Comparative Analysis of Afghanistan's Criminal Policy and the Policies of Budapest Convention Member States in Responding to Cybercrimes

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

*Correspondence: Mahdi.esmaeili@iaustb.ac.ir

Abstract

With the expansion of information technology and the growing dependence of societies on cyberspace, cybercrimes have become one of the principal challenges faced by legal systems. Afghanistan, too, in the last decade—due to the rapid increase in Internet accessibility—has witnessed a significant rise in such offenses. The main objective of this study is to examine and evaluate Afghanistan's criminal policy regarding cybercrimes and its level of alignment with international standards and instruments. The research method is descriptive–analytical and is based on documented legal data, national and international instruments, and content analysis of the Law on Combating Cybercrimes (2014) and the Penal Code (2017). The findings indicate that Afghanistan's criminal policy toward cybercrimes is predominantly reactive, focusing on punishment and post-crime control rather than prevention and education. Despite the partial criminalization of digital behaviors and the establishment of institutions such as the Cyber Police, the legislative and institutional framework of the country suffers from shortcomings, including lack of coordination among agencies, shortages of specialized personnel, and technological underdevelopment. Moreover, Afghanistan's alignment with international instruments such as the Budapest Convention remains limited and requires substantial reform and revision. The conclusion demonstrates that for an effective cyber-criminal policy, Afghanistan must shift from a reactive to a proactive and preventive approach, expand its international cooperation, and emphasize public education and the strengthening of specialized institutions.

Keywords: Cybercrimes, Criminal Policy, Afghanistan, Penal Law, Budapest Convention

Received: 02 August 2025
Revised: 07 December 2025
Accepted: 14 December 2025
Initial Publication 16 December 2025
Final Publication 01 June 2026

Citation: Amirzoy, M. K., Esmaeili, M., & Tadayyon, A. (2026). Comparative Analysis of Afghanistan's Criminal Policy and the Policies of Budapest Convention Member States in Responding to Cybercrimes. *Legal Studies in Digital Age,* 5(2), 1-15.

1. Introduction

Cybercrimes are a modern phenomenon in the communication era that have expanded significantly with the development of information technologies and the emergence of the Internet. The integration of computer technology and telecommunications

has created a new environment known as "cyberspace," distinguished from physical spaces by characteristics such as speed, vastness, and the absence of geographical boundaries (Sobhkhīz, 2019). While this space has introduced unprecedented opportunities in scientific, economic, and social domains, it has simultaneously produced new threats for committing crimes, whereby many traditional offenses now appear in new and complex forms within cyberspace (Walczak, 2021). The remarkable advancement of information technology has brought humanity into a realm where data transmission and human interaction occur without physical movement. With the expansion of global communication networks, this environment has produced a new virtual lifestyle in which human, economic, and cultural interactions have undergone fundamental transformation (Beigī, 2019). Thus, cybercrimes constitute a new generation of offenses committed using electronic tools and Internet networks, including acts such as hacking, online fraud, and data theft (Ahmadi, 2019).

As a developing nation, Afghanistan has become increasingly exposed to cyber threats with its entry into the digital age and the rising use of the Internet. Weak security infrastructures, the absence of comprehensive laws, and the lack of specialized institutions for combating cybercrimes have transformed the country into a primary target for cybercriminals (Maleksha'ār & Tadayyun, 2019). Following warnings from the Security Council and the growth of cyberattacks on sensitive institutions, Afghanistan enacted the "Law on Combating Cybercrimes" in 2014 to enhance virtual security and promote international cooperation; however, deficiencies in implementation and shortages of specialized personnel have hindered its effectiveness (Bakhtiyārī, 2019).

Despite the adoption of multiple laws—such as the Penal Code and the Law on Combating Cybercrimes—the rate of cyber offenses in Afghanistan continues to rise. The lack of alignment between the country's criminal policy and international developments, alongside weaknesses in prevention and crime detection, highlights the necessity of revising Afghanistan's criminal justice approach. This issue is particularly important because Afghanistan ranks among the countries with the highest cyber vulnerability, according to the Global Cybersecurity Index (Bakhtārī, 2023).

The main question of this study is the extent to which Afghanistan's criminal policy toward cybercrimes is effective and whether it aligns with international instruments and the experiences of developed countries. The primary objective of this article is to explain and analyze the diverse dimensions of Afghanistan's criminal policy in the field of cybercrimes, evaluate its strengths and weaknesses, and compare it with the criminal policies of Budapest Convention member states. Using a descriptive–analytical method and relying on national and international legal sources, this study aims to determine whether Afghanistan's criminal policy toward cybercrimes is proactive or reactive and to assess its effectiveness in ensuring virtual security (Beigī, 2019).

2. Theoretical and Conceptual Foundations

2.1. The Concept of Cybercrimes

a) Linguistic and legal definition of "cyber"

Linguistically, the term "cyber" denotes "virtual" or "non-tangible," and in technical and legal contexts, it refers to an environment where human and data interactions occur through communication technologies without geographical limitations. In Afghan law, the term refers to the virtual space created through tools such as computers, mobile phones, or tablets, enabling the exchange of information (Maleksha'ār & Tadayyun, 2019). Legally, any criminal conduct committed through technology within a virtual environment that violates recognized rights of individuals is categorized as a cybercrime.

b) Composite and nominal concepts of cybercrimes

In the composite sense, cybercrimes refer to offenses that combine multiple cyber or non-cyber criminal acts simultaneously or sequentially to achieve complex criminal objectives. (Raddā'ī, 2019).

Conversely, in the nominal sense, cybercrimes encompass all criminal activities carried out using computers, Internet networks, or virtual environments, including hacking, online fraud, virus dissemination, and data theft (Mīrmurādī, 2020).

c) Distinguishing cybercrimes from traditional crimes

Cybercrimes possess features that differentiate them from traditional crimes, such as transnationality, anonymity of offenders, speed and ease of commission, low cost, and difficulties in detection and judicial prosecution (Walczak, 2021). Additionally, while offenders and victims in traditional crimes typically interact physically, cybercrimes occur without physical contact and across international borders, complicating identification and prosecution and compelling governments to reassess their criminal policies.

2.2. Historical Development of Cybercrimes

a) Global origins of cybercrimes

Determining the exact date of the first cybercrime is difficult, but its roots can be traced back to the 1970s when initial attacks on telephone and computer systems occurred and the concept of "hacking" emerged. With the expansion of computers in the 1980s, crimes involving unauthorized access, data theft, and digital sabotage increased (Sobhkhīz, 2019).

Generally, the evolution of cybercrimes can be categorized into three generations:

1. **First generation:** early offenses such as data theft and violations of privacy until the late 1980s.
2. **Second generation:** crimes targeting data and information infrastructures with the rise of global networks in the 1990s.
3. **Third generation:** purely cyber-based crimes in the 2000s that became global threats to information security (Mahdavī Sābet & Abdullāhī, 2020).

b) Emergence of cybercrimes in Afghanistan

In Afghanistan, cybercrimes emerged alongside the rapid spread of the Internet and social networks in the past decade. Growing numbers of users and insufficient awareness of safe technological use facilitated the proliferation of hacking, online threats, extortion, and cyber theft (Maleksha'ār & Tadayyun, 2019).

In response, Afghanistan passed the "Law on Combating Cybercrimes" in 2014 to protect information security and promote international cooperation. However, shortages of specialized staff, weak enforcement, and insufficient university-level training in cyber law remain major challenges (Bakhtiyārī, 2019).

2.3. Relevant Criminological Theories

a) Social Control Theory

Social control theory is one of the foundational criminological perspectives explaining criminal behavior. Hirschi argues that human beings naturally tend toward deviance, and only social controls—attachment, commitment, involvement, and belief—prevent criminal behavior (Sutūdeh, 2020). Durkheim, similarly, viewed deviance as a normal social phenomenon and believed that weakness in social cohesion and norms increases delinquency. Complementary theories such as Reckless's containment theory and Matza's social drift theory also emphasize internal and external controls in preventing deviance (Ghā'emī et al., 2024; Tāj Khorāsānī et al., 2021).

In the cybercrime context, this theory suggests that weakened institutional and social oversight in cyberspace increases both motivation and opportunity for offending.

b) Rational Choice Theory

Rational choice theory assumes that offenders make decisions after evaluating the costs and benefits of committing a crime. If the perceived benefits exceed the risks of being detected and punished, the action is considered "rational" (Wordu et al., 2022).

This theory is highly relevant to cybercrimes because offenders are often skilled and calculative individuals who act based on risk analysis. Therefore, increasing the costs of cyber offending—through technical and legal measures—can effectively reduce cybercrime rates (Raddā'ī, 2019).

c) Social Learning Theory

According to Sutherland's social learning theory, criminal behavior is acquired through association and interaction with others. Individuals learn not only techniques of offending but also the attitudes and justifications that legitimize it (Javādī Ḥosaynābādī & Āghābābā'ī Ṭāghānakī, 2021).

Later extensions of the theory, such as Akers's differential reinforcement perspective, show that learning criminal behavior can occur in virtual environments, where users acquire technical skills and moral justifications for cyber offending through social networks and online communities (Mīrmurādī, 2020).

Overall, the three theories complement one another: social control theory highlights weak oversight and weakened social bonds; rational choice theory stresses calculated cost–benefit analysis; and social learning theory focuses on digital socialization processes that facilitate cyber offending.

The combination of these perspectives demonstrates that an effective criminal policy for combating cybercrimes must strengthen social control and public education, increase the costs of offending, and reshape cultural attitudes toward virtual behaviors.

3. Characteristics and Causes of the Emergence of Cybercrimes

3.1. Characteristics

a) Transnational nature

One of the most prominent characteristics of cybercrimes is their transnational nature. These types of crimes are not confined to geographical borders and occur in an environment that is not physically controllable. According to Articles 5, 6, and 7 of the Statute of the International Criminal Court, such crimes are classified among international crimes (Ghā'emī et al., 2024). Cyberspace makes it possible for an individual in one country to commit an offense whose result appears in another country without any need for physical presence. This characteristic has led to the conclusion that combating cybercrimes requires judicial and security cooperation between states.

b) Concealment of the offender's identity

In cyberspace, offenders can easily act under false or anonymous identities. The lack of effective control over the virtual environment has made it possible for the perpetrator to access computer systems from any point in the world without revealing their real identity. In many cases, the offender uses public computers and networks such as internet cafés or intermediary servers to conceal their digital trail (Ghā'emī et al., 2024). This concealment of identity has turned the identification and criminal prosecution of the offender into a major challenge for security and judicial institutions.

c) Speed and ease of commission

In cybercrimes, the commission of the offense requires very little time; sometimes, with a single click or the pressing of a key, a large-scale violation at the global level may occur. The commission of crimes in cyberspace can take place in a fraction of a second, and because no physical presence is required, the ease of commission is extremely high. Offenders, having access to a computer connected to the internet and a minimal level of technical knowledge, can cause enormous damage (Ghā'emī et al., 2024). Consequently, these characteristics of cybercrimes increase the risk of crime occurrence and make effective prevention difficult.

d) High dark figure and difficulty of detection

Many cybercrimes are never identified or reported. The reasons for this include the concealed manner of commission, the victims' lack of awareness, and the absence of technical tools for crime detection. In addition, the electronic nature of data means that traces of the crime can be quickly deleted or altered. For this reason, the dark figure of cybercrimes is much higher than that of traditional crimes, and their detection requires technical expertise and international cooperation (Ghā'emī et al., 2024).

3.2. Objectives of Committing Cybercrimes

a) Financial objectives

A large portion of cybercrimes are committed with financial motives. Hackers infiltrate banking systems or steal credit card information in order to make unauthorized withdrawals of funds. Moreover, internet fraud and digital extortion are among the most common forms of these crimes (Anṣārī et al., 2019). The principal objective of the offender in this category is to obtain personal gain by exploiting security weaknesses in systems and users.

b) Political and security objectives

Some cybercrimes are committed with political or security motives, such as infiltrating governmental systems, cyberattacks against critical infrastructure, or digital espionage. These types of crimes are often carried out by political groups, terrorist organizations, or even states and can threaten the national security and stability of a country (Anṣārī et al., 2019). Such attacks are considered part of the new information wars in which technology becomes an instrument of power and destruction.

c) Social and psychological objectives

In some cases, the offender's motive is neither financial nor political but rooted in psychological and social factors. Individuals may commit crimes to satisfy curiosity, seek excitement, or prove their ability to penetrate systems. Likewise, feelings of revenge or the desire to damage another person's social reputation are among the common psychological factors in these crimes (Anṣārī et al., 2019).

d) Personal and retaliatory objectives

A portion of cybercrimes has a personal dimension and is usually committed following personal disputes or conflicts. The publication of images or private information on social networks, threats to disclose secrets, or hacking user accounts for the purpose of revenge are among such cases (Anṣārī et al., 2019).

3.3. Factors Contributing to the Expansion of Cybercrimes

a) Socio-cultural factors

From a sociological perspective, weak culture in the use of technology and the lack of public awareness of the risks of cyberspace are among the important factors contributing to the expansion of cybercrimes. In many societies, including Afghanistan, users do not possess the necessary skills to protect their information, which makes them vulnerable to offenders (Bakhtārī, 2023). In addition, the decline of family supervision, cultural disorders, and moral crises arising from globalization also influence the increase of these crimes.

b) Economic factors

Unfavorable economic conditions, unemployment, and financial inequalities may push individuals toward committing cybercrimes. In cyberspace, due to the low cost of committing an offense and the high financial returns, offenders have greater motivation to engage in criminal activity. Moreover, the financial attractiveness of illegal activities on the internet—such as digital fraud—has intensified this trend (Bakhtārī, 2023).

c) Technological factors

The rapid growth of technology and weaknesses in the control and securing of information systems are technological factors that contribute to the spread of cybercrimes. The absence of strong cyber-defense systems, up-to-date security software, and robust digital infrastructure creates favorable opportunities for hackers and offenders (Bakhtārī, 2023). The more societies rely on technology, the higher their level of vulnerability becomes.

d) Legal–political factors

In many countries, including Afghanistan, weaknesses in legislation, failure to accede to international conventions such as the Budapest Convention, and the absence of a judicial system equipped with cyber experts are considered major obstacles to combating cybercrimes (Bakhtiyārī, 2019). Legal gaps and inefficiencies in the enforcement of laws have led offenders to feel immune from punishment, with a consequent rise in crime in this domain.

Therefore, the specific characteristics of cybercrimes—including their transnational nature, the concealment of the offender's identity, and the ease of commission—have caused these crimes to escape the control of national judicial systems. In Afghanistan, weak security and legal infrastructures, together with social, economic, and cultural factors, have created a broad foundation for the occurrence and expansion of such crimes. Accordingly, strengthening cyber education, updating legislation, and developing international cooperation are among the most important strategies for confronting this phenomenon.

4. Legal and Regulatory Framework of Cybercrimes in Afghanistan

4.1. National laws and regulations

a) Law on Combating Cybercrimes (2014)

With the growth of information technology and the expansion of public access to the internet in Afghanistan, the need for specific legislation in the field of cybercrimes was increasingly felt. In this context, the Government of Afghanistan enacted the "Law on Combating Cybercrimes" in 2014. The main objective of this law was declared to be securing the digital environment, protecting users' data, and guaranteeing the integrity of the country's information networks (Bakhtiyārī, 2019).

This law is organized in seven chapters and fifty-three articles and covers a wide range of cybercrimes. Among its most important sections are the definition of offenses related to unauthorized access, data destruction, internet fraud, crimes against privacy, and offenses affecting national security. Under this law, the Ministry of Communications and Information Technology is designated as the competent authority for dealing with cybercrimes.

According to the law, the state is obliged to adopt the necessary technical and legal measures to prevent the occurrence of cybercrimes, ensure the integrity of communication networks, and protect users' information. International cooperation with other countries and global organizations in the detection and prosecution of cybercrimes is also emphasized (Bakhtiyārī, 2019).

Despite this structure, the implementation of the law has faced serious difficulties. The responsible institutions, including the Ministry of Justice and judicial and prosecutorial bodies, lack the facilities and technical expertise needed for the effective application of the provisions of this law. For this reason, despite formal criminalization, the rate of cybercrime in the country has been on the rise, and many cases are closed due to the lack of sufficient digital evidence (Maleksha'ār & Tadayyun, 2019).

Moreover, certain concepts in this law are stated in general and ambiguous terms. For example, terms such as "electronic data" or "information systems" are mentioned without precise legal definitions, which creates problems in interpretation and enforcement. This ambiguity has led judicial authorities to experience confusion in determining the type of crime, the competence of courts, and the appropriate punishment (Bakhtiyārī, 2019).

b) Relevant provisions in the Penal Code

Alongside the standalone Law on Combating Cybercrimes, the Afghan Penal Code also addresses such crimes in several chapters. In this Code, the legislator has attempted to criminalize behaviors related to cyberspace under various headings. Among the most important provisions is Article 860, which is dedicated to the offense of computer theft; under this article, any unauthorized access to electronic information and data and their misuse is considered a criminal act (Ahmadi, 2019).

In addition, provisions concerning electronic fraud, digital forgery, cyber espionage, electronic terrorism, dissemination of false information, and violation of intellectual property rights on the internet are also foreseen in the Penal Code. In this part, the legislator has sought to incorporate the instances of emerging crimes within the framework of general criminal provisions.

Nevertheless, studies show that the Penal Code lacks the necessary comprehensiveness with regard to cybercrimes. In many instances, instead of defining the offense, the legislator merely lists certain instances. For example, instead of providing a precise definition of "cyberterrorism," the Code is content with describing only one of its manifestations. Furthermore, the mental element of the offense is not clearly set out in many provisions, causing different acts of varying gravity to be subsumed under a single criminal title in judicial interpretation (Bakhtiyārī, 2019).

In other words, although the purpose of the Penal Code has been to create a systematic framework for combating computer-related crimes, the failure to distinguish clearly between technical and legal concepts—such as between "unauthorized access" and "data destruction"—has led to conceptual overlap and weakness in the practical application of the law (Ahmadi, 2019).

c) Other laws related to national security

In addition to the two aforementioned laws, several other national regulations are indirectly related to cybercrimes. Among them is the Law on Crimes against the Security of Afghanistan, which classifies some instances of cyberattacks that damage the country's critical and military infrastructure as crimes against national security. Furthermore, regulations concerning the protection of governmental information, telecommunications, and state secrets exist, which can be invoked in support of the country's cyber security (Bakhtiyārī, 2019).

Although these laws are drafted in a scattered and subject-specific manner, they collectively reflect the Afghan legislator's efforts to harmonize domestic criminal policy with new threats arising in cyberspace. Nonetheless, the absence of an integrated legal system and the lack of coordination among executive and judicial bodies have prevented the effective realization of the objectives envisaged in these laws (Bakhtiyārī, 2019).

4.2. Strengths and Weaknesses of Domestic Laws

a) Strengths

• Initial Criminalization and Creation of a Legal Framework

One of the most important strengths of Afghanistan's legal system in this field is the criminalization of new forms of cyber behavior and the adoption of the first specialized law in 2014. This law has provided a basis for the identification and prosecution of cybercrimes and has, to some extent, filled the existing legal vacuum (Bakhtiyārī, 2019). In fact, this step reflects the legislator's awareness of global developments in technology-based crimes and the need to respond to new challenges in the digital environment.

• Creation of an Institutional Structure and Designation of a Specialized Authority

Another strength of the 2014 law is the designation of the Ministry of Communications and Information Technology as the main authority responsible for handling cyber matters and the establishment of special units for the investigation, detection, and prevention of digital crimes. This has been an effective step toward creating an institutional platform for cooperation among security, judicial, and educational bodies. In parallel, a number of cyber police units have also been set up on a limited scale in Kabul and several other provinces (Maleksha'ār & Tadayyun, 2019).

• Relative Alignment with International Instruments

From the perspective of general structure and key concepts, Afghanistan's Law on Combating Cybercrimes has been influenced by the Budapest Convention and other relevant international instruments. Although Afghanistan is not yet a formal party to this convention, basic principles such as international cooperation, information exchange, and protection of personal data were considered in the drafting of the law (Bakhtiyārī, 2019). This alignment can, in the future, facilitate Afghanistan's formal accession to international frameworks for combating cybercrime.

b) Weaknesses

• Ambiguity in Defining Concepts and Offense Elements

One of the most significant weaknesses of the Law on Combating Cybercrimes is the lack of precise and scholarly definitions of key concepts. For example, terms such as "information system," "electronic data," and "unauthorized access" are used without clear technical and legal criteria (Bakhtiyārī, 2019). As a result, in practice, judicial interpretations of a single provision may vary from one court to another, and there is no consistent case law for dealing with similar cases.

• Lack of Specialized Personnel and Weaknesses in Law Enforcement

A fundamental challenge in Afghanistan's legal system when confronting cybercrimes is the shortage of specialized personnel in judicial and law-enforcement institutions. At present, topics related to "cybercrimes" are not taught as an independent subject in university curricula and police academies. Consequently, many prosecutors and police officers, upon graduation, do not even have a basic understanding of the nature of such crimes (Bakhtiyārī, 2019). The lack of specialists leads to major difficulties in the process of crime detection and the collection of digital evidence.

Furthermore, technical infrastructure in judicial and law-enforcement bodies is weak; for example, there is a lack of digital forensic laboratories and specialized software for data tracing. This has caused many cybercrime cases to remain unresolved, thereby weakening public trust in the criminal justice system (Maleksha'ār & Tadayyun, 2019).

• Conflicts between Laws and Lack of Legal Coherence

Despite the adoption of several legal instruments in the field of cybercrime, there is still no required coherence and coordination among them. Some provisions of the Law on Combating Cybercrimes overlap or conflict with similar provisions in the Penal Code; for instance, conduct that is criminalized in one law may be described differently in another. This inconsistency not only makes enforcement difficult but also enables offenders to exploit legal loopholes (Ahmadi, 2019).

• Lack of Effective Enforcement Mechanisms and Weaknesses in Prevention

Many of Afghanistan's legal provisions in the area of cybercrime lack effective enforcement guarantees. Punishments are often general, lenient, and disproportionate to the seriousness of the offenses. Moreover, preventive measures such as public education, awareness-raising, and digital literacy enhancement are not adequately envisaged in the laws. While in more advanced systems, crime prevention is regarded as a key dimension of cybercriminal policy, in Afghanistan the emphasis is mainly on post-crime responses (Bakhtiyārī, 2019).

Thus, Afghanistan's legal system in the field of cybercrime is still in a transitional and evolving stage. Although the adoption of the Law on Combating Cybercrimes in 2014 was an important step toward criminalization and regulation of digital-space conduct, ambiguity in concepts, weaknesses in implementation, shortage of specialized staff, and lack of institutional coordination remain major obstacles to the realization of an effective criminal policy in this domain. For greater effectiveness of this legal framework, revision of the existing law, strengthening of specialized cyber training within judicial bodies, and expansion of international cooperation are essential.

5. Afghanistan's Criminal Policy on Cybercrimes

5.1. Definition and Dimensions of Criminal Policy

a) The Concept of Criminal Policy (Proactive and Reactive)

"Criminal policy" refers to the set of measures, decisions, and strategies adopted by the state in response to criminal phenomena; this policy includes both preventive (proactive) and punitive (reactive) actions (Nāṭeqī, 2019). In reality, criminal policy is a multidimensional system that analyzes criminal behavior and designs strategies for crime prevention and control.

In proactive policy, the focus is on preventing crime through education, cultural initiatives, enhancing public awareness, and strengthening institutional supervision; whereas reactive policy refers to the criminal justice response after a crime has occurred, primarily via punishment or security measures (Ḥaqqānī & Badakhsh, 2022).

Structurally and culturally, Afghanistan's criminal policy is predominantly reactive; that is, existing laws generally come into play after the commission of offenses, while extensive preventive and educational planning is lacking. This pattern is also evident in the cybercrime field, where state responses are more often in the form of arrest, filtering, or criminal punishment than awareness-raising and educational initiatives (Bakhtiyārī, 2019).

b) Tools for Prevention and Control

The tools of criminal policy fall into two general categories:

1. Penal tools (such as criminalization, determination of penalties, and establishment of specialized courts).
2. Non-penal tools (such as public education, cyber-defense technologies, institutional oversight, and international cooperation).

In the area of cybercrime, Afghanistan relies heavily on penal tools. The adoption of the 2014 Law on Combating Cybercrimes and subsequent criminal reforms in the 2017 Penal Code are examples of punitive measures. However, non-penal tools such as cultural initiatives, public education, and collaboration with international organizations have been far less developed (Maleksha'ār & Tadayyun, 2019).

5.2. Review of Afghanistan's Criminal Policy

a) Predominant Approach (Reactive Character)

According to the thesis findings, Afghanistan's criminal policy toward cybercrimes is predominantly reactive. That is, competent agencies intervene mainly after an offense has taken place rather than through preventive programs. The 2014 Cybercrimes Law and the Penal Code criminalize behaviors such as unauthorized access, dissemination of illegal content, and data destruction, yet there is no effective preventive structure for reducing the incidence of these offenses (Amīrzūrī, 2024).

The statutory criminal sanctions range from fines to long-term imprisonment; however, the absence of intelligent monitoring and digital education has meant that these penalties do not have sufficient deterrent effect (Bakhtiyārī, 2019). In many cases, instead of enhancing cyber security through defensive technologies, the state has resorted to blocking websites and social

networks—an indication of the predominance of reactive and security-oriented responses over preventive policy (Amīrzūrī, 2024; Maleksha'ār & Tadayyun, 2019).

b) Involved Institutions (Ministry of Communications, Prosecutor's Office, Cyber Police)

Under the 2014 Law on Combating Cybercrimes, the Ministry of Communications and Information Technology is designated as the primary institution responsible for cybercriminal policy. This ministry is tasked with identifying cyber threats and, in coordination with judicial and security bodies, planning preventive and responsive measures (Bakhtiyārī, 2019).

Alongside this, the Office of the Attorney General (Saranwalī) serves as the principal prosecuting authority for cybercrimes. However, the shortage of specialized training and technical equipment has led to serious challenges in the investigation and prosecution of digital offenses (Maleksha'ār & Tadayyun, 2019).

At the operational level, Afghanistan's Cyber Police functions under the Ministry of Interior. Its mandate is to track online crimes, identify offenders, and protect the country's communication infrastructure. Nevertheless, its activities are limited to a few provinces, and it lacks sufficient technical and human capacity (Amīrzūrī, 2024).

c) Operational and Institutional Challenges

According to the research findings, Afghanistan faces major challenges in enforcing its cybercriminal policy, including:

1. Lack of institutional coordination among the Ministry of Communications, the Prosecutor's Office, and the police.
2. Shortage of human resources specialized in digital technologies.
3. Absence of technical infrastructure such as digital forensic laboratories.
4. Weak international cooperation in data exchange and cross-border prosecution of offenders.

These factors have confined Afghanistan's criminal policy, in practice, to largely passive responses and have eroded its capacity for effective prevention (Amīrzūrī, 2024; Bakhtiyārī, 2019).

5.3. Consistency with International Instruments and Policies

a) The Budapest Convention

The 2001 Budapest Convention is the first and most important international treaty on cybercrime, providing a framework for judicial cooperation, harmonization of laws, and facilitation of data exchange. Although Afghanistan has not yet formally acceded to this convention, the 2014 Law on Combating Cybercrimes was partially modeled on its structure and concepts (Fatḥī, 2019).

Resolutions of the United Nations General Assembly, which emphasize the Budapest Convention, have called on states to adopt similar measures, and Afghanistan has repeatedly stressed in its official documents that its cyber laws should be inspired by this convention (Fatḥī, 2019). Nevertheless, due to technical and political weaknesses, Afghanistan has been unable to benefit fully from international cooperation mechanisms under this treaty.

b) Resolutions of the UN General Assembly

Since the 2000s, the UN General Assembly has adopted several resolutions on cybersecurity and information crimes. These instruments underline principles such as respect for human rights, state sovereignty, and the necessity of international cooperation (Fatḥī, 2019). Afghanistan, by incorporating some of these principles into its official policies, has declared that its cyber legislation should conform to international standards. However, political fluctuations and the change of government in 2021 have created interruptions and ambiguities in the implementation of these policies (Amīrzūrī, 2024).

c) The Role of ITU, Interpol, and Europol

The International Telecommunication Union (ITU), as the UN's technical arm in cyberspace, has developed programs to assist developing countries in the field of cybersecurity. Afghanistan has participated in several ITU initiatives, but due to limited financial and administrative resources, the benefits of this cooperation have been quite modest (Khanjarī et al., 2019).

Interpol and Europol are other active international bodies in this domain. By establishing specialized centers such as the European Cybercrime Centre (EC3), they have promoted multilateral cooperation in combating cybercrime. Although Afghanistan has expressed its willingness to cooperate with these organizations at a declaratory level, it has not yet joined their

technical and judicial cooperation networks because it has not acceded to the Budapest Convention and lacks adequate judicial infrastructure (Amīrzūrī, 2024).

d) Comparison of Afghanistan's Policy with Developed States

According to the comparative analysis in the thesis, Afghanistan's criminal policy on cybercrime is reactive, unstable, and lacks a robust institutional framework when compared with that of developed countries (Amīrzūrī, 2024).

In the European Union, a coordinated legislative framework—including the NIS2 Directive and the General Data Protection Regulation (GDPR)—has been implemented. Member states have established a multi-layered preventive system through coordination among governments, the private sector, and civil society organizations (Amīrzūrī, 2024).

In the United States, cybercriminal policy is based on the Computer Fraud and Abuse Act (CFAA), with multiple agencies such as the FBI, the Department of Justice (DOJ), and the Cybersecurity and Infrastructure Security Agency (CISA) playing prominent roles. The primary emphasis is on active prevention, capacity-building, and advanced digital tracking (Amīrzūrī, 2024).

In the United Kingdom, criminal policy is structured around a whole-of-society approach. Institutions such as the National Cyber Security Centre (NCSC) and the National Crime Agency (NCA) operate within a coherent network tasked with identifying threats and implementing preventive measures against digital crimes. This multifaceted and preventive policy stands in stark contrast to Afghanistan's largely reactive approach and represents a successful example of proactive criminal policy (Amīrzūrī, 2024; Bakhtiyārī, 2019).

Accordingly, Afghanistan's criminal policy toward cybercrimes is predominantly reactive, punishment-oriented, and lacking a comprehensive preventive perspective. Despite the adoption of the 2014 Law on Combating Cybercrimes and subsequent reforms, institutional incoherence, insufficient technical expertise, and weak international cooperation have undermined its effectiveness. Alignment with international standards and the experience of developed countries indicates that Afghanistan must move toward a proactive criminal policy, establish specialized institutions, and accede to the Budapest Convention in order to take meaningful steps toward improving its criminal policy in the cyber domain.

6. Analysis and Evaluation of Afghanistan's Criminal Policy

6.1. Strengths in the Legislative and Institutional Framework

One of Afghanistan's most important achievements in combating cybercrimes is the adoption of the Law on Combating Cyber Crimes in 2014, which constitutes the first formal step toward establishing a legal framework to address this phenomenon (Amīrzūrī, 2024). By criminalizing behaviors such as unauthorized access, data destruction, information theft, and the dissemination of immoral content, this law has filled a significant legal gap in the country's criminal justice system (Amīrzūrī, 2024).

In addition, the incorporation of certain information technology–related concepts into the 2017 Penal Code reflects the legislature's attention to emerging forms of criminality (Bakhtiyārī, 2019). Furthermore, the establishment of the Cyber Police within the structure of the Ministry of Interior and the creation of a Cyber Crimes Directorate in the Office of the Attorney General are among the institutional strengths in this area (Amīrzūrī, 2024).

From a legislative-structural perspective, the presence of relatively comprehensive definitions of technical concepts such as "unauthorized access," "information system," and "electronic data" in the 2014 law has, to some extent, aligned the country's legal framework with international standards (Maleksha'ār & Tadayyun, 2019). Moreover, the explicit reference in the provisions of this law to jurisdiction over offenses committed outside national borders reflects the legislature's awareness of the transnational nature of cybercrimes (Amīrzūrī, 2024).

At the institutional level, cooperation between the Ministry of Communications and Information Technology and security and judicial bodies for monitoring cyber activities and enhancing technical capacity represents a step forward in implementing national criminal policy (Bakhtārī, 2023). Although such cooperation has so far been implemented only in a limited manner,

the existence of these structures in itself indicates the beginning of the institutionalization of cyber criminal policy within Afghanistan's legal system (Bakhtārī, 2023).

6.2. Weaknesses and Challenges (Lack of Coordination, Deficits in Training and Technology)

Despite these legislative advances, Afghanistan's criminal policy on cybercrimes faces significant weaknesses and challenges. The most important of these can be summarized under three main headings: lack of institutional coordination, shortage of specialized human resources, and technological backwardness.

First, the absence of effective coordination among responsible institutions—including the Ministry of Communications, the Cyber Police, the Office of the Attorney General, and the judiciary—is one of the main obstacles to implementing criminal policy (Amīrzūrī, 2024). Owing to overlapping mandates and the lack of clear mechanisms of communication among these bodies, the prosecution of cybercrimes is often confronted with delays, jurisdictional conflicts, or duplicative efforts (Amīrzūrī, 2024).

Second, the shortage of specialized personnel in information technology and digital criminology means that, even when appropriate laws exist, their implementation remains difficult. Most judicial officers and police personnel lack technical training in the detection and documentation of cybercrimes; as a result, digital evidence is not collected or analyzed properly (Bakhtiyārī, 2019). In addition, the absence of systematic training programs for judges and prosecutors has led to an inadequate understanding of the technical concepts of cybercrimes in adjudication processes (Amīrzūrī, 2024).

Third, from an infrastructural standpoint, Afghanistan suffers from severe technological deficiencies. Vulnerable internet networks, the absence of secure data centers, and the lack of digital forensic equipment are among the key obstacles to detecting and preventing cybercrimes (Maleksha'ār & Tadayyun, 2019). In many cases, the Cyber Police are compelled to rely on private companies or international bodies for tracing cyber offenses, which makes judicial proceedings lengthy and complex (Amīrzūrī, 2024).

Moreover, ambiguities in certain legal definitions and the failure to distinguish between computer-related offenses and content-related offenses (such as the dissemination of anti-religious or political material) have sometimes led to the application of the Law on Combating Cyber Crimes on the basis of political or non-legal interpretations (Fatḥī, 2019). This not only reduces the effectiveness of criminal policy but also increases the risk of violations of individual freedoms (Fatḥī, 2019).

Another challenge is the lack of effective international cooperation in prosecuting cross-border offenders. Although the law emphasizes jurisdiction over extraterritorial offenses, Afghanistan has not yet acceded to the Budapest Convention and therefore cannot benefit from global mechanisms of judicial cooperation in the detection and exchange of information (Amīrzūrī, 2024).

6.3. The Need to Revise Laws and Structures

According to the dissertation's analysis, Afghanistan's criminal policy on cybercrimes requires fundamental revision on three levels: legislative, institutional, and operational.

At the legislative level, revision of the 2014 Law on Combating Cyber Crimes appears necessary, as this law—although advanced at the time of adoption—is now inadequate in dealing with emerging offenses such as ransomware, cryptocurrency-related crimes, and the misuse of artificial intelligence (Amīrzūrī, 2024). Furthermore, statutory definitions must be made more precise, and a clear distinction between "technology-based crimes" and "content-related crimes" should be incorporated into the text of the law, to prevent arbitrary interpretations (Fatḥī, 2019).

At the institutional level, the establishment of a National Cybercrime Coordination Center has been proposed to integrate the responsibilities of the Ministry of Communications, the police, the Office of the Attorney General, and judicial bodies. Such a center, relying on experts in technology and digital criminology, could guide investigations and prevent institutional overlap and duplication of effort (Amīrzūrī, 2024).

At the operational level, focusing on specialized training for judicial officers, judges, and digital experts is essential. Without enhancing technical skills, even comprehensive laws will remain ineffective in practice (Bakhtiyārī, 2019).

In addition, for greater effectiveness of criminal policy, it is recommended that Afghanistan formally accede to the Budapest Convention and engage actively with international bodies such as INTERPOL, EUROPOL, and the ITU (Khanjarī et al., 2019). This step could facilitate the exchange of judicial data, the training of personnel, and access to advanced technologies for crime detection (Amīrzūrī, 2024; Khanjarī et al., 2019).

Ultimately, Afghanistan's criminal policy must shift from a purely reactive and punitive model toward a proactive and preventive approach—that is, focusing on education, awareness-raising, enhancement of public digital literacy, and the creation of structured cybersecurity, rather than relying solely on punishment after the commission of offenses (Amīrzūrī, 2024).

Therefore, although Afghanistan's criminal policy in the cybercrime domain has taken an essential step with the adoption of the 2014 law and the establishment of specialized institutions, it still faces fundamental challenges. The absence of institutional coordination, insufficient specialized training, technological backwardness, and the lack of international cooperation are the main obstacles to its effectiveness. To reform and update criminal policy, revising existing laws, creating a national coordination center, and acceding to international instruments are urgent priorities (Amīrzūrī, 2024).

7. Conclusion

The present study shows that Afghanistan's criminal policy in the field of cybercrimes is predominantly reactive in nature. State laws and measures are mostly activated after an offense has occurred, and systematic, awareness-based preventive actions receive relatively little attention (Amīrzūrī, 2024). The primary focus of relevant institutions—including the Ministry of Communications and the Cyber Police—is on technical countermeasures and criminal prosecution, while preventive components such as education, promoting a culture of safe use of cyberspace, and developing cybersecurity infrastructure remain at an early stage (Bakhtiyārī, 2019).

Furthermore, the findings indicate that Afghanistan's criminal policy is only partially aligned with international instruments. Although the 2014 Law on Combating Cyber Crimes is to some extent inspired by the Budapest Convention and United Nations resolutions, the country's failure to formally accede to these instruments has prevented it from benefiting from international mechanisms for judicial and technical cooperation (Fatḥī, 2019). As a result, Afghanistan remains deprived of global capacities in detecting and prosecuting transnational cybercrimes and continues to depend on occasional assistance from other states (Amīrzūrī, 2024).

The results of the research show that, although Afghanistan has taken important steps over the past decade toward establishing a legal framework for combating cybercrimes, these measures remain institutionally and operationally insufficient. The adoption of the 2014 Law on Combating Cyber Crimes and the incorporation of related concepts into the 2017 Penal Code are among the strengths of the legislative system, but the absence of a national coordinating authority, the lack of specialized training, and the weakness of technical and technological infrastructure have prevented these laws from being implemented effectively (Bakhtiyārī, 2019; Maleksha'ār & Tadayyun, 2019).

From a criminological perspective, Afghanistan's criminal policy lacks a balance between proactive (preventive) and reactive (punitive) measures. While developed countries engage in crime prevention through early warning systems, digital education, and multi-level international cooperation, Afghanistan still relies primarily on criminal reaction as its main tool for addressing cyber-offending (Amīrzūrī, 2024).

From an international standpoint, although the Afghan legislature drew on the provisions of the Budapest Convention and United Nations recommendations when drafting the 2014 law, non-membership in key treaties, weak legal diplomacy, and the absence of systematic exchange of judicial data with other states have left Afghanistan largely detached from the global network for combating cybercrimes (Khanjarī et al., 2019).

Overall, the findings show that Afghanistan's criminal policy regime in the cyber domain is still in a formative stage and requires structural, technical, and educational reform in order to achieve the desired level of effectiveness (Amīrzūrī, 2024).

7.1. Practical Recommendations

1. Strengthening the Structure of the Cyber Police

- Establishing a General Directorate of Cyber Police with independent powers and a clear organizational structure.
- Sending officers to countries with strong cybersecurity experience for specialized training.
- Creating a "Joint Digital Investigation Unit" between the Cyber Police and investigative authorities.
- Forming covert online operations teams to: infiltrate criminal groups, identify online trafficking networks, and disrupt extortion and ransomware groups.
- Using undercover identities in cyberspace to uncover criminal operations.

2. Public Education and Digital Culture-Building

- Designing a "National Digital Literacy Program" that includes cybersecurity concepts, data protection, encryption, and safe online behavior.
- Producing simple and accessible educational packages for all segments of society (students, parents, civil servants, businesses).
- Preparing short courses and multilingual video tutorials (Dari, Pashto, and a third local language such as Uzbeki, Nuristani, Pashai, etc.).
- Incorporating cybersecurity topics into school curricula (from grade 7 onwards).
- Launching nationwide campaigns via television, radio, social networks, and billboards with clear messages.
- Using famous and influential public figures to attract public attention.
- Introducing mandatory cybersecurity training programs for all civil servants.
- Involving banks, telecommunications companies, and online retailers in providing security information to their customers.
- Preparing training packages for protecting websites, transactions, and customer data.

3. Expanding International Cooperation

- Concluding cybersecurity cooperation pacts with neighboring countries (Iran, Pakistan, Central Asian states) so that attack routes, cross-border offenders, and suspicious financial flows can be jointly managed.
- Training "cyber diplomats" capable of negotiating with international bodies such as UNODC, ITU, and INTERPOL.
- Establishing a cooperation mechanism with states from which cyber attackers operate.

4. Establishing a National Cybercrime Coordination Center

- Creating a single entity to coordinate all security, judicial, telecommunications, and financial bodies in the field of cybercrimes.
- Reducing the time needed to detect, analyze, and respond to cyber incidents.
- Enhancing national capacity to face emerging threats such as hacking, ransomware attacks, digital financial crimes, cyber espionage, and data misuse.
- Providing a unified standard for managing cyber crises at the national level.
- Creating a national database of cyber threats and incidents.
- Facilitating and coordinating information flows among security agencies, the Cyber Police, the central bank, telecommunications operators, and the private sector.
- Developing technical and legal frameworks for the detection, investigation, and prosecution of cybercrimes.
- Implementing public awareness and specialized capacity-building programs.

In the area of medium- and long-term development programs:

- Establishing a national center for training cybersecurity specialists.
- Creating a National Cyber Threat Repository.
- Expanding the use of artificial intelligence for attack detection.
- Setting up a Cyber Emergency Response Team (CERT).

7.2. Research Recommendations

It is recommended that future researchers in the field of cyber criminal policy conduct comparative studies between Afghanistan and regional countries such as Iran, India, Pakistan, and Turkey, in order to identify similarities and differences in

their legal policies. Such studies could guide the reform of Afghanistan's legislative system within a regional framework (Amīrzūrī, 2024).

In addition, examining the role of the private sector and technology companies in preventing cybercrimes could open a new path for interdisciplinary research at the intersection of law and technology. Future studies should focus on the effectiveness of non-criminal preventive measures such as education, counseling, and cyber self-regulation (Amīrzūrī, 2024).

The overall conclusion of this research is that, although Afghanistan has taken significant steps at the legislative level, its criminal policy—compared with the criminal policies of Budapest Convention member states—has not yet moved beyond a reactive stage and still requires structural and institutional reforms. To enhance the effectiveness of criminal policy in the field of cybercrimes, prioritizing prevention, education, strengthening the Cyber Police, and expanding international cooperation is essential.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Ahmadi, A. (2019). *Legal Analysis of Cyber Crimes in the Penal Code of Afghanistan*. Kabul University Press.
Amīrzūrī, M. (2024). *Afghanistan's Criminal Policy Regarding Cyber Crimes* Kabul University].
Anṣārī, J., Aṭāzādeh, S., & Qayyūmzādeh, M. (2019). The Criminal Policy of Iran and the U.S. Regarding Cyber Fraud and Theft Crimes. *Information and Criminal Research Quarterly*, *14*(55), 136-137.
Bakhtārī, F. (2023). Cyber Crimes and New Threats to Afghanistan's National Security. *Journal of Comparative Law*, *8*(1), 65-80.
Bakhtiyārī, A. F. (2019). *Analysis of the Constituent Elements of Cyber Crimes in Light of the Penal Code of Afghanistan*. Judicial Legal Research Center.
Beigī, A. (2019). *The Impact of Cyberspace on Security from Legal, Social, Political, and Military Perspectives*. Fānūs-e Donya Publishing.
Fatḥī, Ṣ. (2019). *The Role and Function of Governmental and Non-Governmental International Organizations in the Field of Cyber Crimes* Payame Noor University, Tehran Center].
Ghā'emī, A., Peyvandpūr, S., Andī, H., Gholāmī, S., & Gholāmī, S. (2024). Analysis of Criminological Theories Regarding Cyberspace (Cyber) Crimes.
Ḥaqqānī, J., & Badakhsh, L. (2022). Criminal Policy and Methods of Crime Prevention in Afghanistan. *Law and Penalty Quarterly*(2), 8.
Javādī Ḥosaynābādī, H., & Āghābābā'ī Ṭāghānakī, A. (2021). Criminological Analysis of Government Crime from the Perspective of Learning Theory. *Ārā' Quarterly*, *4*(8), 23.
Khanjarī, M., Majīdī, M., & Mokhtārī, F. (2019). The Role of the International Telecommunication Union (ITU) and the Media in Promoting World Peace. *Human Rights Research Journal*, *18*(7), 103.
Mahdavī Sābet, M., & Abdullāhī, S. (2020). Securing Children from Harms and Threats of Cyberspace with Emphasis on Interpol's Measures. *International Police Studies*, *11*(43), 11.
Maleksha'ār, M., & Tadayyun, A. (2019). The Impact of Cyberspace on Committing Acts Against Public Decency. *Legal Excellence Quarterly*(6), 12.
Mīrmurādī, S. M. (2020). *Cyber Crimes*. Māhvareh Publications.
Nāṭeqī, M. B. (2019). *The Criminal Policy of Islam and the Penal Law of Afghanistan Regarding Sexual Crimes*. Vāzheh Publishing.
Raddā'ī, M. (2019). Investigating Criminological Theories in the Formation of Cybercrime. *Iranian Political Sociology Quarterly*, *2*(4), 12.
Sobhkhīz, R. (2019). *Cyber Crimes in the Legal System of Iran and the World*. University of Police Sciences Publications.
Sutūdeh, H. (2020). *Social Pathology (Sociology of Deviance)*. Āvā-ye Nūr Publications.
Tāj Khorāsānī, S., Mas'ūd, G., & Shokrchīzādeh, M. (2021). An Indigenous View on the Social Control Theory of Crime with Attention to Islamic-Iranian Foundations. *Journal of Criminal Law and Criminology Research*, *10*(20), 331-334.
Walczak, S. (2021). Predicting crime and other uses of neural networks in police decision making. *Frontiers in psychology*, *12*, 31. https://doi.org/10.3389/fpsyg.2021.587943

Wordu, H., Uche, C., & Wali, C. B. (2022). 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*, *3*(1), 61-72. https://doi.org/10.5281/zenodo.6688231