Analysis of Criminal Laws Related to Cybercrimes Against National Security (Such as Cyber Espionage) and Examination of the Challenges of Identifying and Punishing These Crimes

1. Iman Nezam Eslami*: Department of Criminal Law and Criminology, ST.C., Islamic Azad University, Tehran, Iran
2. Ehsan Yavari: Assistant Professor, Department of Law, Ayatollah Boroujerdi University, Boroujerd, Iran

*Correspondence: aymannzamy99@gmail.com

Abstract

Security is the most important component of the political authority of states, and cyberspace, even while acknowledging its valuable achievements, violates this essential component. Therefore, the formulation of an effective preventive criminal policy alongside a coherent penal policy against the violation of cybersecurity is so crucial that negligence in this area can expose the criminal justice system to irreparable challenges. Despite the adoption of the International Cybersecurity Document, within the legal systems of many countries, comprehensive sets of laws aimed at countering and combating cybercrimes—which encompass numerous offenses—have been drafted and enacted. The policy in the laws of other countries suggests that criminal and penal policymaking in Iran, particularly in the field of social preventive measures against violations of cybersecurity, can play a significant role. Accordingly, different countries have adopted several security approaches to prevent violations of cybersecurity. Based on the findings of this research, although Iran's criminal justice system has considered various strategies to strengthen the security foundations of cyber interactions, due to the absence of an appropriate differential policy, it has not yet succeeded in adopting focused and effective social prevention mechanisms to prevent violations of cybersecurity. Moreover, the measures implemented, such as education and the promotion of digital literacy, often possess a non-technical nature.

Keywords: Cybercrimes, Security, Penal Policy, Espionage, Cyberspace, Punishment, Prevention

Received: 01 July 2025
Revised: 07 September 2025
Accepted: 14 September 2025
Published: 30 September 2025

Citation: Nezam Eslami, I., & Yavari, E. (2025). Analysis of Criminal Laws Related to Cybercrimes Against National Security (Such as Cyber Espionage) and Examination of the Challenges of Identifying and Punishing These Crimes. *Legal Studies in Digital Age,* 4(3), 1-13.

1. Introduction

Today, the overwhelming majority of security threats originate from cyberspace, leading to a significant transformation of national security systems (Mozaffari Nia, 2025). Behind these transformations, organizational and functional responses to technological developments can be identified, since national security performance is inseparable from the social environment and its processes (O'Hanlon, 2020). On the other hand, cybercrimes have a complex nature and encompass many disciplines,

including criminology, computer science, psychology, sociology, economics, geography, political science, and law (Jaishankar, 2011). Efforts in computer science and cybersecurity have primarily focused on the use of technical approaches such as intrusion detection systems, intrusion prevention systems, firewalls, and antivirus software to mitigate cyber-attack threats (Di Franco, 2018). These methods may, to some extent, help reduce the adverse effects of cybercrimes on organizations and individuals.

In other words, cybercrime is a broad term used by governments, businesses, and the public to describe various criminal activities and harmful behaviors involving computers, the internet, or other forms of information and communication technologies (Stuart, 2001). As an emerging social phenomenon in the information age, cybercrimes, due to their high destructiveness and wide penetration, have raised increasing global concerns (Merloe, 2017). In 2017, a cyberattack, commonly known as ransomware, affected more than 230,000 computers in 150 countries, leading to economic losses exceeding 4 billion dollars and posing a serious threat to educational, governmental, financial, and global healthcare sectors (Lewis, 2020). Moreover, cybercrimes have substantial impacts on the global economy, national security, social stability, and individual interests (Borhani & Haj Mohammadi, 2019). Current efforts to reduce cybercrime threats are mainly focused on technical measures. However, these crimes must be considered as a social phenomenon, and a theoretical framework should be established that integrates social, economic, political, technological, and cybersecurity factors influencing cybercrimes (Sobhe Khiz, 2015).

On the other hand, national security is essentially achieved as part of broader security structures, alongside other members of security organizations, which, due to their complex responsibilities, are engaged in many areas of combating illegal activities (Heydarian Zarneh, 2024). All these factors require the development of specific intelligence and reactive capabilities, as well as the continuous enhancement of their effectiveness, of which we have witnessed numerous international examples in recent years (Nishimura et al., 2019). This study, reflecting only the author's perspective, examines the complex relationship between cyberspace and the national security sector, in which national, historical, political factors, and current challenges of the security policy environment—along with the technological and information communication environment—have the greatest influence on the aforementioned structures (Rahimi & Rashidi, 2024).

1.1. Theoretical Literature

1.2. The Concept of Cyberspace

Cyberspace is a complex domain where structure (topology), dynamics, and functional processes are intertwined. Therefore, it is not surprising that disagreement persists when using related terminologies (Misuraca & Lusoli, 2010). To support the generalization of cyberspace theory, formalization and a solid foundation are essential. "Cyber" carries the notion of relation to computing and modern technology. For example, early computing in the 1980s and 1990s did not typically employ the term "cyber." In other words, "cyber" is a prefix indicating a relationship with information technology (IT). Anything related to computing, such as the internet, falls into the cyber category (Mozaffari Nia, 2025). In the late 1940s, the term "cybernetics" was coined by mathematician Norbert Wiener, defining it as the study of control and communication systems between humans and machines. Wiener borrowed the term from the ancient Greek word for "governance." In his book *Cybernetics*, Wiener described a computer system operating on feedback, essentially a self-regulating system. This concept was groundbreaking for the 1940s and introduced the idea of cybernetics into the fields of science and information technology (Nishimura et al., 2019). In short, the meaning of "cyber" is broad, encompassing a wide range of concepts, applications, and notions essential to our digital age (SentinelOne, 2025).

1.3. The Concept of Crime in Cyberspace

Cybercrimes, or information crimes, are a complex form of online crimes occurring within the internet environment (Jaishankar, 2011). These crimes, at times involving organized criminal groups, exhibit unique complexity and occur in

environments lacking specific characteristics or borders (Amiriyan Farsani, 2020). Perpetrators and victims of cybercrimes can be located in different regions, committing crimes from anywhere in the world without geographical restrictions. Conversely, the effects of these crimes can extend across societies worldwide, thus necessitating an immediate, dynamic, and global response (Ansari Mahyari et al., 2024).

The development of digital tools and the emergence of cyberspace have a relatively short history, but their growth has been remarkable, involving increasing numbers of individuals, institutions, and processes each day (Nishimura et al., 2019). A massive volume of content is produced in cyberspace daily, with internet users able to access this content in diverse ways. One of the key challenges in such an environment is the protection of information security and the prevention of its violation (Ghasemi et al., 2016). While safeguarding this right in the physical space is not particularly difficult, as various laws and regulations guarantee it, numerous challenges exist in maintaining information security in cyberspace (Deh Abadi & Ehsan, 2020). However, the rapid pace of development and expansion of digital tools complicates these challenges (Ghalevand et al., 2020). In this context, countries have sought to support preventive measures and legislation in cyberspace, either independently or through regional and international treaties, which have had positive impacts (Borhani & Haj Mohammadi, 2019).

The term "cybercrime" is essentially a journalistic term that still lacks a legal definition in most countries. Several international treaties (e.g., the United Nations Guidelines on Computer Crime Prevention and Control, the Convention on Cybercrime) also provide no official definition, opting instead for practical definitions (Sobhe Khiz, 2015). Hence, definitions of "cybercrime" often originate from academic literature. New technologies create new criminal opportunities but generate only a few new categories of crime (Barzegar & Pour Gharamani, 2016). What distinguishes cybercrimes from traditional criminal activities is, above all, the use of digital computers. However, technology alone is insufficient for differentiating between fields of criminal activity (Stuart, 2001). Criminals do not need computers to commit fraud, child exploitation, intellectual property theft, identity theft, or privacy violations—all of which existed before the spread of the "cyber" prefix. Cybercrimes, particularly involving the internet, represent an expansion of existing criminal behavior alongside some newly emerging illegal activities (Joks, 2010).

Most cybercrimes target the information of individuals, companies, or governments. Although these attacks are not carried out on the physical body, they occur within a personal or corporate "virtual body," defined by sets of informational attributes that identify individuals and institutions on the internet (Lewis, 2020). In the digital age, our virtual identities are essential elements of everyday life: we are represented by numbers and identifiers across numerous government and corporate databases (Javid Nia, 2009). Cybercrimes highlight the centrality of networked computers in our lives and the fragility of seemingly solid realities such as individual identity (Aghigh, 2023). A crucial aspect of cybercrimes is their non-local nature: offenses can occur across jurisdictions separated by vast distances (Mohammadi & Kalantari, 2024). This creates serious challenges for law enforcement, as even local or national crimes already required international cooperation (Rahimi & Rashidi, 2024). Cyberspace can be seen as a more complex version of the space in which a phone call takes place—existing between the two communicating parties. The internet, as a global network, provides criminals with numerous hideouts in both the real world and within the network itself (Baranlou & Pour Gharamani, 2024). Yet, just as individuals leave traces while walking on the ground that skilled trackers can follow, cybercriminals also leave clues about their identity and location despite their efforts to cover their tracks (Jahanshiri et al., 2015). To follow such trails across national borders, international cybercrime treaties must be adopted (Ansari Mahyari et al., 2024).

Later, however, due to rapid advances in cyberspace and information technology, the need for comprehensive legislation became apparent. As a result, the Computer Crimes Act of 2009 was enacted in Iran, comprising 56 articles (Deh Abadi & Ehsan, 2020). Simultaneously, with criminals entering commercial and economic spaces, the necessity of enacting laws to regulate such activities emerged. Consequently, the Electronic Commerce Act of 2003 was adopted, comprising 80 articles, which served as a model for the adoption of portions of other existing laws (Jalali Farahani, 2011).

2. The Concept of National Security in the Context of Cyberspace

Regardless of political or social systems, the existence of national security agencies and institutions can be considered a global reality across almost all countries. Although there are many formulas and interpretations of the concept of national security and the issues it covers, there is no universally accepted definition (Rahimi & Rashidi, 2024). This concept may be broadly interpreted to encompass wide areas of security, or more narrowly understood in relation to intelligence services and their functions. In this interpretation, the extensive application of national security information can be observed in academic literature (Mozaffari Nia, 2025).

At the same time, the rapid expansion of new technologies such as 5G networks, artificial intelligence, and the Internet of Things (IoT) is transforming everyday life, while the full extent of their impact on security structures—particularly at the level of national security—remains unclear (Nishimura et al., 2019). These technologies, in addition to providing significant benefits in facilitating services, improving productivity, and enhancing quality of life, also generate new risks that confront the cyber dimension of national security with increasingly complex challenges (Ghalevand et al., 2020). Simply imagining the potential consequences of intrusions into IT-dependent critical infrastructure, violations of privacy through the misuse of personal data, or the spread of misinformation and the manipulation of reality in cyberspace is sufficient to illustrate the importance of these threats in the conceptual framework of cyber national security (Sobhe Khiz, 2015).

In recent decades, cyberspace has become a key platform for producing, transmitting, and storing information, with the volume of generated digital data increasing exponentially. This phenomenon is not only an indicator of the rapid pace of digitalization but also a sign of rising security vulnerabilities (Deh Abadi & Ehsan, 2020). Specialized literature in the field of cyber governance repeatedly emphasizes that technology is advancing at a pace far exceeding the capacity of social and institutional structures to adapt (Misuraca & Lusoli, 2010). A clear example of this is the explosive growth of IoT devices, many of which operate with voice-based technologies and lack adequate safety and security standards (Lewis, 2020). According to a scenario projected by the European Union Cybersecurity Agency, by 2025 nearly 80 billion devices (about 10 per person) will be connected to the internet, and the volume of global data production will double every two years (O'Hanlon, 2020). This massive connectivity and data volume unprecedentedly expand the surface and scope of cyberattacks, compelling governments to allocate greater resources to develop and strengthen their cyber defense capacities (Heydarian Zarneh, 2024).

In this context, the concept of national security is increasingly being redefined—not only as the protection of physical borders but also as the safeguarding of the information space and cyber sovereignty (Ansari Mahyari et al., 2024). Dependence on imported technologies, foreign infrastructures, or non-national suppliers creates structural vulnerabilities that may become serious threats to national security through infiltration, cyber espionage, or even disruptions in digital supply chains (Aghigh, 2023). For example, the geopolitical disputes between the United States and China over the development and control of technology are merely one instance of these confrontations, showing that the control of key technologies in the future will be directly tied to the national security equations of states (Merloe, 2017).

3. The Nature and Types of Cyber Espionage

Cyber espionage is among the most significant emerging threats of the digital age, and given the increasing global connectivity and electronic data exchange, it has become a fundamental challenge to national security (SentinelOne, 2025). This phenomenon refers to the unauthorized and covert access to classified, confidential, or strategic information through digital tools and platforms (Barzegar & Pour Gharamani, 2016). Threats arising from this destructive activity have grown alarmingly in recent years, especially considering that a substantial portion of sensitive governmental, military, economic, and even personal information is stored and transmitted online (Amiriyan Farsani, 2020).

From the perspective of national security, cyber espionage involves interconnected and multidimensional threats. On the one hand, it may endanger a country's critical infrastructure; on the other, it can provide unfair advantages in commercial competition, particularly in sensitive and high-tech industries (Baranlou & Pour Gharamani, 2024). Furthermore, violations of citizens' privacy through cyber espionage also jeopardize government legitimacy and undermine public trust in digital

governance systems (Borhani & Haj Mohammadi, 2019). In a world where information is regarded as the most valuable strategic asset, control or unauthorized access to classified data can grant non-state actors or hostile states bargaining power and destructive capabilities (Ghasemi et al., 2016).

One of the earliest known cyber espionage cases occurred between September 1986 and June 1987, when a group of German hackers successfully infiltrated computer networks associated with U.S. military contractors, research universities, and military bases, selling the stolen strategic information to Soviet intelligence (Stuart, 2001). This incident is considered the first documented case of cyber espionage at the international level, after which cybersecurity became a core pillar of national security policy (Lewis, 2020).

Today, cyber espionage can be carried out through advanced tools such as intrusive malware, targeted phishing attacks, software backdoors, or even exploiting hardware and software vulnerabilities (Jahanshiri et al., 2015). Moreover, the increasing involvement of nation-states in conducting or supporting cyber espionage operations has blurred the line between cyber warfare and cyber espionage (Mohammadi & Kalantari, 2024). This development not only challenges international legal norms governing digital sovereignty but also makes responding to such threats a strategic and multidimensional issue for governments (Ansari Mahyari et al., 2024).

4. Types of Cyber Espionage

Cyber espionage can be classified into several categories based on the goals and motivations of the attacking parties. Each type is conducted with specific political, economic, or military-strategic objectives, and the information sought is typically aligned with such strategic aims (Aghigh, 2023). Some of the main categories include:

a) Political Espionage: This involves targeting governments, political figures, or elections. The motivation lies in obtaining information relevant to policy decisions, international negotiations, or political outcomes. Political espionage often involves surveillance of government officials and sometimes includes eavesdropping or hacking sensitive political documents. Such campaigns may also involve cyberattacks aimed at altering electoral processes, where hackers attempt to influence public opinion or undermine trust in elections by stealing and disclosing sensitive information (Merloe, 2017).

b) Military Espionage: This type targets information related to military activities, defense contractors, or weapons manufacturers. It involves retrieving sensitive defense strategies, weapons technologies, troop movements, and military capabilities. Military cyber spies may compromise defense systems and disrupt military operations. Much of the intelligence gathered is used to design countermeasures against defense projects or to prepare for preemptive strikes in the event of war (O'Hanlon, 2020).

c) Corporate Espionage: Also known as industrial cyber espionage, this entails the theft of business-related information, including trade secrets, proprietary technologies, intellectual property, and financial data, often from rival firms. Such activities can be conducted by competitors or state actors seeking strategic market advantages. Common practices include stealing product designs, patents, or R&D data; hacking supply chains to obtain pricing strategies or supplier contracts; and breaching email systems to gather intelligence on business strategies, mergers, or market launches (Bazvand & Nour, 2024).

5. Analysis of Iran's Criminal Laws in the Field of Security-Oriented Cybercrimes

The trans-spatial and borderless nature of cyberspace has rendered traditional concepts of sovereignty, territory, and geographical borders less functional against threats that may originate thousands of kilometers away yet directly impact the domestic governance of a state (Sobhe Khiz, 2015). The global interconnectedness of digital networks enables attackers to easily bypass physical boundaries, target national infrastructures, or use the internet to promote extremism, propaganda, and psychological warfare (Lewis, 2020). This situation underscores, more than ever, the necessity of transnational cooperation, the development of common legal frameworks, and the enhancement of international oversight regimes (Ansari Mahyari et al., 2024).

In addition to geographical challenges, the complexity of cyberspace manifests in the increasing interdependence of diverse social, economic, and security subsystems (Misuraca & Lusoli, 2010). This phenomenon has its roots in the most advanced applications of communication technologies over the past four decades, which have weakened the boundaries between civilian and security domains (Mozaffari Nia, 2025). At the same time, while citizens seek to benefit from freedom of information, digital mobility, and individual autonomy, the same environment can become a vehicle for committing new types of crimes such as financial fraud, human trafficking, money laundering, terrorist financing, and the illegal sale of data (Borhani & Haj Mohammadi, 2019).

One of the fundamental challenges in this environment is the use of encrypted technologies and modern communication tools by criminal groups to evade surveillance and prosecution by national security institutions (Jahanshiri et al., 2015). These groups exploit the uncertainty of geographical location and the speed of digital mobility to leverage cyber capacities, staying ahead of legal institutions (Mohammadi & Kalantari, 2024). Cyber-related threats are not limited to conventional cyberattacks such as malware, ransomware, or network disruptions; rather, they extend into traditional domains of security as well (O'Hanlon, 2020). For example, modern terrorism exploits cyberspace for propaganda, recruitment, training, and even financing (Jaishankar, 2011). Against this backdrop, the need to develop updated criminal laws and deterrent punishments—complementing the functions of intelligence and national security organizations in cyberspace to monitor, analyze, and counter such threats—is greater than ever (Aghigh, 2023).

Accordingly, in Iran's criminal legal system, the concept of "security" has always been a central pillar of penal laws. In recent decades, with the expansion of cyberspace and the emergence of new threats in the digital domain, attention to new dimensions of crimes against national security has become increasingly vital (Heydarian Zarneh, 2024). In this regard, the Iranian legislature attempted to address some of the existing gaps in confronting cybercrimes, including security-oriented offenses, by enacting the "Computer Crimes Act" of 2009 (Deh Abadi & Ehsan, 2020).

6. Review of the Computer Crimes Act and the Islamic Penal Code

In the Iranian legal system, the Computer Crimes Act of 2009 and the Islamic Penal Code of 2013 constitute the two main legislative pillars in confronting cybercrimes (Rahimi & Rashidi, 2024). Together, these laws provide a framework for combating security-oriented threats in cyberspace, including cyber espionage, digital sabotage, and other forms of organized cybercrimes (Barzegar & Pour Gharamani, 2016). Within the Islamic Penal Code, cybercrimes are addressed as a distinct chapter in Book Five, which was approved in 2013. This chapter classifies crimes under headings such as the confidentiality of data and the security of computer and telecommunication systems, the integrity and authenticity of data and systems, computer theft and fraud, offenses against public morality, and the dissemination of false information, prescribing punishments for each (Ghasemi et al., 2016). The laws aim to preserve the security and privacy of individuals in cyberspace, protect the health of computer systems, and prevent cybercrimes (Amiriyan Farsani, 2020).

In the definitions adopted within Iran's legal system, cybercrimes are offenses committed in the non-physical and virtual space against information technologies. With the advancement of information and communication technologies, traditional crimes have also undergone transformations, acquiring cyber dimensions (Javid Nia, 2009). Due to their broad scope, the term "cybercrime" has increasingly replaced terms such as "computer crimes" or "internet crimes," since "computer" alone cannot fully describe the wide-ranging environment in which these crimes occur. Many modern tools work with data without being classified as computers in the conventional sense. Thus, terms such as computer crimes or internet crimes fail to precisely cover all offenses in this field (Joks, 2010). For example, an electronic recording and playback system is not technically a computer but is nonetheless part of cyberspace. Accordingly, the term "cybercrime" is more accurate for describing such offenses in the context of information technology (Stuart, 2001).

The Computer Crimes Act specifically addresses the technical and emerging nature of these crimes, criminalizing acts committed in digital and information technology environments (Deh Abadi & Ehsan, 2020). Chapter One, titled "Crimes against the Confidentiality of Data and Computer and Telecommunication Systems," constitutes the most important legal basis

for prosecuting cyber espionage and intrusions into the country's security systems. Article 1 of this law criminalizes unauthorized access to systems, while Article 2 defines the unauthorized interception of transmitted data as an offense. More importantly, Article 5 addresses the crime of data or computer system forgery, which, from a national security perspective, may constitute cyberattacks designed to disrupt critical infrastructures (Baranlou & Pour Gharamani, 2024). Furthermore, Article 10 explicitly addresses "crimes against public security and order" in cyberspace, criminalizing any disruption or interruption in the country's vital systems. This provision is especially significant in countering cyber sabotage activities, such as attacks on water, electricity, energy, and transportation infrastructures (Ghalevand et al., 2020).

Alongside the Computer Crimes Act, the Islamic Penal Code also provides the overarching conceptual framework and general principles governing crimes against national security (Rahimi & Rashidi, 2024). In Book Five, Chapter One of Part Two, crimes against the internal and external security of the Islamic Republic of Iran are addressed. Articles 498, 499, 500, 508, and particularly Article 501 (espionage) are notable in this regard. Article 501 states: "Whoever engages in espionage for the benefit of foreign governments, if the disclosed information harms national security, shall be sentenced to imprisonment from one to ten years." Although this provision was originally drafted with reference to traditional (physical and human) espionage, judicial practice and interpretation allow its broader application to cyber espionage, especially in cases where individuals or groups access classified military, political, or economic information through digital intrusion and provide it to foreign entities (Aghigh, 2023).

Nevertheless, a serious challenge lies in the lack of explicit legislative acknowledgment of the cyber nature of this form of espionage, which can lead to restrictive interpretations by courts (Mohammadi & Kalantari, 2024).

7. Analysis of the Legal, Material, and Mental Elements of the Crime

The legal element, as the first foundation of analysis, refers to the existence of explicit legal provisions that criminalize a specific act or omission and prescribe penal sanctions for it (Rahimi & Rashidi, 2024). In Iran's criminal law structure, although the legislature has not explicitly defined the terms *cyber espionage* or *cybercrimes against national security*, by combining various articles from the two main laws—namely, the 2009 Computer Crimes Act and the 2013 Islamic Penal Code—it is possible to infer the legal framework required to prosecute such offenses (Deh Abadi & Ehsan, 2020). For example, Article 501 of the Islamic Penal Code, which concerns the crime of espionage, although designed at the time of enactment with the classical notion of transferring information to the enemy, due to its general wording with respect to "any action for the benefit of foreign governments," can also be extended to cyberspace (Aghigh, 2023). On the other hand, multiple provisions of the Computer Crimes Act—Articles 1 (unauthorized access), 2 (unauthorized interception), 3 (data theft), 5 (data forgery), 6 and 7 (destruction and disruption of data and systems), and Article 10, which targets disruptions in the nation's vital systems—constitute important capacities for criminalizing behaviors that represent new forms of threats against national security in the digital environment (Baranlou & Pour Gharamani, 2024). This legislative combination, though fragmented in appearance, collectively enables the establishment of a foundation for the criminal prosecution of cyber espionage and similar crimes, provided that their interpretation and implementation are accompanied by a technical-security understanding of the nature of cybercrimes (Borhani & Haj Mohammadi, 2019).

The material element in these types of crimes is accompanied by particular complexities. Unlike traditional crimes that manifest in tangible external forms, criminal acts in cyberspace are often invisible and hidden from a physical perspective (Ghasemi et al., 2016). Regarding security-oriented crimes, this element often appears in the form of intrusions into sensitive government systems, access to classified information through technical tools such as malware, transmitting this information to external servers, or disrupting the functioning of vital state institutions (such as defense, energy, banking, transportation, and communication systems) (Lewis, 2020). In other words, the material element of crime in this field usually consists of a chain of technological actions, beginning with the identification of security vulnerabilities and extending to data transfer and the concealment of digital traces (Jahanshiri et al., 2015). Such behaviors, if carried out with the intention of weakening the foundations of national security or aiding the enemy, may also correspond with traditional concepts of espionage and treason (Heydarian Zarneh, 2024). Given that the material element in this field lacks classical manifestations such as physical

presence, document delivery, or audio recording, proving it requires data analysis, extraction of communication logs, IP address tracking, and technical cooperation with specialized cybersecurity institutions—issues that were rarely relevant in traditional criminal law (Deh Abadi & Ehsan, 2020).

The mental element, as the third essential component, is of heightened importance in crimes against national security, particularly in cyberspace. This element not only refers to the intention to commit an unauthorized technical act but must also include the special criminal intent of harming national security or assisting the enemies of the Islamic Republic of Iran (Aghigh, 2023). This means that mere unauthorized access to systems or collection of information, without establishing a security-hostile intent, may constitute a criminal offense but does not fall within the classification of crimes against national security (Mohammadi & Kalantari, 2024). Establishing the mental element in such crimes is difficult due to the opaque nature of cyberspace and is often possible only through external evidence, such as the destination of transmitted information, the nature of the recipient organization, the perpetrator's communication records, the use of advanced encryption technologies, or the concealment of digital identities (Barzegar & Pour Gharamani, 2016). In some cases, the mental element is revealed through confessions, extracted data from seized digital devices, and analysis of digital communication networks (Amiriyan Farsani, 2020).

8. Judicial Practice and Legislative Shortcomings

With respect to judicial practice, it can be stated that Iran's criminal justice system has not yet developed a coherent and specialized approach in addressing security-oriented cybercrimes (Rahimi & Rashidi, 2024). Due to the absence of dedicated judicial branches and specialized judges in the field of cybercrimes with a security-oriented perspective, many cases of cyber espionage or intrusions into vital systems are examined under general charges such as "unauthorized access," "data disruption," or "propaganda against the system," without properly distinguishing and analyzing their security dimensions (Jalali Farahani, 2011). In the limited and publicly known cases of cyber espionage, criminal courts have often resorted to broad interpretations of Article 501 of the Islamic Penal Code or Article 10 of the Computer Crimes Act in order to classify the offender's conduct as security-related. While this approach partially compensates for legislative gaps, it raises serious concerns from the perspective of fundamental principles of criminal law, such as the principle of restrictive interpretation of penal laws and the principle of clarity in criminalization (Stuart, 2001). Particularly in cases where mere "internet communication" with a foreign individual or institution, without establishing hostile intent or a clear material element, has been regarded as "cyber espionage," one can observe conceptual confusion and a lack of specialized analysis (Sobhe Khiz, 2015).

Moreover, the absence of clear rules in distinguishing between "cyber espionage," "non-security-related informational intrusions," and "purely financial cyber offenses" has resulted in divergent, sometimes contradictory, and legally inconsistent judicial approaches (Javid Nia, 2009). In some cases, judges, due to unfamiliarity with the technical infrastructure of cyberattacks, rely heavily on superficial evidence or preliminary reports from security agencies without independently and accurately verifying the authenticity of digital evidence (Joks, 2010). This highlights the pressing need for independent forensic-technical expertise and continuous specialized training (Ansari Mahyari et al., 2024).

From the perspective of legislative shortcomings, it can be said that although the 2009 Computer Crimes Act was an initial step toward addressing technological threats, it largely focused on technical aspects and user privacy rather than the security-oriented dimension of cyberspace (Deh Abadi & Ehsan, 2020). None of its provisions specifically and explicitly address issues such as cyber espionage, digital sabotage with security-hostile motivations, technological collaboration with the enemy, or the transfer of sensitive information to foreign intelligence services (Aghigh, 2023). The lack of a precise legal definition of "national security in cyberspace" and "cyber espionage" has left their interpretation to inconsistent and sometimes arbitrary judicial practices (Mohammadi & Kalantari, 2024).

Likewise, in the Islamic Penal Code, especially in the chapter on crimes against state security, all provisions were drafted with assumptions of traditional physical conduct. Concepts such as "delivering documents," "gathering information from military sites," or "organized contact with foreigners" remain in classical form and lack direct adaptability to data-driven

crimes, remote intrusions, or encrypted transmissions of sensitive information (Baranlou & Pour Gharamani, 2024). This shortcoming not only creates a gap in precise identification of offenses but also increases the possibility of misuse or misinterpretation (Borhani & Haj Mohammadi, 2019). Furthermore, the current laws make no reference to the "categorization of cyber threats" based on their security significance. The distinction between a simple intrusion into a public institution's system and organized access to classified defense information is not properly clarified in legislation, and the punishments do not provide adequate differentiation. This deficiency undermines the proportionality between crime and punishment, and consequently, the principle of criminal justice (Heydarian Zarneh, 2024).

9. Challenges of Identifying and Punishing Cybercrimes Against National Security

The challenges of identifying and punishing cybercrimes against national security constitute some of the most significant issues in the realm of criminal law for information technology and national security (Sobhe Khiz, 2015). These crimes, utilizing digital infrastructures within the intangible cyberspace, not only transcend traditional territorial and sovereign boundaries but also confront conventional legal systems with serious difficulties in detection, prosecution, proof, and enforcement of punishment (Rahimi & Rashidi, 2024). The trans-spatial, covert, and technological nature of these crimes has made existing legal tools insufficient to address emerging threats (Lewis, 2020).

10. Technical Challenges in Identification and Evidence Collection

One of the most important challenges is the unstable and mutable nature of digital data. Information related to the occurrence of cybercrime may reside in temporary system memory, browser caches, network packets, or even RAM, which disappears once the system is shut down or settings are changed (Jahanshiri et al., 2015). This requires crime detection processes to be carried out urgently and with high sensitivity; otherwise, vital evidence may be completely lost or altered, rendering it inadmissible in court. Another major challenge is the *deterritorialization* and dispersion of data across international platforms. In many cases, crime-related data are stored on servers located outside national borders (Mohammadi & Kalantari, 2024). For example, a cyber spy may infiltrate a system in Iran from a third country and transfer sensitive data to a server located in a fourth state. Under such circumstances, immediate and effective international cooperation is necessary, though in practice this often fails due to political, legal, or technical obstacles (Ansari Mahyari et al., 2024). Moreover, some countries, citing privacy protections or user rights, refuse to provide stored data on their servers to the judicial authorities of other states (Khosrow Zadeh et al., 2022).

Another challenge is the use of advanced technologies by criminals to conceal their activities. Today, cybercriminals employ tools such as end-to-end encryption, anonymizing networks like Tor, anti-tracking and anti-analysis utilities, and self-erasing malware (Di Franco, 2018). These tools make it not only difficult to identify the source of criminal activity but also highly challenging to collect valid and admissible evidence. Additionally, the issue of proving the authenticity, integrity, and reliability of digital evidence is crucial. Any data intended for use in court must possess qualities such as authenticity, integrity, reliability, and admissibility (Fattahi, 2018). However, digital data can easily be manipulated. Therefore, the collection process requires the use of specialized digital forensic tools that comply with international standards. Weakness in this area can undermine evidence and lead to the acquittal of offenders (Deh Abadi & Ehsan, 2020).

A further challenge is the insufficient technical expertise among judicial officers, experts, and even judges in analyzing and assessing digital evidence. Specialized processes such as network traffic analysis, recovery of deleted information, reverse engineering of malware, and tracing attack origins require teams of skilled IT and cybersecurity experts (Ghalevand et al., 2020). Without this knowledge, admissible evidence may be overlooked or improperly analyzed (Amiriyan Farsani, 2020).

11. Jurisdictional Problems and Transnational Prosecution

One of the most significant jurisdictional problems is the multiplicity and conflict of jurisdiction among states over a single crime (Barzegar & Pour Gharamani, 2016). In cases where a foreign actor infiltrates a state's security systems through

servers located in multiple countries, several states may claim jurisdiction: the country where harm occurred (the victim state), the state of the offender's residence, the state hosting the servers, and even the transit state of the data (Stuart, 2001). This multiplicity may lead to overlapping jurisdiction or, conversely, to a situation where no state asserts jurisdiction—especially when states refrain from exercising criminal jurisdiction for political or diplomatic reasons (Rahimi & Rashidi, 2024).

Another difficulty lies in the absence of a binding global mechanism to determine jurisdiction or resolve conflicts. Unlike crimes such as hijacking or money laundering, for which conventions define jurisdictional frameworks, the only relatively comprehensive international instrument in the field of cybercrime is the Budapest Convention (2001), which some countries—including Iran—have not ratified (Sobhe Khiz, 2015). Consequently, in the absence of a binding global framework, each state may assert or deny jurisdiction based on national interests, leading to a criminal accountability gap in addressing cyber-offenders (Borhani & Haj Mohammadi, 2019).

Regarding transnational prosecution, one of the major problems is the lack of judicial and law enforcement cooperation among states. Requests for extradition, international data searches, or the collection and exchange of digital evidence require effective police cooperation (e.g., Interpol) and bilateral or multilateral judicial assistance mechanisms (Mohammadi & Kalantari, 2024). In practice, however, particularly in cases of crimes against national security, many states refuse to cooperate because such offenses often have political, intelligence, or military dimensions (Merloe, 2017). In some cases, the host state may not only decline to prosecute but may also support or benefit from the offender's operations, creating deadlock in extradition or prosecution (O'Hanlon, 2020).

State-sponsored cybercrimes pose another serious challenge. In such cases, the perpetrator operates under the protection or command of their home state, making extradition or trial in a third country virtually impossible (SentinelOne, 2025). Here, traditional international criminal law, which rests on individual criminal responsibility, loses effectiveness, underscoring the need for mechanisms to impose state responsibility for cyber operations against national security (Ansari Mahyari et al., 2024).

Another problem arises from fundamental legal differences across states in defining crimes, jurisdictional scope, and trial procedures. For instance, behavior criminalized as "cyber espionage" in one country may be deemed freedom of information or a legitimate political act in another (Aghigh, 2023). These definitional divergences severely weaken prospects for transnational cooperation and foster impunity for international cyber-offenders (Mozaffari Nia, 2025).

12. Weaknesses in International Cooperation

As mentioned earlier, due to the unique features of cyberspace—such as trans-spatiality, technical anonymity, rapid occurrence, and technological complexity—cybercrimes can only be effectively identified and prosecuted through broad and effective cooperation among governments, international organizations, and private entities (Jaishankar, 2011). Nevertheless, international cooperation in practice has been plagued by weakness, delays, and in some cases, outright failure (Rahimi & Rashidi, 2024).

The first and most fundamental weakness is the absence of comprehensive, binding, and universal international frameworks to combat cybercrimes (Sobhe Khiz, 2015). Currently, the only relatively comprehensive instrument is the Budapest Convention on Cybercrime (2001), which, due to political and legal considerations, has not been adopted by many states, including Iran, Russia, and China (Baranlou & Pour Gharamani, 2024). This lack of membership has excluded these countries from the circle of judicial and informational coordination under the convention, depriving them of the benefits of mutual legal assistance mechanisms (Borhani & Haj Mohammadi, 2019).

Operationally, one of the most important problems is states' weakness or refusal to share technical information, user data, and digital evidence in sensitive national security cases (Khosrow Zadeh et al., 2022). Many cybercrimes against national security involve intelligence, military, or political dimensions, and states—especially those with hostile or absent diplomatic relations—are reluctant to share vital information or extradite offenders (Amiriyan Farsani, 2020). For example, if a

cyberattack against critical infrastructure originates from an individual sheltered in another country, and that country refuses to extradite or disclose information, prosecution becomes practically impossible (Lewis, 2020).

Another obstacle to cooperation is the deep legal and cultural divergences among states in defining cybercrimes, assigning responsibility, and applying criminal procedure principles (Rahimi & Rashidi, 2024). Some states interpret cyber intrusions as exercises of free expression or legitimate political activities, and therefore refuse to criminalize or prosecute them (Aghigh, 2023). Others prioritize privacy rights of users over the prosecution of cyber-offenders, declining to provide user information to third countries (Fattahi, 2018).

This conceptual gap severely reduces the feasibility of judicial cooperation. Additionally, the absence of permanent, efficient, and neutral institutions for international coordination in cybercrime aggravates these weaknesses (Misuraca & Lusoli, 2010). Unlike fields such as human trafficking or money laundering, where bodies like the UN Office on Drugs and Crime or the Financial Action Task Force operate, cybersecurity lacks a supervisory authority with supranational jurisdiction and broad enforcement capacity (Ansari Mahyari et al., 2024). Organizations such as Interpol or Europol cover some cyber activities but their competence, resources, and mandates are insufficient to address complex global national security threats (Nishimura et al., 2019).

Finally, mutual mistrust among governments and fears of misuse of shared intelligence further undermine cooperation. Often, states refuse to share digital data or cooperate in prosecuting offenders due to concerns about information leakage or its instrumental use by the requesting country (Merloe, 2017). In cases involving cyber espionage in particular, mutual trust is virtually absent, and even legal mechanisms cannot overcome this structural mistrust (Mohammadi & Kalantari, 2024).

13. Conclusion

Cyber espionage is a growing, fast-evolving, and dynamic threat in the cybersecurity landscape. As technology advances, the methods employed by cyber offenders targeting governments, corporations, and individuals also change. Therefore, it is rapidly becoming an urgent matter for every organization to implement strong internal security measures. Emphasis on cybersecurity must be accompanied by investment in appropriate detection and prevention strategies that enable organizations to safeguard sensitive information while simultaneously enhancing resilience against the constantly changing threat environment.

First, the structure of Iran's criminal law is still based on traditional concepts of criminalization and territorial jurisdiction, and it lacks the capacity to adapt to the specific features of cybercrimes, including their transnational nature, the anonymity of perpetrators, and the technology-driven character of criminal conduct. Existing laws, such as the 2009 Computer Crimes Act, despite their initial progress, have not been able to respond effectively to the rapid evolution of the digital environment and the complex diversity of national security–related activities in cyberspace. Furthermore, the incomplete or general definitions of concepts such as "unauthorized access," "computer espionage," or "cyber sabotage" allow for inconsistent and sometimes unjust interpretations in judicial proceedings.

Second, in the area of crime detection and evidence collection, technical challenges such as the instability of digital data, the dispersion of servers across international jurisdictions, advanced encryption, and the limited technical capacity of certain law enforcement bodies have weakened the ability to detect, document, and prove security-oriented cybercrimes. In the absence of specialized digital forensic teams and technology-based infrastructures within the criminal justice system, these shortcomings have become serious obstacles to achieving criminal justice.

Third, at the international level, the inefficiency of judicial and police cooperation, the absence of binding global instruments, jurisdictional conflicts, and mutual distrust among states—especially in political or intelligence-related cases—have rendered the prosecution and extradition of transnational offenders practically impossible. Under such circumstances, cybercrimes against national security exploit legal loopholes and international incoherence, becoming one of the least costly and lowest-risk tools of national and international threat.

Therefore, a fundamental rethinking of the country's legislative and judicial criminal policy is essential. This reform must be pursued through an interdisciplinary, technological, and comparative approach. Practical recommendations in this regard include:

1. Drafting and enacting a comprehensive cybercrime law with a specific focus on security-oriented threats.
2. Updating crime definitions in line with international standards and technological developments.
3. Strengthening specialized structures for the detection and analysis of digital evidence by employing trained technical experts.
4. Establishing dedicated departments within the judiciary to handle national security–related cybercrimes.
5. Joining international conventions such as the Budapest Convention or actively participating in drafting alternative instruments.
6. Designing a clear legal framework for exercising criminal jurisdiction over transnational cybercrimes and reinforcing cyber diplomacy to enhance international cooperation in the field of digital security.

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

Aghigh, R. H. (2023). Legislative inadequacies of the crime of espionage in the Islamic Penal Code compared to the Penal Code of France. *Journal of Scientific Research in Criminal Law and Criminology*(22).

Amiriyan Farsani, A. (2020). Public and legal challenges in combating cybercrimes. *Journal of Journalism and Communication Law*(3).

Ansari Mahyari, A., Khalili Samani, K., Poladian, M., & Ahmadi, M. (2024). Solutions to combat cybercrimes from the perspective of international law. *Journal of New Human Sciences Studies in the World*(4), 61-80.

Baranlou, A., & Pour Gharamani, B. (2024). The impact of virtual social networks on security crimes. In National Conference on Cyber Defense,

Barzegar, S., & Pour Gharamani, B. (2016). Cyber espionage as a contemporary challenge. In National Conference on Passive Defense in Cyber Space,

Bazvand, V., & Nour, M. (2024). The dual role of computer tools in achieving fraud. *Judiciary Legal Journal*(122), 9-30.

Borhani, M., & Haj Mohammadi, A. (2019). Comparative study of cyber terrorism in the penal laws of Iran and the USA. *Quarterly Journal of Legal Studies*(30).

Deh Abadi, M. A., & Ehsan, S. (2020). *Principles of criminalization in virtual space with a critical approach to the Computer Crimes Law*. Tehran: Jungle Publications.

Di Franco, F. (2018). Analysis of the European R&D priorities in cybersecurity.

Fattahi, M. (2018). Analyzing the material and moral components of computer crimes. *Quarterly Research Journal of Law Yar*(6).

Ghalevand, K., Karimi Ghahrudi, M. R., & Haji Malamirzaei, H. (2020). The impact of transformative technologies on the regulation of the virtual space of the country. *Quarterly Journal of Strategic Studies of NAJA*(18).

Ghasemi, V., Hadi, D., & Dadiyar. (2016). Examining the material element of computer crimes and the jurisdiction of courts handling them in Iranian criminal law. International Congress of Islamic Sciences and Humanities,

Heydarian Zarneh, M. R. (2024). Analysis and examination of the components constituting the crime of conspiracy against national security. 6th International Conference on New Studies in Humanities, Educational Sciences, Law, and Social Studies,

Jahanshiri, J., Hosseini, M. R., & Ebrahimi, A. (2015). Explaining the process of preliminary investigations in cyber crimes. *Quarterly Journal of Information and Criminal Research*(3).

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, CRC Press. https://doi.org/10.1201/b10718

Jalali Farahani, A. H. (2011). *Introduction to the criminal procedure of cyber crimes*. Tehran: Khorasandi.

Javid Nia, J. (2009). *Electronic commerce crimes*. Tehran: Khorasandi Publications.

Joks, Y. (2010). *Crime and the Internet*. Tehran: Police University Publications.

Khosrow Zadeh, A., Sepahri, R. H., & Babaei, H. (2022). The legitimacy of obtaining evidence in virtual space crimes in Iranian criminal law. *Quarterly Journal of Comparative Penal Jurisprudence*(3).

Lewis, J. A. (2020). Telecom and National Security (commentary).
Merloe, P. (2017). International electoral espionage is political warfare, violating sovereignty & human rights.
Misuraca, G., & Lusoli, W. (2010). *Envisioning Digital Europe 2030*. European Commission Joint Research Centre Institute for Prospective Technological Studies, Luxembourg, Publications Office of the European Union.
Mohammadi, S., & Kalantari, K. (2024). Prosecution and extradition of cyber criminals in the international criminal system: Challenges and strategies to enhance judicial authority. *Quarterly Journal of International Criminal Law*(4).
Mozaffari Nia, M. (2025). Cyberpower: Nature, dimensions, components, and global indicators. *Monthly Report of Expert Studies of the Islamic Consultative Assembly Research Center*(4).
Nishimura, H., Kanoshima, E., & Kono, K. (2019). *Advancement in Science and Technology and Human Societies*. Science of Societal Safety Living at Times of Risks and Disasters Singapore: Springer. https://doi.org/10.1007/978-981-13-2775-9_2
O'Hanlon, M. (2020). *Forecasting change in military technology, 2020-2040*. Washington D.C.: The Brookings Institution.
Rahimi, Z., & Rashidi, R. (2024). Examining methods for resolving conflicts of laws in Iranian substantive law. *Journal of Law and Political Studies*(1).
SentinelOne. (2025). *What is cyber espionage? Types & examples*. Cybersecurity Magazine.
Sobhe Khiz, R. (2015). Legal challenges of cyber crimes in international law and Iranian legal system. *Quarterly Journal of Information and Criminal Research*(3).
Stuart, B. (2001). *Beyond our control? Confronting the Limits of our Legal System in the Age of Cyber Space*. The MIT Press, Cambridge, Massachusetts London. https://doi.org/10.7551/mitpress/1583.001.0001