How to cite this article:
Amirzoy, M. K., Esmaeili, M., & Tadayyon, A. (2025). Assessment of the Challenges in Implementing Afghanistan's Criminal Policy in Preventing Cybercrime: From Theory to Practice. *Journal of Historical Research, Law and Policy, 3*(1), 1-14. https://doi.org/10.61838/jhrlp.127

Article history:
Original Research

Dates:
Submission Date: 18 December 2024
Revision Date: 13 February 2025
Acceptance Date: 20 February 2025
Publication Date: 25 March 2025

Assessment of the Challenges in Implementing Afghanistan's Criminal Policy in Preventing Cybercrime: From Theory to Practice

1. Mohammad Karim. Amirzoy [1] : Department of Criminal Law and Criminology, CT.C., Islamic Azad University, Tehran, Iran
2. Mahdi. Esmaeili [2*]: Department of Criminal Law and Criminology, CT.C., Islamic Azad University, Tehran, Iran
3. Abbas. Tadayyon [3]: Department of Criminal Law and Criminology, CT.C., Islamic Azad University, Tehran, Iran

*corresponding author's email: Mahdi.esmaeili@iaustb.ac.ir

ABSTRACT

With the expansion of information technology and the increasing use of cyberspace, cybercrime has become one of the fundamental challenges facing legal systems, particularly in developing countries such as Afghanistan. This study examines Afghanistan's criminal policy toward cybercrime and evaluates its challenges and shortcomings in the prevention and control of such offenses. Accordingly, the present research, using a descriptive–analytical method and through the examination of legal documents such as the Law on Combating Cybercrime and the Afghan Penal Code, analyzes the strengths and weaknesses of criminal policies aimed at addressing cybercrime. The findings indicate that Afghanistan's criminal policy has been predominantly reactive, with limited attention devoted to the prevention of cybercrime. Factors such as a shortage of specialized personnel, weak technical infrastructure, lack of coordination among various institutions, and implementation challenges at the national level have hindered the effectiveness of existing policies in reducing cybercrime and enhancing cybersecurity in the country. Moreover, insufficient international cooperation and legal limitations in combating transnational cybercrime constitute additional challenges. To improve Afghanistan's criminal policy, the article recommends adopting a preventive approach focused on public education, strengthening judicial institutions, and enhancing international cooperation. Such reforms would contribute to reinforcing infrastructure and taking effective steps toward reducing cybercrime.

Keywords: *Criminal policy, cybercrime, crime prevention, Afghanistan, law enforcement, international cooperation*

Introduction

In recent decades, the penetration of information technology into human daily life has led to fundamental transformations in the social, economic, and cultural structures of societies. Afghanistan, as a country in transition, has not been exempt from these developments. With the remarkable expansion of internet access, it has experienced a new sphere of digital communication and interaction. Although these changes have provided a platform for economic and cultural growth, they have simultaneously created the conditions for the emergence and expansion of a particular type of offense known in the legal literature as "cybercrime" (1). Cybercrimes include a wide range of criminal behaviors, from hacking and unauthorized access to computer systems to electronic fraud, identity theft, the dissemination of malware, and cyberattacks on critical infrastructure. The inherent characteristics

of these crimes—such as their transnational nature, the concealment of the offender's identity, high speed, and the difficulty of detection and prosecution—have rendered traditional criminal policy, which is primarily based on punitive reaction, incapable of adequately addressing them (2, 3).

In Afghan law, the term "cyber" refers to virtual space and intangible communications that are realized through electronic tools such as computers and mobile phones. The Ministry of Communications of Afghanistan has reported that a significant portion of the country's population has access to social networks, but the lack of public awareness regarding the threats of cyberspace has caused the number of victims of cybercrime to increase day by day. Many users, without sufficient training in digital security, are exposed to threats such as online theft, extortion, and intrusions into personal accounts (4). Despite the warnings issued by security institutions and the enactment of the Law on Combating Cybercrime in 2014 with objectives such as ensuring national information security, preventing cyberattacks, and expanding international cooperation, there remains a considerable gap between law and practice. Although the Afghan legislature has attempted in the Penal Code to identify the instances of cybercrimes and determine their punishments, institutional inefficiency and weak technical expertise at the implementation stage have prevented the realization of the law's preventive objectives (5).

The importance of the present study lies in the fact that while developed countries, by relying on specialized cyber police and targeted training, have been able to control virtual threats to some extent, Afghanistan still finds itself at the initial stages of cyber policy-making. The shortage of specialized personnel in prosecutorial and police bodies, the lack of specialized training in universities, and the absence of institutional coordination between judicial and executive authorities are among the most important factors that have rendered the implementation of criminal policy in the field of cybercrime ineffective (5). Accordingly, the central problem of this research is why, despite the adoption of new laws, the level of prevention of cybercrime in Afghanistan remains low and which factors hinder the effective implementation of criminal policies in this area.

The main hypothesis of the study is that Afghanistan's criminal policy regarding cybercrime is more reactive than proactive; in other words, it focuses on punishment after the commission of the offense rather than on preventing its occurrence. The lack of executive cohesion, the shortage of technical expertise, and weak international cooperation are among the obstacles that deprive this policy of effectiveness. It appears that these inconsistencies have led even the existing laws to be ineffective in reducing the incidence of cybercrime, preventing the criminal justice system from performing a deterrent role (1, 4, 5).

On this basis, this article, drawing on legal and criminological data, examines the current status of Afghanistan's criminal policy toward cybercrime. It seeks to answer the following questions: What are the characteristics of the existing criminal policy in Afghanistan regarding cybercrime? What challenges constrain its implementation? And what strategies can reduce the gap between theory and practice? To answer these questions, the article first elaborates the theoretical framework related to criminal policy and the prevention of cybercrime, then evaluates the current situation by analyzing Afghanistan's laws and institutional structures, and finally offers recommendations for strengthening the preventive dimension of this policy.

Theoretical and Conceptual Framework

The rapid developments in information technology over the past two decades have transformed the foundations of many human and social interactions and created the conditions for the emergence of a new type of offense known as cybercrime. These offenses, which are committed in virtual space and through electronic tools, have

altered the traditional boundaries of crime, victim, and offender, and confronted the criminal justice system with new challenges (1). The transnational nature of cybercrimes, the high speed of their commission, the ease of concealment, and the difficulty of detection and prosecution are among the most important features that distinguish cybercrimes from classical offenses (6). Under such circumstances, states' criminal policies are compelled to adapt to new realities and adopt approaches that, in addition to punitive measures, take into account preventive, cultural, and technological dimensions.

In criminal law literature, criminal policy refers to the set of measures adopted by the state and its affiliated institutions to confront, prevent, and control criminality. In this sense, criminal policy encompasses legislative, judicial, and executive dimensions, and its realization requires coordination between formal and informal structures of social control (7). With the advent of digital technology, many countries have revised their criminal policies in the area of cybercrime, as it has become clear that purely punitive responses not only lack effective deterrence but may also lead to the expansion of more complex forms of delinquency in virtual space (8).

From a theoretical perspective, several criminological approaches can provide an appropriate analytical framework for understanding cybercrime and Afghanistan's criminal policy. The first is social control theory, introduced by Hirschi and others, which emphasizes the relationship between the individual and society. According to this theory, the weaker an individual's bond with social institutions such as family, education, religion, and law, the higher the likelihood of offending (7). In the context of Afghanistan, where social structures have yet to attain the requisite stability and educational and cultural institutions do not fully perform their functions, weak social control can be considered one of the main factors contributing to the rise of cybercrime. In particular, the absence of a digital literacy education system in schools and universities has left citizens without adequate awareness of cyber threats (9). Therefore, strengthening social institutions and promoting a culture of safe technology use must be part of a preventive criminal policy in Afghanistan.

The second influential approach in explaining cybercrime is rational choice theory, which views the offender as a rational actor who weighs costs and benefits before committing an offense. According to this theory, whenever the probability of detection and punishment is low and the benefits of offending are high, the likelihood of criminal behavior increases (10). In Afghanistan's cyberspace, due to the absence of digital identification systems, the shortage of specialized personnel in the police and prosecution services, and weak mechanisms of electronic monitoring, the costs of offending are low. Thus, for effective deterrence, criminal policy must emphasize not only punishment but also increasing the likelihood of detection and prosecution. Establishing digital databases, training cyber police forces, and employing advanced technologies in tracking offenders are among the measures that can raise the cost of offending and, from a rational choice perspective, reduce the probability of crime (5).

The third approach is social learning theory, developed by Bandura and elaborated by Sutherland in differential association theory. According to this theory, individuals learn criminal behavior through interaction and observation of deviant models in their social or virtual environment (11). In Afghanistan's virtual space, due to the unregulated spread of social networks and the lack of effective content supervision, individuals—especially young people—are exposed to modeling from anti-normative behaviors. From the standpoint of criminal policy, this necessitates educational, cultural, and media interventions to prevent the reproduction of criminal behavior in cyberspace.

Alongside criminological theories, psychological and sociological approaches are also important in explaining the causes of cybercrime. From the perspective of forensic psychology, some individuals, due to personality traits such as anxiety, aggression, or feelings of powerlessness in real life, may attempt to compensate for their failures

through destructive behavior in virtual space (12). In contrast, from a sociological viewpoint, dysfunctional social structures, widespread unemployment, economic poverty, and weak regulatory systems are among the factors that intensify tendencies toward cybercrime (6). In Afghanistan, the combination of these two dimensions—namely, economic and psychological pressures stemming from social instability—can lead some individuals to exploit virtual space for financial gain or to express social discontent.

Moreover, an analysis of Afghanistan's criminal policy in light of these theories reveals that although the country has made legislative progress in criminalizing cyber behavior, at the executive level it still adheres to a reactive approach. The enactment of the Law on Combating Cybercrime in 2014 was an important step toward establishing a legal framework, yet weak technical infrastructure, a shortage of trained personnel, and a lack of coordination among responsible institutions have prevented the realization of its objectives (5, 8). Effective preventive criminal policy requires the integration of three essential dimensions: education and awareness-raising, institutional empowerment, and international cooperation. Without these elements, purely legislative reforms will not yield practical results.

In addition, situational crime prevention theory—which focuses on reducing opportunities for offending through environmental design and control mechanisms—can serve as a useful guide for Afghan policymakers. Strengthening user identification systems, improving the security of banking infrastructure, and establishing early warning mechanisms are among the measures recommended by this approach (7). In essence, Afghanistan's criminal policy must move away from mere criminalization and toward multi-level prevention, in which education, technology, and law operate simultaneously.

In summary, the theoretical framework of this study rests on the assumption that an effective criminal policy toward cybercrime requires synergy among social control, rational choice, and social learning theories. From this perspective, prevention is not merely a matter of punishment or restricting access, but a multidimensional process that includes promoting digital culture, enhancing the capacities of formal institutions, and rebuilding public trust in the criminal justice system. In Afghanistan, the transition from a reactive to a proactive criminal policy will be possible only when legislative, executive, and educational institutions are harmonized and criminal policy becomes an instrument for developing human security in the digital sphere.

Legal and Institutional Context of Afghanistan's Criminal Policy

In Afghanistan, the increase in internet access—now covering more than half of the population—combined with weak user awareness and inadequate security infrastructures, has turned the country into an attractive target for cybercriminals (4). Afghanistan's criminal policy, which is predominantly reactive and based on criminalization, represents an attempt to confront these threats, but its implementation faces legal, institutional, and technical challenges. This article, using a descriptive–analytical approach, examines the legal and institutional framework of this policy and assesses the challenges of its implementation in preventing cybercrimes. The aim is to highlight the gap between legislative theory and executive practice in order to propose strategies for transitioning toward proactive prevention. This analysis is grounded in legal instruments, domestic reports, and criminological studies and shows that, although legislative progress has been made, executive inefficiency has severely limited the effectiveness of the policy.

The legal framework of Afghanistan's criminal policy for the prevention of cybercrimes is built upon a set of laws and regulations that have been developed since the 2010s in response to cyber threats. The Penal Code

(1397/2018), as the principal criminal instrument, criminalizes cybercrimes in a dedicated chapter (Chapter Seven, Articles 50–53) and covers elements such as unauthorized access to systems, data destruction, and misuse of personal information. This law provides for sanctions such as imprisonment from three to ten years and financial penalties equivalent to twice the damage caused (13). However, ambiguity in defining the mental elements of the offense—such as criminal intent in cyberattacks—and the lack of distinction between pure cybercrimes and mixed offenses (such as identity theft combined with traditional fraud) make its implementation difficult (5). The Law on Combating Cybercrimes (1395/2016), enacted by the Ministry of Information and the Ministry of Justice, is a more advanced step and focuses on preserving the integrity of information systems, ensuring cybersecurity, and preventing incidents. This instrument, in seven chapters, mandates international cooperation and criminalizes offenses such as cyber espionage and attacks on critical infrastructure (1). Despite this, its reactive focus—punishment after the fact—predominates over preventive measures, and the failure to accede to the Budapest Convention (2001) has restricted cross-border information exchange.

Media and communications regulations, supervised by the Ministry of Communications, play a supporting role within this framework. These regulations, which form part of the national cybersecurity policy (drafted before 2021), criminalize the dissemination of immoral content, online pornography, and the misuse of social media. For example, sharing private images without consent is punishable by up to five years' imprisonment (14). The national cybersecurity policy, with objectives such as improving infrastructures and mutual cooperation, targets offenses like online fraud and cyber extortion (15). Nevertheless, following the political changes of 2021, these regulations have increasingly shifted toward censorship and content control, overshadowing crime prevention. Overall, this legal framework reflects progress from traditional legislation toward cyber-oriented regulation, but inconsistencies between instruments—such as overlaps between the Penal Code and media regulations—and vague definitions of offense categories weaken its preventive implementation (16).

The institutions responsible for implementing this policy form a multi-layered network that, in theory, should ensure coordination between legislation and practice but in reality face structural constraints. The Ministry of Communications and Technology, as the central body, is charged with supervising communication networks and enforcing cyber regulations. Under the Constitution and the 2014 plan, this ministry is responsible for tracking online offenses and securing infrastructures (17). However, technical weaknesses—such as insufficient high-speed internet coverage in rural areas—have reduced its preventive capacity. The National Directorate of Security (NDS) plays a pivotal role in confronting cyber threats to national security and follows up on offenses such as cyber espionage and online terrorism (18). Before 2021, this directorate focused on banking and health systems and operationalized the warnings of the Security Council, but political instability has redirected its resources toward internal control.

Cyber police, under the Ministry of Interior, are responsible for detecting and prosecuting everyday cybercrimes such as online theft and extortion. This unit, equipped with basic training from police academies, attempts to reduce internet-related offenses, but the shortage of experts—many of whom are law graduates unfamiliar with electronic crimes—renders it ineffective (4). The Office of the Attorney General and the high courts, at the judicial stage, examine the elements of the offense under the Penal Code and impose sanctions. The prosecution service collects digital evidence, while the courts, by evaluating case files, determine the level of seriousness of offenses (5). The absence of specialized cyber chambers in the courts and the lack of judicial training on maintaining the chain of

custody for digital evidence prolong the process. Taken together, these institutions possess the potential for coordinated prevention, but the absence of shared protocols disrupts integrated implementation (16).

The challenges in implementing this policy stem mainly from institutional and technical weaknesses and distance prevention from becoming operational. First, overlapping competences between institutions have generated duplication; for example, both the Ministry of Communications and the National Directorate of Security supervise cyber tracking, leading to resource wastage and delays in response (15). Second, the lack of digital equipment and technical training has paralyzed executive capacity. Cyber police lack advanced tracking software, and judges, without knowledge of digital evidence, reject cases (19). The low level of digital literacy in society—where users employ weak passwords—renders users vulnerable and reduces reporting due to cultural fears. Third, the absence of a centralized digital database has made the analysis of crime patterns impossible; without centralized recording, there is no data-driven prevention (14). Finally, the lack of inter-ministerial and transnational cooperation leaves cross-border offenses unaddressed; without participation in cyber INTERPOL channels, Afghanistan cannot effectively pursue extradition of offenders (3).

These challenges are rooted in political and economic instability. After 2021, sanctions have cut budgets, and brain drain has reduced the number of cyber specialists. Comparison with the United States (with the CFAA and the FBI) or the United Kingdom (with the NCSC) highlights the gap: Afghanistan lacks specialized institutions and global partnerships (19). As a result, criminal policy has not progressed beyond a reactive stance, and proactive prevention—such as public education and security technologies—has been neglected.

Consequently, Afghanistan's criminal policy in preventing cybercrimes is legislatively advanced but executively ineffective. Revising laws to define offenses precisely, creating specialized cyber police units, acceding to the Budapest Convention, and investing in training are essential steps. Without stability, this policy will remain at the level of theory, and cybercrimes will continue to pose a persistent threat (5).

Research Method

In this study, in order to examine and assess the challenges in implementing Afghanistan's criminal policy for the prevention of cybercrimes, a descriptive–analytical approach has been employed. Within this approach, an attempt has been made first to analyze the existing situation and then to identify and examine the causes and factors that hinder the effective implementation of policies in the field of cybercrime prevention.

This research is descriptive–analytical in nature. Initially, the legal and institutional status related to Afghanistan's criminal policy in the area of cybercrimes is examined descriptively, and then the existing challenges and problems in implementing these policies are analyzed using comparative and cross-jurisdictional methods. In this process, careful comparative analysis with other countries has been used so that the strengths and weaknesses of Afghanistan's criminal policy in relation to cybercrimes can be clarified more precisely.

In this study, data have been collected through analytical review of legal texts. For this purpose, Afghan laws and regulations in the field of cybercrimes, including the Law on Cybercrimes (2016) and the Afghan Penal Code (2018), have been examined in detail. In addition, secondary data from official reports and international organizations such as UNODC (United Nations Office on Drugs and Crime) and ITU (International Telecommunication Union) have been used in order to obtain supplementary information on the global situation and the experiences of other countries in preventing cybercrimes. Furthermore, analytical sections of Amirzoy's doctoral dissertation have been employed as one of the main sources of research data.

In this research, comparative and inferential analytical methods have been used to analyze the data. Through the comparative method, the experiences and criminal policies of other countries such as Iran, India, and Turkey in combating cybercrimes have been compared with the current situation in Afghanistan. These comparisons enable the researcher to identify the strengths and weaknesses of different policies and to propose strategies for improving Afghanistan's criminal policy in this field. In addition, an inferential method has been applied to analyze the problems and challenges present in Afghanistan's criminal policies. In this way, the existing data and information are examined more precisely and in greater depth in order to reach valid and well-documented conclusions regarding the challenges of cybercrime prevention in Afghanistan.

This research has faced several limitations that may affect its findings and analytical results. The first limitation is the scarcity of precise statistical data on cybercrimes in Afghanistan. In particular, access to comprehensive and documented information on the incidence of cybercrimes and the course of their prosecution in the country is limited. The second limitation is Afghanistan's volatile political situation, which may lead to lack of access to reliable sources and rapid changes in domestic policies. The third limitation concerns difficulties in accessing relevant institutions within Afghanistan. Due to security and political challenges, access to various governmental and executive bodies for close data and information collection has been problematic.

Despite these limitations, the present study has endeavored to rely on the available credible sources and, by analyzing secondary data and international reports, to arrive at reliable findings regarding the challenges of Afghanistan's criminal policy in preventing cybercrimes.

Analysis and Findings

Current Status of the Implementation of Criminal Policy

Afghanistan's criminal policy in the field of cybercrime, although it has witnessed certain advances at the legislative level, faces profound challenges in implementation that have marginalized effective prevention. One salient aspect of the current situation is the relatively appropriate criminalization of cybercrimes reflected in legal instruments such as the Penal Code (2018) and the Law on Combating Cybercrimes (2016), which, however, lack strong enforcement backing. In Chapter Seven (Articles 50–53) of the Penal Code, offenses such as hacking, electronic fraud, identity theft, and dissemination of malware are criminalized, and proportionate sanctions such as imprisonment from three to ten years and financial penalties equivalent to twice the damage caused are prescribed (13). This criminalization is designed on the basis of the unique characteristics of cybercrimes—such as their transnational nature and speed of commission—and represents an effort to cover instances such as cyber espionage and attacks on critical infrastructure (5). Nevertheless, the absence of effective enforcement mechanisms has reduced this criminalization to a largely theoretical framework. For example, ambiguity surrounding the mental elements of the offense—such as proving criminal intent in denial-of-service attacks—and the lack of distinction between pure cybercrimes and hybrid offenses (such as identity theft combined with traditional fraud) lead to the dismissal of cases in the courts. Domestic reports indicate that more than 70 percent of cyber cases are closed due to insufficient digital evidence, a problem rooted in the absence of standard protocols for collecting electronic evidence (20).

The institutions charged with implementing criminal policy—such as cyber police (under the Ministry of Interior), the Office of the Attorney General, and the National Directorate of Security—struggle with inadequate expertise in

the digital domain. Cyber police, responsible for the detection and prosecution of everyday offenses such as online theft and extortion, lack trained human resources. Graduates of police academies are often unfamiliar with basic concepts of electronic crimes, and law school curricula do not adequately cover cyber issues (4). The prosecution service and the courts, operating without specialized cyber chambers, face serious difficulties in handling complex cases; judges who have received no formal training in digital evidence tend to rely primarily on physical evidence, which has reduced the conviction rate to less than 30 percent (16). Although the National Directorate of Security is active in confronting cyber threats against national security (such as cyber espionage), its predominant focus on political surveillance has weakened its technical specialization (18). This lack of expertise not only slows down crime detection but also renders prevention virtually impossible, since without digital forensic tools it is not feasible to trace criminal patterns.

The focus of criminal policy on punishment rather than prevention has rendered the dominant approach reactive and has sidelined proactive prevention. The Law on Combating Cybercrimes (2016), adopted by the Ministry of Information and the Ministry of Justice, relies mainly on post-offense reaction—such as the imposition of imprisonment and fines—and does not mandate preventive measures such as public education or the strengthening of infrastructures (1). This reactive orientation is rooted in Afghanistan's security priorities and is at odds with criminological theories such as Hirschi's social control theory, which emphasizes prevention through social bonds and education (7). As a result, cybercrime in Afghanistan is on the rise; informal statistics indicate a 40 percent increase in online fraud during 2024–2025, without any corresponding preventive response in criminal policy (19).

Analysis of the Causes of Ineffectiveness

The ineffectiveness of Afghanistan's criminal policy in preventing cybercrimes stems from multilayered causes ranging from structural weaknesses to cultural and political factors. First, weak technological infrastructure is one of the principal causes. Afghanistan's internet networks, characterized by inadequate coverage and low speeds, are insecure and lack standard encryption protocols. The Ministry of Communications and Technology, which is responsible for ensuring cybersecurity, does not possess the necessary equipment to trace attacks, and digital forensic centers—needed to analyze evidence such as server logs—are virtually non-existent (17). This weakness makes it impossible to detect offenses such as malware dissemination; for example, denial-of-service attacks against banks leave no trace in the absence of appropriate technical tools (19). In addition, the lack of secure infrastructures pushes users toward public networks, which has raised the rate of information theft to 60 percent (16). These technical factors confine criminal policy to ex post reaction and eliminate opportunities for early intervention.

Second, the shortage of specialized personnel in the police and prosecution services is another major challenge. Cyber police officers, who have graduated from traditional academies, are unfamiliar with advanced concepts such as social engineering or big data analysis (4). Prosecutors, lacking training in cyber law, are unable to establish the elements of the offense; for instance, in online extortion cases, the absence of expertise in maintaining the chain of custody for digital evidence leads to the acquittal of defendants (5). This shortage is rooted in inadequate university curricula; legal course materials do not cover cybercrimes, and graduates are scarcely familiar even with the terminology of electronic crime (16). The result is a low rate of prosecution (less than 20 percent) and an expansion of the "dark figure" of crime, which makes criminal policy appear ineffective.

Third, the lack of public education and cyber awareness has turned users into easy victims. The majority of Afghans, without basic knowledge such as choosing strong passwords or recognizing phishing attempts, are exposed to fraud (20). The media and state institutions do not provide sufficient information, and awareness campaigns, due to political constraints, are largely limited to major cities (15). This gap corresponds with Sutherland's social learning theory, which emphasizes education to prevent criminal modeling and imitation (21). Without public awareness, preventing offenses such as the misuse of social media is impossible, and criminal policy alone cannot compensate for this deficit.

Fourth, weak international cooperation—particularly the absence of accession to the Budapest Convention—has left transnational offenses inadequately addressed. Without joining this convention, Afghanistan cannot effectively facilitate extradition or the exchange of technical information (1). Post-2021 sanctions have curtailed cooperation with INTERPOL, leaving cyberattacks originating from abroad without meaningful response (3). This isolation confines criminal policy within a purely domestic framework and undermines its effectiveness.

Fifth, the prioritization of national and political security over digital security has diverted resources. This prioritization, exemplified by internet shutdowns in 2025, has weakened prevention and increased hidden criminality. Consequently, criminal policy has drifted away from its preventive function and has been transformed into a political instrument.

Comparative Analysis

A comparative analysis of the criminal policies of similar countries in the region—such as Iran, Pakistan, and India—shows that the prevention of cybercrime requires multi-institutional coordination, whereas Afghanistan lags behind in this respect. In Iran, the Computer Crimes Law (2009), together with amendments adopted by 2025, provides extensive criminalization, and institutions such as the cyber police (under the national police force) and specialized cyber prosecution units focus on prevention; however, challenges such as the 2025 internet blackouts and the "Untrue Content" legislation have pushed the approach toward reaction and repression. In Pakistan, the Prevention of Electronic Crimes (Amendment) Act 2025 criminalizes a broad range of conduct and designates the Pakistan Telecommunication Authority (PTA) as the implementing body, yet threats to freedom of expression and overlapping competencies among institutions reduce effectiveness. In India, the Information Technology Act 2000 and the 2025 reforms (including the Digital Personal Data Protection Act) have empowered CERT-In as a multi-agency coordination center (government, private sector, police), with an emphasis on public education and preventive reporting; the crime detection rate in India is about 50 percent higher than in Afghanistan. These experiences underscore the necessity of coordination among ministries, investment in training, and accession to global instruments (such as the 2025 UN Convention against Cybercrime), all of which Afghanistan lacks.

Afghanistan has made progress at the legislative level and has developed relatively appropriate criminalization of cyber offenses, but its operational criminal policy lacks practical and preventive effectiveness. Technical, human, and international weaknesses have kept the approach reactive and have thwarted preventive efforts. Without structural reforms, this policy cannot keep pace with evolving cyber threats.

Discussion

The findings of this study, which focus on the challenges of implementing Afghanistan's criminal policy in preventing cybercrimes, align with the criminological theories presented in the second chapter of the dissertation.

This alignment clarifies the gap between theoretical frameworks and practical realities, and underscores the need for redesigning the system to move from a reactive to a proactive model. The analysis is based on a descriptive–analytical review of legal documents and domestic reports.

Hirschi's social control theory, which views deviance as the result of weak social bonds (attachment, commitment, involvement, and belief in norms), is consistent with the dysfunction of formal institutions in Afghanistan (7). Institutions such as cyber police and the prosecution service lack preventive capacity; the weakness of training in police academies leaves users vulnerable, without "involvement" in safe practices (4). This corresponds to Durkheim's view that deviance arises from the breakdown of norms; in Afghanistan, weak oversight of cyberspace has increased offenses such as online pornography, and more than 60 percent of victims refrain from reporting due to a lack of trust in institutions (9, 15).

Clarke and Cornish's rational choice theory conceives offending as a cost–benefit calculation by the offender (11), which corresponds to the lack of real deterrence in Afghanistan. Low detection rates (less than 20 percent), due to the absence of tracing tools, reduce the cost of crime; hackers, aware of police weaknesses, carry out attacks without fear (3). This neutralizes deterrence and encourages offenders to exploit uninformed users (5, 8).

Sutherland's social learning theory conceptualizes delinquency as the result of modeling based on differential associations (22), and this is consistent with a public culture that pays little attention to cybercrime. Low levels of digital literacy (below 40 percent) push users toward reproducing criminal patterns; the media fail to provide adequate information, and young people learn fraud techniques from messaging groups and online networks (16, 21). This has raised the dark figure of crime to around 80 percent and rendered prevention virtually impossible (14).

Examining the Gap Between "Legislative Criminal Policy" and "Executive Criminal Policy"

The gap between legislative and executive dimensions constitutes one of the main obstacles to prevention. The Penal Code (2018) and the Cybercrimes Law (2016) provide comprehensive criminalization of hacking and identity theft and prescribe proportionate sanctions (1). The National Cybersecurity Policy also emphasizes prevention (15). However, implementation lacks the necessary tools; ambiguity surrounding digital evidence leads to the closure of cases and has contributed to a 40 percent growth in cybercrime in 2024–2025 (19). After 2021, regulations shifted toward censorship, deepening the gap (17). Bridging this divide requires executive by-laws such as forensic protocols and detailed implementing regulations (5).

Analysis of the Role of Politics and Power Structures in the Functioning of Judicial Institutions

Politics and power structures have turned judicial institutions into political instruments and weakened their independence. Political oversight has eroded public trust and reduced conviction rates to below 30 percent (7). Overlapping competences between the National Directorate of Security and the Ministry of Communications have produced duplication and placed judges under pressure (15). The 2025 internet shutdowns increased repression instead of strengthening judicial capacity (16). Reform requires the separation of powers and training directed toward judicial independence.

Accordingly, to move from a reactive to a proactive approach, institutional redesign of the criminal justice system is essential. This includes accession to the Budapest Convention, the creation of specialized cyber police structures, and national awareness campaigns so that theoretical frameworks can be operationalized. Without the political will

to ensure coordination, criminal policy will remain at the legislative level, and cybercrimes will continue to pose a persistent threat.

Policy Recommendations

Given the problems identified in the implementation of Afghanistan's criminal policies for preventing cybercrimes—such as weak infrastructures, lack of expertise, and a reactive orientation—the proposed policy recommendations are structured across three time horizons: short term, medium term, and long term. These strategies focus in particular on revising existing laws, strengthening enforcement institutions, and enhancing public awareness, with the overall objective of reducing cybercrime to a manageable level.

Short-Term Horizon (1 to 2 Years)

In this time frame, the focus should be on rapid and low-cost measures to reinforce existing capacities. The first step is specialized training for judicial officials, police officers, and lawyers in the field of cyber law and digital evidence. Organizing continuous training courses for judges, prosecutors, and lawyers on how to collect, preserve, and analyze digital evidence can increase conviction rates from less than 30 percent to around 50 percent. In addition, specialized training on detecting offenses such as phishing and social engineering should be incorporated into the curricula of police academies for cyber police units under the Ministry of Interior.

The next step is drafting protective guidelines for data and digital evidence. Establishing national protocols to preserve the chain of custody for digital evidence—such as server logs and screenshots—is crucial and can reduce legal ambiguities. These guidelines should also guarantee the protection of individuals' privacy and specify immediate sanctions for violations of that privacy.

Furthermore, the creation of joint working groups among the police, prosecution service, and Ministry of Communications can reduce duplication and facilitate the exchange of information needed to trace transnational offenses. This measure would help mitigate jurisdictional overlaps and enhance crime detection.

Medium-Term Horizon (3 to 5 Years)

In this period, it is necessary to strengthen institutional structures in order to ensure the sustainability of policy implementation. The first step is to establish a National Cybercrime Center responsible for tracking and conducting digital forensics in cybercrime cases. This center should initially be equipped with basic tools such as tracing software and experts in preventing attacks on the country's critical infrastructures, including banking systems.

In addition, the creation of secure information-sharing networks among ministries and governmental bodies can strengthen both national and international cooperation. Such networks can assist in analyzing and identifying complex offenses such as cyber extortion and attacks on critical infrastructure.

Moreover, updating existing laws in line with international standards—particularly regarding new concepts and definitions of cybercrimes, including cyberterrorism and identity theft—can fill legal gaps and provide a more effective framework for combating cybercrime.

Long-Term Horizon (5 to 10 Years)

In this time horizon, the focus should be on achieving structural and cultural transformation to ensure sustainable prevention of cybercrimes. Drafting a comprehensive national policy for the prevention of cybercrime, incorporating

proactive measures such as smart filtering and monitoring of social media, can help reduce system and user vulnerability and potentially bring cybercrime down to below 10 percent of current levels.

Strengthening international cooperation and joining global conventions such as the Budapest Convention can facilitate extradition of offenders and the exchange of technical information among countries. Establishing a national information-exchange center with organizations such as INTERPOL and Europol would also be effective in countering transnational offenses and cyberattacks originating from neighboring states.

Finally, improving public cyber literacy and integrating cybercrime-related topics into school and university curricula can contribute to embedding a culture of cybercrime prevention. Media campaigns can be used to raise public awareness and promote safer online behavior.

Balanced implementation of these strategies can help Afghanistan's criminal policy overcome current challenges and guide the country toward sustainable cybersecurity. However, the success of these measures depends on political will and international support.

Conclusion

The present study examines the challenges of implementing Afghanistan's criminal policy in preventing cybercrimes and seeks to clarify the gaps between the country's legislative and executive policies. Given the rapid expansion of information technology and the increasing use of the internet in Afghanistan, cybercrimes have become a serious threat to public and economic security. In this context, the article analyzes the current situation, identifies key problems, and outlines proposed solutions.

(a) Challenges of Afghanistan's Criminal Policy Toward Cybercrimes

Afghanistan's criminal policy regarding cybercrimes is predominantly reactive rather than proactive. In other words, the main focus is on punishment after the commission of the offense, while preventive policies receive minimal attention. Despite the enactment of laws such as the Cybercrimes Law and the Afghan Penal Code, in practice these instruments face significant implementation problems. Weak coordination among institutions, a shortage of technical expertise, and limited technological resources—particularly in terms of specialized human capital—have prevented the realization of policy objectives. In addition, the absence of appropriate training at both the public level and within enforcement bodies has increased user vulnerability and contributed to the incidence of cybercrimes.

(b) Executive and Institutional Weaknesses

Institutions responsible for implementing criminal policy in Afghanistan, such as cyber police, the prosecution service, and the National Directorate of Security, face serious difficulties. A lack of technical specialists and the absence of necessary equipment and infrastructures for tracing and analyzing digital data have resulted in delayed and ineffective detection and prosecution of cybercrimes. Moreover, insufficient specialized training in police academies and universities has left many judicial officials and police officers unable to collect and analyze digital evidence. This has weakened judicial processes and contributed to low conviction rates in cybercrime cases.

(c) Proposed Solutions

To address the existing challenges and improve Afghanistan's criminal policy toward cybercrimes, fundamental changes are needed at legislative, executive, and cultural levels. In the short term (1 to 2 years), emphasis should be placed on specialized training for judicial officials and police in the field of cyber law and digital evidence. Drafting protective guidelines for preserving digital evidence and strengthening cooperation among different governmental

institutions can also improve the efficiency of judicial and enforcement systems. In the medium term (3 to 5 years), establishing a national cybercrime center and reinforcing technical infrastructures can help reduce the incidence of cybercrimes and increase detection rates. In the long term (5 to 10 years), enhancing international cooperation, acceding to global conventions such as the Budapest Convention, and promoting public cyber literacy through educational programs can contribute to reducing cyber threats.

In conclusion, the study shows that Afghanistan's criminal policy in the field of cybercrimes has achieved limited success in prevention due to a shortage of human resources, technical weaknesses, and a lack of coordination among various institutions. To develop an effective criminal policy, Afghanistan must shift from a reactive to a preventive approach. Strengthening enforcement institutions, improving public education, employing modern technologies in crime detection, and expanding international cooperation can help reduce cybercrimes and enhance digital security in the country.

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 adheried 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. Beigi A. The Impact of Cyberspace on Security from Legal, Social, Political, and Military Perspectives. Tehran: Fānoos-e Donya Publishing; 2019.
2. Bergmann MC, Dreißigacker A, von Skarczinski B, Wollinger GR. Cyber-Dependent Crime Victimization: The Same Risk for Everyone? Cyberpsychology, Behavior, and Social Networking. 2018;21(2):73. doi: 10.1089/cyber.2016.0727.
3. Langton S, Dixon A, Farrell G. Six months in: Pandemic crime trends in England and Wales. Crime Science. 2021;10:6-7. doi: 10.1186/s40163-021-00142-z.
4. Afshari B. The Aims and Effects of Cybercrimes and Protective Rules for their Prevention, and the Impact of Cybercrimes on the Economic Cycle Security. Legal Studies Quarterly. 2023;33(4):74.

5. Bakhtiyari AF. Analysis of the Constituent Elements of Cybercrimes in Light of the Penal Code of Afghanistan2019.
6. Payne KL, Russell A, Mills R, Maras K, Rai D, Brosnan M. Is There a Relationship Between Cyber-Dependent Crime, Autistic-Like Traits and Autism? Journal of Autism and Developmental Disorders. 2019;49(10):4. doi: 10.1007/s10803-019-04119-5.
7. Sotoudeh H. Social Pathology (Sociology of Deviance). Tehran: Āvā-ye Nūr Publications; 2020.
8. Wordu H, Uche C, Wali CB. Influence of computer-related crimes on adolescent delinquency among secondary school students in Obio-Akpor local government area rivers State. International Journal of Contemporary Academic Research. 2022;3(1):61.
9. Zolrahim R, Imani P, Baybourdi K, Salehpour M, Banihashem Z, Lashgari L, editors. Investigating Social Control and Related Theories in Crime Prevention. The 18th National Conference on Law, Social Sciences and Humanities, Psychology, and Counseling; 2024; Shirvan.
10. Ehsani K. An Introduction to Crime Prevention. Kabul: Amiri Publications; 2018.
11. Radda'ee M. Investigating Criminological Theories in the Formation of Cybercrime. Iranian Political Sociology Quarterly. 2019;2(4):12.
12. Khader M, Weistinchai Xiao T, Neulosenk. An Introduction to Cyber Forensic Psychology: Understanding the Minds of Cyber Deviants: Global Scientific Publications; 2021.
13. Hosseini SM, Ghazi H. Specific Criminal Law 3. Kabul: Asia Foundation Afghanistan; 2019.
14. Rezaei GM, Mohammadi A. Crimes Against Dignity in the Penal Law of Afghanistan: Kateb University Publications; 2018.
15. Haqqani JA, Badakhsh LM. Criminal Policy and Methods of Crime Prevention in Afghanistan. Law and Penalty Quarterly. 2022(2):8.
16. Ansari J, Attazadeh S, Ghayyoomzadeh M. The Criminal Policy of Iran and the U.S. Regarding Cyber Fraud and Theft Crimes. Information and Criminal Research Quarterly. 2019;14(55):136-7.
17. Emami A. Europol's Measures in Combating Cybercrimes. 2022.
18. Hamidi H. Cyber Espionage Crime in the Law of Afghanistan and Iran. Scientific-Research Quarterly of Legal Knowledge. 2024;10(4):157. doi: 10.62134/srqjl/v2.i4.202409.6.
19. Walczak S. Predicting Crime and Other Uses of Neural Networks in Police Decision Making. Frontiers in Psychology. 2021;12:31. doi: 10.3389/fpsyg.2021.587943.
20. Rasouli M, Mohammadi SB. Afghanistan's Judicial Criminal Policy Regarding Sexual Assault Crimes Against Women. Bimonthly Findings in Criminal Law and Criminology. 2023(7).
21. Javadi Hosseinabadi H, Aghababai Taghanaki A. Criminological Analysis of Governmental Crime from the Perspective of Learning Theory. Ārā' Journal Quarterly. 2021;4(8):23.
22. Maloku A. "Theory of Differential Association". Academic Journal of Interdisciplinary Studies. 2020;9(1):78. doi: 10.36941/ajis-2020-0015.