacy training
Emotional manipulation	Inducing fear and urgency	Psychological pressure	Behavioral warnings and prompts
Social network analysis	Personalized attacks	Disclosure of personal information	Privacy policy and controls
Flexibility and adaptation	Rapid tactic switching	User unpreparedness	Dynamic training and response drills

Offenders' social skills are a decisive factor in translating technical tools into operational success in digital environments. The ability to gain victim trust and manipulate emotions means that even low-technical-complexity attacks can be effective. In addition, analyzing social networks and users' personal data enables the personalization of attacks and increases their success rates. Flexibility and adaptive capacity in response to environmental changes and victim reactions make digital crime less predictable and more complex, indicating that success in digital crimes extends beyond purely technical and cognitive competence. Overall, the analysis suggests that without this social/deception dimension, even well-planned offenses with strong cognitive capacity may not be effective; social skill operates as the link between cognitive capacity and practical impact and is the operational guarantor of digital crime success.

To illustrate the interaction among the three psychological dimensions, the following conceptual model can be used:

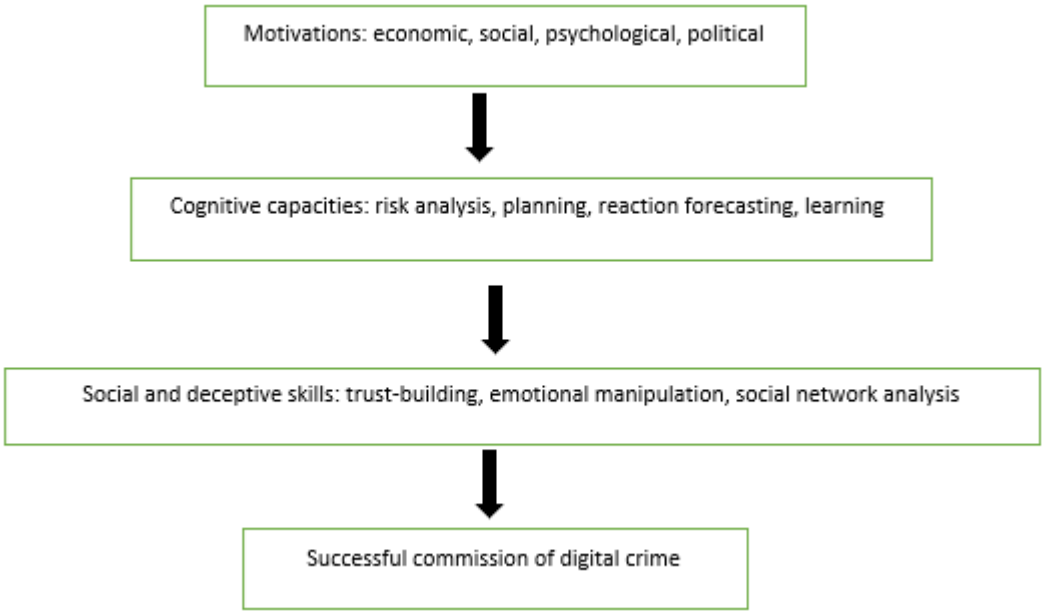

Figure 1. Conceptual Model of the Interaction Between Motivations, Cognition, and Social Skills in Digital Crime Success

The overall analysis of the findings indicates that the success or failure of digital crimes results from a dynamic interaction among three psychological dimensions: motivations, cognitive capacity, and social/deceptive skills. Within this cycle, motivations operate as the initial driver and activate the offender's cognitive capacity so that the pathway and method of offending can be designed. Cognitive capacity enables the effective use of social and deceptive skills, and ultimately, the coordination of these three dimensions ensures the successful commission of digital crime. These dimensions influence one another reciprocally: cognitive capacity affects how and to what

extent social skill is deployed, while success in social manipulation, in turn, reinforces the offender's future motivations. An analysis of this interaction shows that one-dimensional measures—such as training alone or legislation alone—are ineffective, and that prevention policies must simultaneously target motivations, cognitive capacity, and social skills.

The conceptual model derived from the findings suggests that motivations—comprising economic, social, psychological, and political factors—are activated first, followed by cognitive capacities such as risk analysis, planning, forecasting victim behavior, and learning from experience. Cognitive capacity then facilitates social and deceptive skills such as trust-building, emotional manipulation, and social network analysis, ultimately leading to successful digital offending and generating preventive and legal implications.

In summary, the macro-level findings show that the success of digital crimes is the product of a three-dimensional interaction: motivations act as the initial stimulus, cognitive capacity determines the route and method of offending, and social skills ensure operational effectiveness. Prevention policies and legal frameworks must be designed in a comprehensive and dynamic manner, because any isolated measure—without analyzing the interaction among these three dimensions—will be ineffective. Scientifically, these findings indicate that the study of digital crimes must extend beyond technical competence and existing laws and adopt an interdisciplinary approach encompassing psychology, criminology, and cybersecurity. Practically and legally, criminal and preventive frameworks should account for the offender's motivational profile, cognitive capacity, and social skill level, and should develop flexible, educational, and technology-enabled policies. The final implication of this analysis is that without a comprehensive examination of psychological dimensions and their interaction, no preventive policy or legal intervention will be able to reduce digital crime success or guarantee the security of users and organizations.

Conclusion

The present study showed that the mental element of digital crime has three principal dimensions: motivations, cognitive capacities, and social/deceptive skills. These three dimensions interact with one another, and the success or failure of digital offending depends largely on the degree of coordination among them. The findings are consistent with prior domestic and international research and confirm that psychological analysis of offenders is necessary not only for prevention but also for designing criminal policies and countermeasures.

1. Motivations and offender behavior analysis: The findings show that economic, social, psychological, and political motivations constitute the core of digital offenders' behavior, and without understanding them, preventive measures will remain incomplete. This conclusion aligns with Biglari and Jafari, who treat the mental element as a prerequisite for designing effective criminal policy (16, 29). In addition, research by Stylianou et al. and Thomopoulos et al. indicates that motivations are often hybrid and that offender planning involves multi-dimensional complexity (4, 18). From this perspective, criminal and educational policies cannot focus exclusively on economic motivation and must also incorporate psychological and social dimensions.
2. Cognitive capacities: The cognitive dimension includes risk analysis, strategic planning, and dynamic learning, and it forms the primary distinction between professional and amateur offenders. The reviewed sources indicate that professional offenders, by leveraging advanced cognitive skills, can identify system vulnerabilities, predict victim reactions, and design multi-stage attacks. These findings align with domestic

research showing that existing laws, without a cognitive analysis of offender behavior, may not create effective deterrence (2, 6).

3. Social skills and deception techniques: The findings indicate that the ability to build trust, manipulate emotions, and exploit victims' personal information is a decisive factor in the success of digital crime. Social skills, together with the cognitive dimension, enable the design of complex and personalized attacks; without analyzing this dimension, criminal and educational policies will remain ineffective. These findings are consistent with domestic studies emphasizing that the mental element must be comprehensively incorporated into preventive interventions (16, 29).

Scientific and legal implications: The analysis of these dimensions indicates that preventing digital crimes requires a multi-dimensional approach incorporating psychological, cognitive, and social analysis of offenders. From a legal standpoint, existing laws in Iran and in many other jurisdictions focus primarily on criminalization and criminal liability, while paying less attention to motivations, cognition, and social skills (14, 17). This gap reduces the effectiveness of criminal and preventive policies and highlights the need to reform legal and administrative frameworks.

Based on the findings of the study, four core recommendations are proposed: development of psychological frameworks; reform of criminal laws and policies; design of offender behavior analysis systems; and expansion of interdisciplinary research.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adhered in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Aliverdinia A, Anvari A, editors. Cybercrimes in Iran: Instances of cybercrimes and strategies to combat them. International Conference on Humanities, Psychology, and Social Sciences; 2015; Tehran.
2. Razavi Fard B, Mousavi SN. Criminal responsibility in cyberspace in Iranian law. Criminal Law Research Quarterly. 2016;5(16):29-45.
3. Quibell J. Towards in situ psychological profiling of cybercriminals using deception. 2024.
4. Thomopoulos GA, Lyras DP, Fidas CA. A systematic review of phishing from neuro/behavioral perspective. Personal and Ubiquitous Computing. 2024. doi: 10.1007/s00779-024-01794-8.
5. Haber E. The criminal metaverse. Indiana Law Journal. 2024;99(3):842-91.
6. Yekrangi M, Morsi H. Analysis of the criminalization of the production and distribution of purely criminal software and electronic tools in Iran's criminal policy in light of transnational documents. Judicial Law Views Quarterly. 2020;25(92):311-32.
7. King TC, Aggarwal N, Taddeo M, Wahbi Z. Artificial intelligence crimes: An interdisciplinary analysis; threats and predictable solutions. Tamadon-e Hoghoghi. 2023(18).
8. Stănilă LM, editor On the curiosities of the future: Meta criminal law. SHS Web of Conferences; 2023.
9. Kostenko OV. Electronic jurisdiction, metaverse, artificial intelligence, digital personality, digital avatar, neural networks: Theory, practice, perspective. World Science. 2022;1(73):1-13. doi: 10.31435/rsglobal_ws/30012022/7751.
10. Zolfaghari S, Tavangar A. Criminal policy in computer crimes. Legal Journal. 2017.
11. Bullée JW. On the anatomy of social engineering attacks. Journal of Investigative Psychology and Offender Profiling. 2018.
12. Rogers MK. Psychological profiling as a tool for digital forensics. Digital Forensics2016.
13. Rowe NC, Rrushi J. Introduction to cyber deception: Springer; 2016.
14. Saleh-Nejad Behrastaghi S, Soufi S. The impact of artificial intelligence in committing cybercrimes. Journal of Law Studies. 2023;11(51):1-18.
15. Abouzari M. Metaverse and Rethinking in Criminal Policy. Iranian Journal of Public Policy. 2024;10(3):86-98.
16. Biglari P. Investigating the mental element of the international crime of genocide in jurisprudence and law. Comparative Research on Islamic and Western Law. 2017;4(1):1-3.
17. Arabie Ayask Z, editor Investigating the legal dimensions of cybercrimes and modern challenges in cyberspace. 1st International Conference on Emerging Research in Psychology and Educational Sciences; 2025; Ahvaz.
18. Stylianou I, Bountakas P, Zarras A, Xenakis C. Suspicious minds: Psychological techniques correlated with online phishing attacks. Computers in Human Behavior Reports. 2025;19:100694. doi: 10.1016/j.chbr.2025.100694.
19. Shiri A. A central issue in criminal policymaking. Public Policy Quarterly. 2023;9(2):68-82.
20. Razavi M. Cybercrimes and the role of the police in preventing and detecting these crimes. Danesh-e Entezami Quarterly. 2007;9.
21. Lee WS. The role of criminal law in the metaverse. Legal Journal. 2022;42(3):177-202. doi: 10.38133/cnulawreview.2022.42.3.177.
22. Latif Zadeh M, Gubouli Darfashan MM. Introducing digital identity in the metaverse: Identifying related legal challenges and solutions. Private Law Studies Quarterly. 2023;53(2):349-72.
23. Darabpour MR. Metaverse, nature and legal challenges (governance, persons and property). Modern Technologies Law. 2023;4(7):65-81.
24. Boujar E. Investigating the dimensions of computer espionage. Payam-e Ghanoon. 2009(38).
25. Torki GA. The nature of computer crimes. Dadrasi Monthly. 2009;13(77).
26. Torki GA. Computer espionage. Dadrasi Monthly. 2010;14(79).
27. Jalali Farahani AH. Situational prevention of cybercrimes in light of human rights standards. Fiqh and Law Quarterly. 2005;2(6).
28. Jalali Farahani AH. Criminal jurisdiction in cyberspace. Fiqh and Law Quarterly. 2007(11).
29. Jafari F. The position of the mental element (mens rea) and criminal responsibility in the definition of crime. Teachings of Criminal Law. 2022;19(24):33-62.