Interdisciplinary Studies in Society, Law, and Politics 2025; 4(1): 31-49

ISSLP

Original Research

Study of Opportunities and Challenges of Cyberspace and Its Impact on Cybercrimes in the Armed Forces of Iran

Mohammad. Amirmohammadi[1], Saleh. Abdinezhad[2*], Alireza. Shekarbeigi[3]

[1] Phd Student, Department of Law, Kish International Branch, Islamic Azad University, Kish Island, Iran.
[2] Visiting Assistant Professor, Department of Law, Kish International Branch, Islamic Azad University, Kish Island, Iran
[3] Assistant Professor, Department of Law, Payame Noor University, Tehran, Iran

*** Corresponding author email address**: silahlawyer29@gmail.com

Received: 2024-10-06 **Revised:** 2024-11-20 **Accepted:** 2024-11-27 **Published:** 2025-01-01

In the contemporary era, following the expansion of globalization and the subsequent growth of cyberspace, discussions have increasingly revolved around both physical and virtual spaces. Similar to the physical world, cyberspace has created numerous potentials and challenges, leading to the displacement of many crimes from the physical to the virtual domain. This shift affects various groups, including the armed forces. Given these conditions, the present study seeks to examine the impact of cyberspace on cybercrimes within the armed forces by employing a descriptive-analytical research method. This study poses the following research question: What are the most significant characteristics of cyberspace, and how do these characteristics influence cybercrimes within the armed forces? The findings indicate that the most critical features of cyberspace—globalization, uncontrollability, anonymity, interactivity, and diversity—significantly affect cybercrimes within the armed forces, creating numerous challenges in this regard. The conclusion of the study highlights that in the context of the armed forces and their associated crimes, there has been a notable shift from physical to virtual crimes. This transformation underscores the necessity of revising criminal policy to address emerging cybercrime challenges effectively.

Keywords: *Crimes, Cybercrimes, Cyberspace, Armed Forces.*

How to cite this article:

Amirmohammadi, M., Abdinezhad, S., & Shekarbeigi, A. (2025). Study of Opportunities and Challenges of Cyberspace and Its Impact on Cybercrimes in the Armed Forces of Iran. *Interdisciplinary Studies in Society, Law, and Politics, 4*(1), 31-49. https://doi.org/10.61838/kman.isslp.4.1.4

1. Introduction

With the advent of the new era (the second millennium AD) and the expansion and growth of communication tools—leading to what is referred to as the "global village"—various social necessities have emerged. Given that today's computerized and electronic systems have become deeply integrated into human social life, one of the most contemporary and relevant social issues is cyberspace. Cyberspace possesses unique characteristics and influences all aspects of human life, organizations, and various groups, including the armed forces. This transformation has given rise to a new category of crimes known as "cybercrimes," which can manifest in multiple dimensions and pose significant threats to national interests and security.

In response to these conditions, Iranian legislators have sought to formally recognize cyberspace, define the relevant criminal offenses within the armed forces, and criminalize such acts to mitigate the associated threats and challenges of cybercrimes within the military domain. Therefore, this study is significant for two main reasons: first, it examines the characteristics of

cyberspace and their impact on cybercrimes within Iran's armed forces; second, it explores specific instances of cybercrimes within the military sector and identifies the existing challenges in this field.

Accordingly, the necessity of this study lies in its effort to analyze certain instances of cybercrimes and the existing criminal laws related to them while proposing appropriate solutions to achieve optimal legal and policy measures in this area. As for the novelty of this research, despite the importance of developing military cyber capacity, limited studies have examined the characteristics of cyberspace and their impact on cybercrimes within Iran's armed forces. Nevertheless, gaining a deeper understanding of these challenges is crucial, as it directly influences our comprehension of military cyberization and shapes the trajectory of future cyber conflicts.

The lack of critical attention to understanding the challenges of military cyber capacity development can be attributed to two potential reasons. First, academic research has primarily focused on cyberspace and cybercrimes in a general sense, rather than from the perspective of the armed forces and their specific cybercrimes. Second, studying the impact of cyberspace on cybercrimes within the Iranian armed forces requires an examination of their operations, which, due to the sensitive nature of such information, presents inherent challenges.

Thus, this study will first explore cyberspace and its characteristics, followed by an analysis of specific instances of cybercrimes within the Iranian armed forces. Finally, it will propose solutions to address these challenges.

2. Theoretical Foundations and Concepts

Given the importance of theoretical foundations and concepts in defining the scope and limits of any scientific research, the following section will define and examine the key concepts relevant to this study.

2.1. Armed Forces

The term "armed forces" literally means an army, but in technical terminology, it refers to a country's organized forces that are maintained for ensuring security, independence, territorial integrity, law enforcement, and public order. The preamble of Iran's Constitution, under the section titled "Ideological Army," states: *"In the formation and equipping of the country's defense forces, the emphasis is on faith and ideology as the foundation and criterion. Thus, the Islamic Republic Army and the Islamic Revolutionary Guard Corps are established in accordance with this objective, undertaking not only the protection of borders but also the ideological duty of jihad in the path of God and the struggle to expand the rule of divine law in the world. (Prepare against them whatever force and steeds of war you can muster, to strike terror into the enemy of God and your enemy, and others besides them whom you do not know but whom God knows…)"*

Additionally, the Iranian Constitution states that the armed forces—including the army, the Revolutionary Guard, the police, and the Basij—are responsible for maintaining the country's independence and territorial integrity from both military and non-military threats, both within and, under certain conditions, beyond national borders. Accordingly, these defense institutions, with their vast human and technological resources, play a critical role in safeguarding the territorial boundaries of the Islamic Republic of Iran and ensuring national security.

Based on the above definitions, the armed forces can be defined as comprising the General Staff of the Armed Forces, the Army, the Islamic Revolutionary Guard Corps, the Law Enforcement Force, the Ministry of Defense, and affiliated organizations (Regulations of the Disciplinary Code of the Armed Forces of the Islamic Republic of Iran). This definition highlights two key points. First, unlike the Constitution and other legal texts that discuss the armed forces, this definition has a broader scope, encompassing most military and paramilitary forces. Second, while providing a general definition of the armed forces, it also identifies specific entities included within this category (Fattahi Zafarghandi, 2020).

2.2. Definition of Cyberspace

The term "cyberspace" was first coined by William Gibson in 1982 in his short story *Burning Chrome*, where he used it to describe a computer-generated virtual reality. However, the term became widely recognized in 1984 following its use in Gibson's novel *Neuromancer*.

Etymologically, cyberspace is a compound word. The root of "cyber" originates from the Greek word kybernetes, meaning pilot, governor, or ruler. The term "cyber" is also related to "cyborg," a term that describes

the integration of human and machine, referring to a hybrid of biological and technological systems (Fourkas, 2004).

In line with this etymology, the Oxford English Dictionary defines cyberspace as "the notional environment in which communication over computer networks occurs."

India's National Cyber Security Policy (2013) defines cyberspace as "a complex environment consisting of interactions between people, software, and services, supported by globally distributed information and communication technology (ICT) networks and equipment."

The United Kingdom's Cyber Security Strategy defines cyberspace as "an interactive domain composed of digital networks used to store, modify, and transport information." This definition includes the Internet, as well as other information systems that support businesses, infrastructure, and services (Chawla, 2016).

Thomas Folsom (2007), in his article *"Defining Cyberspace: Finding Real Virtue in Virtual Reality,"* defines cyberspace as "an embodied switch network for moving information traffic, characterized by varying degrees of access, navigation, and increased information activity (and trust)." He further defines the Internet as a gateway to cyberspace, stating that the gateway itself is an embodied switch network for information movement. According to Folsom, the Internet is the most prominent example of such a gateway, while the telephone system is another.

He elaborates that the set of activities that constitute cyberspace is primarily characterized by access, navigation, and information activities, all facilitated through the gateway. Collectively, the gateway and the activities occurring beyond it shape cyberspace in an objective manner, expressing values that can be derived from its intended functions (Folsom, 2007).

2.3. Definition of Cybercrimes

Cybercrime is a widespread phenomenon globally and encompasses a range of activities where individuals disrupt networks, steal important and private information, documents, hack identities and bank accounts, and transfer money to their own accounts. Cybercrime has gained prominence, particularly through the internet, as computers have become central to commerce, entertainment, and governance.

More precisely, cybercrimes—also referred to as computer crimes—can be defined as *"the use of computers as tools for illegal purposes, such as committing fraud, intellectual property trafficking, identity theft, or invasion of privacy. Cybercrime and its impact on society manifest as economic disruption, psychological distress, national defense threats, and more."* Effectively limiting cybercrime requires a proper analysis of its functions and an understanding of its impact on different societal levels. Today, cybercrimes are increasing at an alarming rate, causing significant distress to individuals and organizations. Therefore, cybercrimes are among the major offenses committed by computer specialists (Goni et al., 2022).

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrime as *"crimes committed against individuals or groups of individuals, directly or indirectly, through modern telecommunication networks such as the internet (chat rooms, email) and mobile phones, with a criminal motive to intentionally harm the victim or cause physical or psychological damage or financial loss."* (Goni et al., 2022).

The Oxford Dictionary defines cybercrime as *"criminal activities carried out using computers or the internet."* Cybercrimes can include offenses that resemble conventional crimes but involve computers either as tools, objects, or means of committing the crime. Cybercrime refers to *"any crime that is conducted using electronic communications or information systems through any device, the internet, or a combination thereof."* Cybercrime is a broad term describing various criminal activities where computers or computer networks serve as instruments, targets, or locations of criminal activity. Cybercrimes can halt trains where they operate, misdirect airplanes in flight through false signals, compromise critical military information to foreign nations, and disrupt media and other digital systems (Goni et al., 2022).

Various types of cybercrimes include hacking, virus dissemination, logic bombs, denial-of-service attacks, phishing, email bombing and spamming, web hijacking, cyberstalking, identity theft and credit card fraud, salami attacks, software piracy, cyber pornography, and pharming (Goni et al., 2022).

3. Legislation on Cybercrimes

The expansion of transnational cybercrimes has been exacerbated by the absence of effective global norms and cooperation mechanisms for prosecuting and punishing offenders. The United Nations General Assembly (UNGA) has reflected these concerns by passing several resolutions emphasizing that *"the spread and use of information technologies and tools impact the interests of the entire international community, and criminal misuse of information technology may lead to disastrous consequences. These technologies can potentially be used for purposes that conflict with maintaining international stability and security."*

At the World Summit on the Information Society (WSIS), held in two phases—Geneva in 2003 and Tunis in 2005—the UN actively supported efforts to curb cybercrimes. The International Telecommunication Union (ITU) facilitated Action Line C5, "Building Confidence and Security in the Use of ICTs," in response to which, in 2007, it launched the Global Cybersecurity Agenda (GCA) as a framework for international cooperation in this field (Gastorn).

In the information society, due to the globalization of communications and the vast scope of cyberspace activities, traditional mechanisms have become ineffective in countering cyber intrusions, hacking, viruses, and other threats. These new conditions necessitate modern laws and tools to provide adequate security for protecting digital assets and information in networks and computers. Some countries have been pioneers in developing new legal frameworks and have taken significant steps in this regard. However, in nations that have not yet addressed emerging challenges in cyberspace, including recognizing new cyber environments and enacting necessary laws for regulation, control, and combating cybercrimes, the need for appropriate legal frameworks is critical.

For example, the Council of Europe's Convention on Cybercrime (Budapest Convention) of 2001 provides a framework for defining and classifying cybercrimes (Sobhkhiz, 2014). In advanced countries, legislators have identified various types of cyber offenses and incorporated them into their criminal laws based on societal needs. Concurrently, international bodies have also taken steps to categorize and provide model laws for national legislation.

Among the key international and regional organizations leading efforts in this domain are the Organization for Economic Cooperation and Development (OECD), the Council of Europe (CoE), the International Association of Penal Law, the United Nations, INTERPOL (the International Criminal Police Organization), the Budapest Convention's classification, the Group of Eight (G8) initiative in 1999, and the McConnell Initiative (Sobhkhiz, 2014).

4. International Legal Measures Against Cybercrime

International legal actions play a crucial role in preventing and combating cybercrime. Over the past decade, significant developments have occurred in the establishment of both binding and non-binding international and regional instruments aimed at addressing cybercrimes.

Several key agreements—such as the Council of Europe's Cybercrime Convention, the Shanghai Cooperation Organization (SCO) Cybersecurity Agreement, and the Arab League Cybercrime Convention—are legally binding, imposing obligations on member states. Meanwhile, other documents, including the Commonwealth Model Law, the Draft Model Bill of the Common Market for Eastern and Southern Africa (COMESA), and the Arab League Model Law on Cybercrime, serve as non-binding guidelines for national regulatory development.

Thus, as observed, non-binding instruments have exerted significant influence at both global and regional levels, providing countries with frameworks for aligning their national laws with modern approaches. Besides formal membership and implementation, multilateral cybercrime instruments have also impacted national legislation indirectly—either by serving as a template for non-state actors or by influencing the laws of member states. Notably, there is substantial overlap between these instruments, as many fundamental concepts from the Council of Europe's Cybercrime Convention appear in several other agreements (Sobhkhiz, 2014).

The most effective approach to addressing cybercrime may involve establishing international conventions that recognize cyber-related human rights as a branch of international law. Unlike previous regulatory methods, which have various drawbacks, such an approach faces only one primary challenge: conflicting state interests.

Technologically advanced nations that provide internet services often prefer national or supranational legal frameworks, whereas developing countries that lag in

information and communication technology (ICT) tend to favor international governance in cyberspace.

The earliest international efforts to combat cybercrime date back to the late 20th century. In 1981, at the proposal of U.S. Attorney General Tele Kousak, INTERPOL began coordinating efforts to harmonize national cybercrime legislation. Later, in 1997, the Group of Eight (G8) industrialized nations established the High-Tech Crime Prevention Working Group, drafting ten legal provisions for combating computer crimes (Pournaqdi, 2014).

5. Crimes in the Armed Forces

As is well known, the armed forces constitute an organization and share the characteristics of an organized entity. The individual significance and social cohesion of its members, along with internal motivations within the structure of military power, remain essential factors that cannot be disregarded, even amid increasing organizational complexity and advancements in warfare technologies. In reality, the faith and commitment of military personnel to their organization and their belief in the necessity of combat remain the most fundamental pillars of the armed forces. If this morale is compromised, the effectiveness of the military diminishes.

Given this significance, Huntington argues that today's military possesses four key characteristics:

1. Specialization in weapon management
2. Dependence on the state
3. Internal cohesion
4. A military ideology that fosters individual subordination to collective objectives and ensures discipline and order (Najafi Abrandabadi, 2009).

These considerations highlight the direct correlation between military efficiency and personnel morale, as well as their attitude toward the organization. When military personnel hold a positive perspective, their behaviors align with organizational norms. However, a negative outlook directly influences their conduct, increasing the likelihood of irrational behaviors, including criminal acts.

Thus, military crimes can be defined as "the failure of military personnel to uphold discipline and violations of duties assigned to them by virtue of their profession" (Ardabili, 2003).

The definition of crimes within the armed forces is also stipulated in Note 1 of Article 1 of the Code of Criminal Procedure for the Armed Forces of the Islamic Republic of Iran (approved on May 12, 1985), which states: *"Crimes related to specific military and law enforcement duties refer to offenses committed by members of the armed forces in connection with their military and law enforcement responsibilities as prescribed by law and regulations."*

Furthermore, Article 1 of the Law on Determining the Jurisdiction of Military Prosecutors and Courts (approved on July 28, 1994) also references "specific military or law enforcement crimes."

Based on these definitions, crimes within the armed forces can be classified into two main categories (Farhoudinia, 2011):

1. General crimes: These are offenses that are criminalized in both society and the armed forces, such as theft, embezzlement, forgery, etc.
2. Specific crimes: These are offenses that are only considered crimes within the armed forces and do not constitute criminal acts outside the military framework (Farhodi-Nia, 2011, pp. 32-88).

Examples of specific military crimes include desertion, disobedience of orders, and abandonment of post. Such acts are not considered crimes in civilian society.

6. The Rationale for Criminalizing Certain Military Offenses

Why does the legislator categorize behaviors such as abandoning a post, sleeping on duty, and disobeying orders as crimes? The answer lies in the significance of the armed forces and the necessity of maintaining their authority. A military force must possess high levels of power and efficiency so that it can exercise command within its hierarchical structure whenever necessary. However, crimes and infractions diminish military authority and ultimately reduce the effectiveness of the armed forces (Farhodi-Nia, 2011, pp. 32-88).

A crucial aspect of adjudicating crimes in the armed forces is Article 597 of the Code of Criminal Procedure, which states: *"Crimes related to the specific military and law enforcement duties of armed forces personnel—except for crimes committed in their capacity as judicial officers—*

shall be adjudicated within the Military Judiciary Organization."

This article clearly distinguishes specific military crimes from general crimes within the armed forces.

7. Expansion of Military Judiciary Jurisdiction

A significant legal development occurred through the authorization of the Supreme Leader via a directive issued by his office (No. 13752/1/M, dated August 11, 2020), in conjunction with a directive from the Head of the Judiciary (No. 100/87221/9000, dated August 4, 2020), which expanded the jurisdiction of the Military Judiciary Organization in five key areas:

1. All security-related crimes committed in connection with military service, including those perpetrated by contract personnel or individuals temporarily employed by the armed forces, their affiliated organizations, institutions, and companies not subject to military regulations.
2. Crimes related to classified military information, committed by individuals directly or indirectly involved in procuring military equipment and weaponry.
3. Security-related crimes committed by armed forces personnel during their service period and up to five years after their service ends.
4. All crimes involving weapons and ammunition committed by active-duty military personnel.
5. Crimes related to the performance of special protective and law enforcement duties by security units of executive agencies.

Recognizing this expanded jurisdiction is crucial for two reasons:

1. It provides specific examples of military crimes.
2. It clearly outlines the adjudication process and competent judicial authorities.

A key provision reinforcing the distinction between general and specific military crimes is Note 2 of Article 597, which states: *"Crimes related to specific military and law enforcement duties refer to offenses committed by armed forces personnel in connection with the military and law enforcement responsibilities assigned to them by law and regulations."*

This provision effectively reiterates the concept of specific military crimes.

From the definitions and legal provisions analyzed, it is evident that military crimes threaten the structural integrity of the armed forces. Addressing this issue requires two primary measures:

1. Fostering a positive attitude among personnel toward the organization, as morale directly influences compliance with military norms.
2. Ensuring favorable service conditions and an optimal working environment to mitigate factors contributing to criminal behavior within the armed forces.

8. Characteristics of Cyberspace

With the advancement of globalization and the expansion of technology, cyberspace has experienced significant growth and development. Corresponding to this expansion, cyberspace has acquired unique characteristics, and a proper understanding of these features can be effective in preventing and controlling crimes that arise within its framework. The following section examines the most important of these characteristics.

8.1. The Globalization of Cyberspace

In the information age, all key aspects of human survival—such as security, politics, management, commerce, finance, transportation, infrastructure, postal services, telecommunications, medicine, and science—are highly dependent on information and communication technologies. This dependence raises the argument that the internet, and cyberspace in general, increasingly assumes the characteristics of "the central nervous system of human society", becoming inseparably linked to people's daily lives. A clear example of this phenomenon is social networks, which can rapidly influence the values, beliefs, and behaviors of large social groups. In practice, the internet offers unlimited opportunities for distributing ideologies and various ideas related to the democratic evolution of social relations and human rights (Armencheva et al., 2019).

The information revolution and emerging threats differ significantly from traditional national security concerns. To fulfill their responsibilities—especially those related to national security—states must develop new capabilities to control and protect information and

communication infrastructure from criminal organizations or attempts to infiltrate critical national information systems. Additionally, individuals motivated by various factors can cause significant harm to critical infrastructure, posing severe challenges to the ability of both large and small states to maintain national security (Armencheva et al., 2019).

In the era of nation-states, before the emergence of the global community, power dynamics and political leadership were primarily based on economic and military superiority at both the national and international levels. Consequently, states and international organizations established and imposed legal and social norms and values through laws and treaties to regulate emerging armed conflicts. To achieve this goal more effectively, states have historically developed and continue to develop various military and economic capabilities across land, air, and sea domains (Armencheva et al., 2019).

However, the processes of globalization have introduced a completely new stage in human societies' development, altering international relations' dynamics. These globalization-driven transformations have reshaped the structure of international relations and power centers while redefining the fundamental characteristics of the nation-state. This shift renders outdated ideological paradigms of confrontation irrelevant, as digital technologies introduce new forms of development across nearly every domain—political, economic, social, and military—along with new customs, norms, and challenges.

This transformation forces scholars to reanalyze the nature of globalization and its cyber dimension, or the emergence of cyberspace globalization. From a philosophical perspective, globalization represents a new stage in human evolution, characterized by a high degree of self-organization and adaptability. The expansion of this evolution results from human activity, turning it into a collective, goal-driven endeavor. The most prominent feature of this endeavor is governance.

Although the mechanisms and tools of cyber globalization processes appear fragmented, they remain significant across ideological, political, economic, and military dimensions. This raises the question:

Does a contradiction exist between the evolutionary and governance aspects of cyberspace globalization?

From an evolutionary perspective, cyberspace globalization does not fulfill the goal of creating a fully integrated digital space with equal opportunities for all actors within it. From a governance perspective, cyberspace globalization has shifted from universal and collective objectives for all of humanity toward specific goals that serve the interests of the most powerful players in cyberspace.

At this stage of human development, technological innovations create a new global environment for interactions. However, in reality, this process is a continuation of classical colonialism, which, after post-World War II economic and social expansion, has now transitioned into a “technological” phase.

The result is that economic and social underdevelopment continues for 80% of the world's population, while cyberspace globalization and technological advancements further widen the gap between wealthy and impoverished societies (Armencheva et al., 2019)

8.2. Uncontrollability

At a broad level, the internet and cyberspace as a whole can be perceived as a vast classroom—or, more precisely, a classroom that extends beyond imagination. Millions of people actively use it, interact with one another, and engage in conversations within this domain. The number of possible connections is incredibly vast—practically incalculable and, in a literal sense, infinite (Glanville).

However, cyberspace is not solely inhabited by human users. It also includes automata (such as websites, interactive pages, and databases) that function as users themselves. Many of these automated systems are now highly sophisticated. This means that cyberspace remains beyond human control due to three key factors:

1. The sheer number of people using it
2. The interconnectedness of computers
3. The increasing complexity of automated systems, which also function as independent users (Glanville).

As a result, cyberspace cannot be effectively monitored or regulated. This lack of control is why one of the most defining characteristics of cyberspace is its uncontrollability.

8.3. *Anonymity in Cyberspace*

The latest developments in the cyber domain have introduced a wide range of techniques that allow government authorities, legal entities, and even criminals to interfere with privacy and violate freedom of expression. Various laws and policies enacted by governments have led to extensive surveillance, targeted data collection, online censorship, and cybercriminal attacks. These measures have disrupted individuals' right to privacy, particularly in societies where religious and linguistic minority groups are marginalized.

To counter these restrictions and ensure online privacy, encryption and anonymity play a crucial role in enabling free access to the internet (Madaan, 2023).

Anonymity can be described as engaging in actions or communications without revealing or disclosing one's identity, thus concealing one's true identity. Anonymity can be achieved through the use of a pseudonym or fictitious name that differs from a person's legal or commonly known identity. In essence, anonymity allows individuals to operate in public spaces without disclosing their true identities.

In cyberspace, this means that a person can communicate online without using their real identity, instead adopting an alternative name that renders them unidentifiable and protects their identity. It can be confidently stated that online anonymity is essential for any democratic and free society when used wisely (Madaan, 2023).

Efforts to remain anonymous in cyberspace have led to the emergence of the "Deep Web", which consists of internet content not indexed by search engines such as Chrome. The content available in the Deep Web is generally inaccessible through surface web searches. The majority of untraceable content is located beneath the surface in deeper layers of the web.

Although browsing the Deep Web is not illegal, its legality depends on how it is used. If illicit activities are conducted within it, such actions are considered illegal.

The Dark Web represents the most secure portion of the Deep Web, providing a safe haven for criminals to engage in illicit activities. Therefore, the ability to remain anonymous or conceal users' identities in cyberspace is of paramount importance. This allows users to operate without being tracked.

Online anonymity creates a sense of security, as users feel protected from surveillance and can freely engage in cyberspace without restrictions. The right to anonymity in cyberspace—particularly within the Deep Web—acts as a lifeline for users, enabling them to access valuable information and protect themselves from harassment. This tool is crucial for communication and also shields individuals from severe consequences, such as criminal prosecution.

The most valuable feature of the Deep Web is its ability to ensure privacy and data protection, especially for individuals who may be monitored by authorities and governments seeking to exploit their data for profit (Madaan, 2023).

However, the anonymity provided by the hidden layers of the internet may encourage individuals to engage in illegal activities. Since authorities cannot monitor users, some may feel liberated from social norms and restrictions, leading to a loss of self-awareness. This contributes to mass radicalization and cyber terrorism.

Cyber extremists use various methods to promote their agendas, including social media platforms and anonymous chat rooms to manipulate and recruit young individuals (Madaan, 2023).

Therefore, anonymity in cyberspace is both a benefit and a risk—while it grants users the freedom to express their opinions and raise awareness about realities in their countries, it also attracts criminals, turning the hidden layers of the internet into a hub for illicit activities, ranging from unethical hacking to cyber terrorism.

8.4. *Interactivity in Cyberspace*

The enhancement of personal identity in cyberspace—through social networks or even through simple account creation based on search history—has placed large corporations with vast databases far ahead of governments with active intelligence services and traditional information-gathering structures.

Efforts by authoritarian governments to restrict citizens' access to information have become increasingly challenging. Over time, cyberspace has evolved into a realm of complete freedom, where any individual with access to a computer can challenge powerful governments (Băncilă, 2018).

As the primary actor in the security environment, the state continues to exert dominance over legal regulations concerning cyberspace governance. In this

context, the United States began designing a new communication system in the late 1960s, intended to facilitate communication between key sectors responsible for national defense.

Simultaneously, multinational corporations took the lead in the private sector's development of the internet, ultimately acquiring the right to regulate operational aspects of this new communication environment.

The World Wide Web Consortium (W3C) is a nongovernmental organization responsible for developing standards for cyberspace through the Internet Corporation for Assigned Names and Numbers (ICANN).

This concept extends beyond the simple use of computers and the internet, encompassing all forms of digital communication, including mobile networks, satellite communications, and even secure intranet systems used by large corporations or government structures (Băncilă, 2018).

In general, the internet and cyberspace have profoundly influenced communication and social interactions. The emergence of the World Wide Web in the 1990s provided people with new ways to communicate, fundamentally transforming human interactions.

The impact of cyberspace on communication is immense. Most notably, cyberspace has made communication faster and more efficient.

Emails, instant messaging, and social media platforms such as Facebook and Twitter have replaced traditional letter writing, phone calls, and face-to-face conversations as the primary tools of communication (Ahuja, 2023).

Moreover, the internet has enabled global communication, eliminating geographical barriers and bringing individuals closer together.

However, this newfound ability for instant and effortless communication has also resulted in negative consequences.

For example, many people struggle to disconnect from their devices, constantly bombarded by notifications and messages, leading to mental fatigue and burnout. Additionally, online anonymity can result in a lack of accountability, fostering cyberbullying, trolling, and other forms of online harassment (Ahuja, 2023).

The impact of the internet on social interactions is similarly complex.

On one hand, the internet has facilitated connections among like-minded individuals, allowing people with shared interests and experiences to engage in online communities.

On the other hand, social media platforms have contributed to increased feelings of loneliness and isolation, particularly among younger generations. The constant pressure to present an idealized version of oneself online can lead to feelings of inadequacy and inauthenticity in social interactions.

Furthermore, the internet has transformed how news and information are consumed. With the rise of social media, accessing news from various sources has become easier than ever.

However, this has also led to the spread of fake news and misinformation, which can have severe consequences for democracy and public health (Ahuja, 2023).

The impact of the internet on communication and social interaction is both positive and negative. While it has enhanced communication efficiency and made global interaction more accessible, it has also led to mental exhaustion, diminished authenticity in social interactions, and the widespread dissemination of misinformation.

8.5. Diversity in Cyberspace

Cyberspace can be categorized into various types based on the nature of digital environments and their usage. Understanding these classifications is essential for implementing appropriate cybersecurity measures:

1. Public Cyberspace: Encompasses the internet and other publicly accessible digital spaces, including social media, e-commerce, and public information exchanges.
2. Private Cyberspace: Consists of private networks and systems accessible only to authorized individuals or organizations, such as corporate networks, personal devices, and encrypted communication channels.
3. Social Cyberspace: Falls within public cyberspace and refers to digital spaces where social interactions occur, such as social media platforms, online forums, and digital communities.
4. Commercial Cyberspace: Encompasses online marketplaces and digital financial systems,

including platforms where business transactions take place.

5. Military Cyberspace: A highly secure and independent digital environment used for communications, intelligence, and operational planning by military and defense organizations (SentinelOne, 2024).

9. Instances of Cybercrimes Committed by Armed Forces Personnel in Cyberspace

This section examines certain instances of cybercrimes committed by armed forces personnel within cyberspace.

9.1. Incitement and Rebellion

One of the crimes that can occur within the armed forces today is incitement and rebellion, also referred to as coercion, persuasion, or disobedience. This offense can have serious negative consequences, not only for the inciter and the rebel but also for national security and interests. If this crime occurs within the armed forces, it becomes even more sensitive due to the critical nature of military discipline and obedience.

Due to its high level of sensitivity, Article 23 of the Armed Forces Penal Code states:

"Any military personnel who compel or incite other military personnel or individuals serving in the armed forces to flee, surrender, or rebel, or in any other way create conditions that encourage others to engage in such actions, shall be considered as mohareb (enemy of God) if the offense is committed with the intent of overthrowing the government and collaborating with the enemy, provided that they are aware of its impact on the government's downfall. Otherwise, they shall be sentenced to imprisonment ranging from three to fifteen years."

This provision highlights several key legal principles:

1. The acts mentioned in this article constitute "aiding and abetting" a crime when committed by military personnel. However, the legislator has classified them as independent crimes rather than merely as acts of complicity in treasonous offenses against national security. The penalty prescribed is relatively severe to reflect the gravity of the offense. The legislator, recognizing the risks posed by such actions, has classified them as equivalent to the direct commission of a crime.
2. Establishing the intent to commit treason is a crucial element of this crime. The perpetrator must have the general intent to incite military personnel to rebel, flee, or surrender to the enemy. Given the severe penalties outlined in this article, it appears that the effectiveness of the incitement or coercion in leading to rebellion, desertion, or surrender is a necessary element of the crime. If the incitement or coercion does not lead to such consequences, classifying it as a crime punishable by *moharebeh* (waging war against God) would be illogical and unjustifiable. Moreover, enforcing *mohareb* punishments in such cases would be legally problematic.
3. The provision considers aiding and abetting as an independent offense, meaning that the accomplice is treated as the principal perpetrator of the crime. Since the direct perpetrator (military personnel committing rebellion, desertion, or surrender) does not always perform the material elements of the crime voluntarily, the instigator is considered the primary moral agent behind the offense.

Article 504 of the Islamic Penal Code provides a more comprehensive and precise formulation compared to previous statutes. It clarifies ambiguities present in earlier versions of the law. However, the provisions of Article 504 (Islamic Penal Code, Book Five: Discretionary Punishments, 1996) closely resemble earlier legal texts.

Notably, this article introduces several significant legal improvements:

The article explicitly states “effective incitement to rebellion, desertion, etc.,” whereas previous laws were silent on the necessity of effectiveness. Earlier versions of the law did not specify whether incitement had to result in actual rebellion or desertion to be punishable. The 1996 Penal Code corrected this weakness by ensuring that the impact of incitement and coercion is a necessary element for imposing penalties (Sarikhani, 2005).

Another noteworthy improvement in Article 504 is the distinction between crimes against the government (political crimes) and crimes against national security. In previous versions, the phrases “intent to overthrow the

government" and "collaboration with the enemy" were connected by the conjunction "and", which caused interpretative difficulties. The new law replaced "and" with "or", clarifying that the two offenses are separate but equally punishable as *mohareb* crimes.

A third major improvement introduced by the 1996 Penal Code is the distinction between effective and non-effective incitement or coercion. Earlier laws did not differentiate between these scenarios, whereas Article 504 establishes three levels of penalties:

First level: Effective incitement or coercion to rebellion, desertion, surrender, or non-fulfillment of military duties, with the intent to overthrow the government or weaken national forces, is punishable as mohareb.

Second level: Effective incitement or coercion to rebellion, desertion, or surrender without the intent to overthrow the government or weaken national forces is punishable by imprisonment ranging from two to ten years.

Third level: Non-effective incitement or coercion, without the intent to overthrow the government or weaken national forces, is punishable by imprisonment ranging from six months to three years.

Despite its improvements, Article 504 still contains legal flaws, including:

1. Failure to clearly differentiate crimes against the government from crimes against national security.
2. Equating treason with *mohareb* and applying *mohareb* punishments to all cases indiscriminately.
3. Failure to address cases where incitement or coercion is ineffective but committed with the intent to overthrow the government or weaken national forces.

It appears that both the first and second levels of offenses (effective incitement with or without intent to overthrow the government) are punishable as *mohareb*. However, imposing *mohareb* penalties for non-effective incitement and coercion is excessive and indefensible.

Some legal scholars argue that Article 504 is not silent on this issue, as the term "effective" in the statute implies that non-effective incitement is excluded from *mohareb* punishments. However, this interpretation is flawed because in criminal law, interpretations should be explicit rather than inferred. Additionally, Article 11, Clause 4 of the Armed Forces Crimes Act supports the position that non-effective incitement should not be considered a criminal offense under this provision.

9.2. *Disclosure of Military Identity and Records of Activities of Oneself, Colleagues, and Commanders*

The Armed Forces of the Islamic Republic of Iran must protect their scientific and military achievements. If proper measures are established to ensure an information protection culture, military personnel will be less vulnerable to internal and external threats and conspiracies. Their vigilance will strengthen national defense and security while preventing potential risks. One of the fundamental principles of information protection within the armed forces is the preservation of military identity and the confidentiality of one's own activities, those of colleagues, and those of commanders. Violating this principle constitutes a crime with serious consequences for both the armed forces and national security.

Recognizing the critical nature of this issue, the legislator incorporated this principle into Article 27 of the Armed Forces Crimes Penal Code (2003), which states:

"Any military personnel who, due to negligence, recklessness, carelessness, or failure to observe government regulations, cause the disclosure of information, decisions, or the loss or destruction of documents mentioned in Article 27 of this law shall be sentenced according to the classification of the disclosed documents as follows:

a. *If the documents, discussions, information, or decisions are classified as "Top Secret," the offender shall be sentenced to imprisonment from six months to two years.*

b. *If the documents, discussions, information, or decisions are classified as "Secret," the offender shall be sentenced to imprisonment from three months to one year.*

c. *If the documents, discussions, information, or decisions are classified as "Highly Confidential," the offender shall be sentenced to imprisonment from two months to six months.*

Note: *If the documents, discussions, information, or decisions are classified as "Confidential," the offender shall be subject to disciplinary punishment by the relevant commander or superior officer.*

This article and its accompanying note indicate several key legal points:

1. The disclosure of military identity and records of one's activities and collaborations is explicitly

criminalized. This provision aligns with Article 26, which defines the types of classified identity and activity-related documents and stipulates criminal penalties for violations in Article 27.

2. The legislator distinguishes between the disclosure of "classified" and "non-classified" documents, ensuring that criminal penalties apply only to classified materials, while disciplinary actions apply to confidential information.
3. Although the Armed Forces Cybercrime Law does not explicitly classify disclosure crimes in cyberspace as distinct offenses, such crimes fall under general laws like the 2003 Armed Forces Penal Code.

A crucial issue to consider is the relationship between the Armed Forces Penal Code and the Cybercrime Law. The Cybercrime Law is considered a general law in comparison to the Armed Forces Penal Code because it is part of Iran's Islamic Penal Code, which itself is a general law. Article 55 of the Cybercrime Law explicitly states that its provisions extend from those of the Islamic Penal Code, reinforcing this classification.

Therefore, Article 131 of the Armed Forces Penal Code (2003) is considered a special law in relation to the broader Cybercrime Law, which covers a wider range of offenses. Based on a well-established legal principle accepted by most legal scholars, a later general law does not repeal an earlier special law. Consequently, Article 131 remains in force for military personnel, and the newer Cybercrime Law cannot be applied to offenses already covered by Article 131.

However, in cases where the Cybercrime Law covers offenses not addressed in the Armed Forces Penal Code, such as:

- Unauthorized access and interception
- Attempting to access classified data
- Violating security measures of computer or telecommunications systems
- Negligence leading to unauthorized access to sensitive data

Then, the Cybercrime Law applies to military personnel as well if they commit such offenses.

If a military personnel member commits a cybercrime, the following legal procedure must be followed:

1. First, the offense must be examined under Article 131 of the Armed Forces Penal Code to determine whether it falls under the specific military crimes defined in that law.
2. If the offense aligns with one of the defined military crimes, the case shall be adjudicated based on the Armed Forces Penal Code.
3. If the offense does not correspond to any military crime defined in Article 131, such as crimes outlined in Chapter Four of the Cybercrime Law or Sections One and Two of Chapter One of the same law, the case shall be referred to the Cybercrime Law for resolution (Fattahi Zafarghandi, 2020).

9.3. Unauthorized Interception

Unauthorized interception, regardless of the method used, is prohibited under both Islamic principles and Iranian law. Islam considers eavesdropping and espionage as forbidden acts, given their potential to lead to sin and numerous harmful consequences for the targeted individual. This prohibition has been reflected in Iranian law, as enshrined in Article 25 of the Constitution, which explicitly bans eavesdropping or interception, except as provided by law.

The legal enforcement of this constitutional provision is stipulated in Article 582 of the Islamic Penal Code, which states:

"Any government employee or official who, in cases not authorized by law, opens, withholds, destroys, inspects, or intercepts private correspondence, communications, or telephone conversations, or discloses their contents without the owner's consent, shall be sentenced to imprisonment from one to three years or a fine ranging from 6,000,000 to 18,000,000 rials."

However, in the amendment to this article on June 19, 2024, the penalty was revised to imprisonment of one to three years or a fine ranging from 264,000,000 to 825,000,000 rials.

It is notable that the legislator has only criminalized interception by government officials, while remaining silent on unauthorized interception by private individuals.

In the digital space, the legislator seeks to safeguard individuals' privacy and has consequently criminalized unauthorized computer interception (Mohammad Nasel, 2019).

Thus, one of the instances of cybercrimes within the armed forces involves the unauthorized interception of

military data. This offense involves the illegal acquisition of computer data during its transmission, as interception refers to receiving transmitted content. Since physically receiving information constitutes an act of data acquisition, it is applicable to transmitted data as well.

In this regard, Iranian lawmakers have drawn inspiration from Article 3 of the Budapest Convention on Cybercrime, which states:

"Each Party shall adopt such legislative and other measures as may be necessary to criminalize, as per their domestic laws, the intentional interception, without right, of non-public transmissions of computer data to, from, or within a computer system, including electromagnetic emissions carrying such data. Parties may require that the offense be committed with wrongful intent or that the computer system is connected to another computer system." (Jalali Farahani, 2016, p. 28).

Iranian legislators have incorporated these principles into Article 2 of the Cybercrime Law Amendments (2024), which states:

"Anyone who unlawfully intercepts the transmission of non-public content in computer or telecommunication systems, or through electromagnetic or optical waves, shall be sentenced to imprisonment from six months to two years or a fine ranging from 25,000,000 rials (2,500,000 tomans) to 150,000,000 rials (15,000,000 tomans), or both."

Based on the above legal provisions, it can be inferred that unauthorized interception is a crime against data confidentiality. The origin and destination of the intercepted data must involve military personnel, who possess the authority to send and receive classified content. Thus, for the crime to be established, the transmitted content must be exchanged within a private military network between two or more military personnel.

A violation occurs when:

1. A military personnel member without proper authorization sends classified content from the source.
2. Another unauthorized military personnel intercepts the transmitted data at an intermediary point.
3. A third unauthorized military personnel receives the data at the destination.

In such cases, all three individuals commit the crime of unauthorized interception (Marsi & Zarang, 2023, pp. 177-187).

For the crime of unauthorized interception, the offender must:

1. Be aware that the intercepted content involves military information (knowledge of the subject and its characteristics).
2. Lack legal authorization from a competent authority (knowledge of the legal conditions).

Given the specific nature of military offenses, legislators have adopted differentiated criminal policies based on the status of the offender:

1. If the offender is a civilian, the punishment follows Article 730 of the Islamic Penal Code, which prescribes imprisonment of six months to two years or a fine ranging from 25,000,000 to 150,000,000 rials, or both penalties.
2. If the offender is military personnel, the punishment follows Clause (a) of Article 754 of the Islamic Penal Code, which increases the maximum punishment by two-thirds.
3. If the intercepted data belongs to the government, public institutions, or service providers, Clause (c) of Article 754 applies, imposing an additional two-thirds increase in penalties specified under Article 729.

Distinction Between Clauses (a) and (c) of Article 754:

- Clause (a) applies when the offender is a military personnel member.
- Clause (c) applies when the intercepted data belongs to the government or military institutions, even if the offender is not a military personnel member.

This differentiation emphasizes the legislator's commitment to protecting classified military data, regardless of the identity of the perpetrator (Mersi & Zarang, 2023).

9.4. Unauthorized Access

Unauthorized access is one of the fundamental cybercrimes, playing a pivotal role in facilitating other computer-related offenses, particularly pure cybercrimes. Consequently, in cyberspace, it is regarded as a primary offense.

Unauthorized access can be defined as: *"Unlawful intrusion into data, computer systems, or telecommunications networks protected by security measures, which ultimately violates individuals' privacy and the confidentiality of their data and information"* (Shahmoradi, 2016).

Alternatively, it can also be described as: *"Illegal penetration into a person's protected computer system or network"* (Pournaqdi, 2014).

These definitions indicate that unauthorized access encompasses crimes that pose severe threats to security, particularly the confidentiality, integrity, and availability of computer systems and data. The need for protection reflects the interests of organizations and individuals in managing, executing, and controlling their systems without interference.

Any unauthorized intrusion—such as hacking, cracking, or forceful entry into a computer system—should be deemed illegal. This principle has been criminalized under Iranian law.

Article 1 of the Cybercrime Law Amendments (2024) states: *"Anyone who unlawfully accesses data or computer or telecommunication systems protected by security measures shall be sentenced to imprisonment from 91 days to one year or a fine ranging from 20,000,000 rials (2,000,000 tomans) to 80,000,000 rials (8,000,000 tomans), or both penalties."*

A critical issue in the military context is whether unauthorized access is classified as an absolute or result-based crime.

The European Committee of Cybercrime Experts considers unauthorized access to be a result-based crime, meaning that for the offense to be established, the intrusion must lead to a specific consequence.

Similarly, the Budapest Convention on Cybercrime, in Article 2, Section 1, Chapter II, criminalizes: *"Any intentional and unauthorized access to all or part of a computer system."*

Since Iranian law remains silent on whether unauthorized access is absolute or result-based, some scholars argue that Iranian cybercrime law has adopted the result-based approach, given that Article 4 of Iran's Cybercrime Law is derived from the Budapest Convention.

Thus, in the military context, due to the high sensitivity of national security, any attempt by military personnel to access restricted information—whether successful or not—constitutes unauthorized access.

Accordingly, for unauthorized access to be established in the military, only general criminal intent is required; proving specific intent (such as intent to harm) is unnecessary (Fattahi Zafarghandi, 2020).

Given that the armed forces handle highly classified documents, discussions, and decisions, unauthorized access to such information should be categorized based on the level of confidentiality:

1. Ordinary
2. Secret
3. Highly Confidential

To determine the appropriate punishment, reference can be made to Article 26 of the Armed Forces Crimes Penal Code (2003), which provides a framework for sentencing based on the level of classification.

A significant legal issue arises: *"If a military personnel member commits a cybercrime such as computer espionage or forgery, should the case be adjudicated under the Armed Forces Crimes Penal Code (2003) or the Cybercrime Law (2009)?*

Furthermore, what is the position of the Cybercrime Law in adjudicating military cyber offenses in military courts and prosecutor's offices?

There are two conflicting judicial opinions among military judiciary judges regarding whether Article 131 of the Armed Forces Penal Code has been repealed by the Cybercrime Law:

The first view argues that with the enactment of the Cybercrime Law (2009)—which explicitly addresses cybercrimes within the armed forces in Article 26 and mandates military courts to establish special branches for cybercrime cases in Article 30—Article 131 of the Armed Forces Penal Code has been repealed. Thus, all cyber offenses committed by military personnel should be prosecuted under the Cybercrime Law.

The second view, held by a significant number of military judges, asserts that Article 131 remains in force because:

- Article 131 is a special law, whereas the Cybercrime Law is a general law with broader scope.
- A general law enacted later does not repeal a prior special law unless explicitly stated, a principle widely accepted among legal scholars.

- Therefore, Article 131 still applies to cybercrimes explicitly listed within it, and the Cybercrime Law cannot be invoked for those specific crimes.
- However, if the Cybercrime Law criminalizes offenses not covered by Article 131—such as unauthorized access, illegal interception, attempted access to classified data, security breaches of computer or telecommunication systems, or negligence leading to unauthorized data access—then the Cybercrime Law applies to military personnel as well.

When a military personnel member commits a cybercrime, the following legal framework applies:

1. First, the act must be assessed under Article 131 of the Armed Forces Penal Code to determine whether it falls under a predefined military offense.
2. If the act aligns with a military cyber offense, the case must be adjudicated under Article 131.
3. If the act does not correspond to any military cyber offense, such as crimes covered in Chapter Four of the Cybercrime Law or Sections One and Two of Chapter One of the same law, the Cybercrime Law will apply (Fattahi Zafarghandi, 2020).

10. Challenges of Cybercrimes in the Armed Forces

With the emergence of cyberspace, many believed it to be a new revolution in human life, offering unprecedented opportunities for progress. However, as cyberspace expanded, its challenges became increasingly evident, exposing the armed forces to numerous threats. This section examines some of these critical challenges.

10.1. Slow Law Enforcement and Coordination of National Frameworks at the International Level

Since Sir Robert Peel established the world's first professional police force, the Metropolitan Police of London, in 1829, the nature of conventional crimes has remained largely unchanged (Goodman, 1997).

Traditional crimes are primarily local, as both the criminal and the victim are situated within the same geographical jurisdiction. However, cyberspace eliminates this localization, enabling criminals to commit offenses from any location worldwide. As a result, transnational criminal activities have surged.

While criminals swiftly adapt to new technologies, law enforcement agencies struggle to keep pace. Several factors contribute to this lag, with budget constraints and competing priorities being among the main challenges (Goodman, 1997).

Legal frameworks require substantial time to evolve, and an even greater challenge lies in harmonizing national laws at the international level. As global travel increased significantly over the past century, the need for extraditing criminals across jurisdictions became apparent. Even before cybercrimes crossed national borders, traditional criminal cases often presented complex legal issues.

This jurisdictional challenge applies equally to cybercrimes within the armed forces, as such offenses are no longer confined to national borders. When military cybercrimes escalate to the international level, law enforcement faces significant difficulties in preventing their spread and prosecuting perpetrators.

10.2. The Extradition Challenge

Historically, most legal disputes between nations arose from differences in domestic laws, where an act considered lawful in one country might be illegal in another. A secondary legal challenge occurs when:

1. The accused is located in one country (X) while the victim resides in another (Y).
2. Both the accused and the victim belong to the same jurisdiction, but the criminal evidence is located abroad.

In extradition cases, one country transfers a suspect to another for prosecution. Extradition is generally governed by bilateral or multilateral treaties. A fundamental principle of extradition is the requirement of "dual criminality", meaning that the crime must be considered illegal in both jurisdictions. Without this principle, extradition is not possible.

Regarding cybercrimes within the armed forces, the extradition challenge is particularly problematic due to the fragility of digital evidence. The timely collection of electronic evidence is critical for successful prosecution. However, when cases involve international cyber offenses, law enforcement agencies face overwhelming

obstacles in securing, preserving, and presenting evidence.

10.3. The Challenge of Identifying Actors

One of the most pressing challenges in cyberspace is the involvement of both state and non-state actors. Distinguishing between these two groups is not always straightforward, complicating law enforcement efforts.

Independent states are responsible for ensuring that non-state actors within their jurisdiction adhere to the law, including their international legal obligations.

For example, cybercriminals or terrorists operating in Country A who target victims in Country B may remain beyond the reach of law enforcement agencies in Country B. However, under international treaties, Country A is still responsible for addressing cybercrimes originating from its territory.

Effective enforcement requires close, proactive, and flexible cooperation between law enforcement agencies in both countries. As the number of participating nations increases, the complexity of international cooperation also intensifies.

A further concern is state actors using cyberspace to advance strategic interests while concealing their involvement. The Snowden revelations demonstrated how governments leverage cyberspace for intelligence gathering and cyber operations (Podhorec, 2012, p. 19).

This poses a dilemma for the global community, as certain states exploit cyber anonymity to further their geopolitical objectives while simultaneously seeking international cooperation against cyber threats.

10.4. The Attribution Challenge

Unlike nuclear tests, which can be easily detected by international monitoring mechanisms, cyberattacks present a significant attribution challenge. For instance, the Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO) effectively identified North Korea's nuclear tests in 2006 and 2009, leading to international condemnation and response (Meyer, 2011).

However, in cyberspace, attackers can easily mask their identities, making it appear as if an attack originated from a third party. This complicates efforts to identify perpetrators and hinders retaliatory or defensive actions.

The current level of research on attribution remains inadequate, and without credible documentation, cybercrime treaties cannot be effectively enforced. Mutual trust between signatory states is essential, as enforcement relies on the shared commitment to identifying cybercriminals (Meyer, 2011).

In the context of cybercrimes within the armed forces, attribution becomes a major concern when:

1. A military personnel member exploits cyber anonymity to threaten national security.
2. A military operative engages in cyber espionage, playing a dual role to manipulate or exploit sensitive data.

Both scenarios pose severe security risks and demand advanced attribution methods to detect, prevent, and mitigate such threats.

10.5. The Jurisdiction Challenge

Since hostile cyber activities are not confined to national security concerns, international legal frameworks are needed to regulate and monitor such actions. The 2001 Budapest Convention on Cybercrime, developed by the Council of Europe, represents an international effort to address cybercrime.

However, the Budapest Convention faces significant obstacles, including:

1. Lack of mutual trust among signatory states.
2. Operational limitations, particularly in remote access to suspect computer systems for timely evidence collection.

Despite Iran and its armed forces adopting many provisions from the Budapest Convention, numerous jurisdictional challenges persist both internationally and domestically.

Given the unique nature of cybercrimes, which often involve remote access to computer systems, the jurisdiction challenge remains unresolved (Saran, 2014).

10.6. The Uncontrollability of Cybercrimes

The globalization of cyberspace has introduced new geopolitical realities, reshaping power dynamics among major political actors. While political and power relations remain complex, the digital revolution has accelerated change, driven by rapid technological advancements.

The internationalization of cyber activities has fundamentally transformed the security environment. One of the greatest challenges for nation-states is their inability to control many events occurring in cyberspace. Whether willingly or unwillingly, the information revolution has altered power relations, making authority more decentralized. Governments now operate in an information-driven global landscape, where new models of political cooperation, competition, and confrontation have emerged.

In this environment:

1. Political processes occur in real time.
2. Physical borders lose their significance.
3. Traditional geopolitical concepts are being redefined.

While nation-states remain the primary political actors, their power is steadily declining. Consequently, governments are seeking new means of influence, particularly through information control and digital superiority (Podhorec, 2012).

11. Conclusion

The criminalization of cybercrimes has emerged as a direct consequence of the expansion and development of cyberspace. The emergence of cyberspace has resulted in two key developments: the creation of new offenses that had no precedent in the physical world and the transfer of certain traditional crimes from the physical domain to cyberspace. These developments have been largely driven by the uncontrollable nature of cyberspace, its confidentiality, and the anonymity of offenders.

As a result, the armed forces have also been significantly impacted by cyberspace. Given their critical role and strategic significance, governments—including Iran—have attempted to define and criminalize cyber offenses within military contexts. However, a review of existing laws indicates that there is no comprehensive and specific legal framework dedicated exclusively to cybercrimes within the armed forces. Instead, these offenses are primarily governed by general laws, such as the Cybercrime Law. Despite this, cybercrimes committed by military personnel have received special attention and heightened sensitivity.

The study indicates that while Article 504 of the Islamic Penal Code addresses "effective incitement to mutiny, desertion, and insubordination," earlier laws failed to explicitly define or distinguish these acts. The article introduces a clear distinction between offenses against the government (political offenses) and offenses against national security and a differentiation between effective and ineffective incitement or coercion. However, certain legal gaps remain, including the failure to address ineffective incitement with the intent of overthrowing the government or aiding enemy forces.

The law does not clearly define the scope of military service records or distinguish between different classifications of identity-related documents. Additionally, it does not explicitly criminalize trained personnel who disclose classified information.

The study highlights significant legal ambiguities regarding unauthorized access to military data. Specifically, there is an ongoing debate between the applicability of the Cybercrime Law (2009) as a general law and Article 131 of the Armed Forces Penal Code (2003) as a specialized law. One legal perspective argues that Article 131, being a special law, should prevail, as a general law cannot repeal a prior special law. This implies that cyber offenses committed by military personnel should be adjudicated under Article 131, except in cases where the Cybercrime Law criminalizes offenses not covered under military law. The opposing view contends that Article 131 has been implicitly repealed by the Cybercrime Law, particularly given Article 26 of the Cybercrime Law, which explicitly states that military cyber offenses fall under its jurisdiction. This legal inconsistency remains unresolved, as Article 131 does not encompass all possible cyber offenses, and its broad application could lead to overly expansive interpretations inconsistent with the principle of legality.

The study confirms that all forms of unauthorized interception are prohibited, both under Islamic law and Iranian legal provisions. However, a major legal gap exists, as Iranian law does not explicitly define the scope and limitations of authorized surveillance. To address these ambiguities, the legislature should clearly delineate the legal conditions under which surveillance is permitted to eliminate legal uncertainties.

Having adequate knowledge and capabilities to engage in cyber operations is essential for military personnel. This capability is not only crucial for developing a strong defense but also for effectively supporting military operations. Military strategies should emphasize the advancement of assets, methodologies, and expertise

specifically designed to enhance cyber capabilities within the armed forces.

The absence of a dedicated legal framework addressing military cyber offenses presents a fundamental challenge. Article 131 of the Armed Forces Penal Code does not comprehensively cover all cyber offenses committed by military personnel. The conflict between general and military-specific laws, particularly between the Cybercrime Law and the Armed Forces Penal Code, must be resolved.

To ensure legal clarity and effective enforcement, it is imperative to enact a specialized Military Cybercrime Law that explicitly defines all military-related cyber offenses, criminalizes specific cyber activities within the armed forces, and resolves conflicts between the general Cybercrime Law and the Armed Forces Penal Code. This would allow for a more comprehensive approach to military cybercrimes while eliminating inconsistencies that hinder effective prosecution and enforcement.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

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

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Ahuja, P. (2023). The impact of the Internet on communication and social interaction. https://www.linkedin.com/pulse/impact-internet-communication-social-interaction-priyanka-ahuja

Ardabili, M. A. (2003). *General Criminal Law* (Vol. 1). Mizan Publishing.

Armencheva, I., Atanasova, N., & Ivanov, I. (2019). CYBER GLOBALIZATION AS AN IN/STABILITY FACTOR. *Ijasos- International E-Journal of Advances in Social Sciences*, 71-81. https://doi.org/10.18769/ijasos.531497

Băncilă, A. (2018). CYBERSPACE - THE NEW DIMENSION OF HUMAN INTERACTION. *Scientific Bulletin*, *XXIII*(1(45)). https://doi.org/10.2478/bsaft-2018-0001

Chawla, R. (2016). Importance of cyberspace for economic Growth and Development - IPleaders. https://blog.ipleaders.in/importance-cyberspace-economic-growth-development/

Farhoudinia, H. (2011). Crime Prevention in the Armed Forces. Special Issue of the Second Scientific-Applied Workshop on Crime and Social Harm Prevention Management, Tabriz.

Fattahi Zafarghandi, S. (2020). Prevention of Cyber Espionage Crimes in the Armed Forces and Its Role in Ensuring the Right to Security. *Biannual Journal of Islamic Human Rights Studies*, *9*(18).

Folsom, T. (2007). Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). *Tulane Journal of Technology & Intellectual Property*, *9*, 75-121.

Fourkas, V. (2004). What is 'cyberspace'? *WACC*. https://www.researchgate.net/publication/328928631_What_is_'cyberspace'#:~:text=Cyberspace%20is%20a%20spatial%20system,an%20artefact%20but%20as%20a

Gastorn, K. RELEVANCE OF INTERNATIONAL LAW IN COMBATING CYBERCRIMES: CURRENT ISSUES AND AALCO'S APPROACH.

Glanville, R. The Value of being Unmanageable: Variety and Creativity in CyberSpace. *CybernEthics Research*.

Goni, O., Ali, M. H., Showrov, Alam, M., & Shameem, M. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, 29-39. https://doi.org/10.56556/jtie.v1i2.113

Goodman, M. D. (1997). Why the police don't care about computer crime. *Harvard Journal Law & Technology*, *10*, 465-469.

Madaan, S. (2023). THE DIGITAL CLOAK - ANONYMITY in CYBERSPACE. *Cyber peace corps*. https://www.cyberpeacecorps.in/the-digital-cloak-anonymity-in-cyberspace/

Mersi, H., & Zarang, M. (2023). Pathology of Iran's Criminal Policy Regarding Unauthorized Acquisition of Military Computer Data. *Quarterly Scientific Journal of Judicial Law Perspectives*, *28*(103).

Meyer, P. (2011). CYBER-SECURITY THROUGH ARMS CONTROL. *The RUSI Journal*, *156*(2), 22-27. https://doi.org/10.1080/03071847.2011.576471

Mohammad Nasel, Z. (2019). A Comparative Study of Unauthorized Computer Interception in the Criminal Laws of Iran, England, and France. *Quarterly Journal of Information and Criminal Research*, *15*(1).

Najafi Abrandabadi, A. H. (2009). Fair Prevention of Crimes in the Armed Forces of the Islamic Republic of Iran. In *Criminal*

Sciences (A Collection of Articles in Honor of Dr. Mohammad Ashouri). Samt.

Podhorec, M. (2012). CYBER SECURITY WITHIN THE GLOBALIZATION PROCESS. *DOAJ (DOAJ: Directory of Open Access Journals)*, 19-26. https://doaj.org/article/8770bd37c8954fc59cbeabee106b26e0

Pournaqdi, B. (2014). Cyber Terrorism and Cyber Crimes in the International Legal System. *Quarterly Journal of Law Enforcement Knowledge of Semnan*, *4*, 10-23.

Saran, S. (2014). Internet realpolitik. *ORF Cyber Monitor*, *II*(3).

Sarikhani, A. (2005). *Crimes Against Security and Public Safety*. Qom University Publications.

SentinelOne. (2024). What is Cyberspace? Types, Components & Benefits. *SentinelOne*. https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-cyberspace/

Shahmoradi, K. (2016). Legal Examination of the Crime of Unauthorized Access to Data and Computer Systems in Iranian Law. National Conference on Future Studies,

Sobhkhiz, R. (2014). Legal Challenges of Cyber Crimes in International Law and the Iranian Legal System. *Quarterly Journal of Information and Criminal Research*, *10*(3), 118-137.