Representation of Preventive Strategies for Cybercrimes in Critical Energy Infrastructures with an Emphasis on the Role of the Energy Police

1. Soudabeh Soleimani: PhD Student, Department of Criminal Law and Criminology, Boushehr Branch, Islamic Azad University, Boushehr, Iran
2. Behzad Razavifard*: Associate Professor, Department of Criminal Law and Criminology, Faculty of Law and Political Science, Allameh Tabatabaei University, Tehran, Iran
3. Maryam Safaei: Assistant Professor, Department of Law, Boushehr Branch, Islamic Azad University, Boushehr, Iran

***Correspondence: e-mail: bzoudlaw.110@gmail.com**

Abstract

The emergence of computer and internet technology has not only revolutionized human life but has also facilitated the rise of cybercrimes, which pose a serious threat to critical infrastructures, particularly in the energy sector. These tools function both as instruments for committing crimes and as targets of such crimes. In Iran, the enactment of the Computer Crimes Act in 2009 aimed to establish a legal framework to combat these offenses. However, significant legal gaps remain in the domain of cybersecurity offenses. This study, employing a descriptive-analytical method, examines preventive strategies against cybercrimes targeting critical energy infrastructures and highlights the role of the Energy Police as a key actor in this field. Cybercrimes, due to the lack of necessity for the offender's physical presence, have a higher likelihood of occurrence and recurrence and may acquire both domestic and international dimensions. Today, cyber warfare is an integral part of inter-state competition, and energy infrastructures, as the backbone of economic and security frameworks, constitute the primary targets of these crimes. Various factors, including political, military, economic, and cultural motives, contribute to the commission of these offenses. From a legal perspective, challenges such as legislative gaps, the absence of effective guarantees to prevent recidivism, and the lack of deterrence in certain penalties persist. The prevention of these crimes requires collaboration and coordination among various institutions at both criminal and non-criminal levels. In this regard, the Energy Police, as a specialized entity, can play a significant role in identifying, preventing, and countering cyber threats in the energy sector. Despite the enactment of the Crime Prevention Act in 2011, criticisms have been raised regarding its excessive generality and the lack of effective coordination among relevant institutions. Ensuring cybersecurity in energy infrastructures necessitates continuous and coordinated efforts across multiple levels.

Keywords: Prevention, Preventive Strategies, Cybercrimes, Critical Energy Infrastructure, Energy Police

Received: 22 February 2024
Revised: 12 March 2024
Accepted: 24 March 2024
Published: 01 April 2024

Citation: Soleimani, S., Razavifard, B., & Safaei, M. (2024). Representation of Preventive Strategies for Cybercrimes in Critical Energy Infrastructures with an Emphasis on the Role of the Energy Police. *Legal Studies in Digital Age*, 3(2), 47-58.

1. Introduction

With the advent of Information and Communication Technology (ICT) tools in human life, societies have transitioned from traditional and rudimentary communication methods to modern and electronic interactions. These technologies have eliminated geographical barriers, enabling users to interact with each other beyond national or regional limitations, giving rise to the concept of the "global village." In this modern village, individuals are continuously connected, sharing their perspectives, data, and thoughts with others. These tools have provided an unparalleled platform for collective progress, such that today, unlike in the distant past, access to knowledge and learning is no longer confined to a specific group or class but is available to all, fostering intellectual advancement. This transformation has also affected the energy sector, introducing new legal and security challenges.

A defining characteristic of cyberspace that distinguishes it from other communication tools is the astonishing speed of data transmission and the crucial role of users in the creation and dissemination of information. In this space, individuals have shifted from being passive recipients to becoming active participants in the information exchange process. This transformation has reached a point where former recipients have now become "creative users," meaning they are not only consumers of information but also contributors to and influencers of content production. In the energy sector, this dynamism has led to the emergence of "prosumers"—producers and consumers—who utilize digital systems for energy management and exchange. However, these very features make energy infrastructures vulnerable to cyber threats, as high-speed access and widespread connectivity facilitate advanced cyberattacks on critical facilities such as power grids and energy transmission lines.

In response to the increasing prevalence of cybercrimes in the energy sector, the need for the development and implementation of effective criminal policies is more urgent than ever. Iran, due to existing limitations in its legal and judicial system, faces multiple challenges in combating these types of crimes. These challenges include deficiencies in criminal laws, a lack of coordination between legislative and executive policies, and inadequate empowerment of human and technical resources. Currently, Iran's criminal policy regarding energy protection and its related infrastructures, especially against cyber threats, requires updates and reforms. The necessity of this research becomes evident due to several weaknesses in Iran's legal and judicial system. Existing Iranian laws concerning cyber threats, particularly in the energy sector, contain significant ambiguities and shortcomings. These deficiencies allow cybercriminals to evade appropriate punishment. Moreover, various governmental and non-governmental entities responsible for managing and safeguarding energy infrastructures operate independently, with insufficient coordination among them. Additionally, legal experts, cybersecurity professionals, and energy management specialists in Iran have not received adequate training and have limited access to advanced technologies.

From an energy law perspective, these changes necessitate the formulation of new legal frameworks that simultaneously foster innovation and ensure cybersecurity. For instance, the digitization of energy networks has enhanced efficiency and expanded the use of renewable resources, but it has also made these networks attractive targets for hackers. Cyberattacks such as the intrusion into Ukraine's power system in 2015 or the disruption of the Colonial Pipeline in the United States in 2021 have exposed the vulnerability of these infrastructures, underscoring the need for stricter regulations to combat cybercrimes. Legislators must strike a balance between technological advancement and the protection of energy facilities to mitigate the economic and security repercussions of these threats. In reality, ICT tools have democratized access to knowledge and resources in the energy sector, while simultaneously introducing emerging challenges to energy law and cybersecurity. This domain, in which users actively contribute as creators and consumers, requires regulations that both harness its potential and minimize the risks associated with cybercrimes targeting critical infrastructures.

2. Conceptual Analysis

Cyberspace, due to its remarkable capabilities and features, facilitates the ease of committing crimes, the transnational nature of offenses, a decrease in the age of offenders, widespread damages, and an increase in the number of victims, while also enabling anonymity. In this context, identifying the obstacles to preventing cybercrimes is crucial for implementing effective strategies to control these threats (Davoodi Dehaqani, 2019).

2.1. Cyberspace and Emerging Challenges

Modern Information and Communication Technology, as exemplified by cyberspace, provides a platform for the rapid exchange of information and the establishment of communications. This space functions as a vast source of "information energy," which can be both constructive and destructive. Cyber fraud, privacy violations, the dissemination of false information, and financial crimes have emerged as serious threats to the security of individuals and societies. As a result, the necessity for a "cyber energy policy" has become evident to manage this vast flow of information and prevent its misuse or dissipation.

2.2. Criminal Policy and Prevention

Criminal measures, such as punitive actions following the commission of a crime, are not sufficient on their own and face multiple obstacles, including the complexity of tracking cybercriminals and the transnational nature of these offenses. In this regard, "prevention" emerges as a proactive and optimal approach, which can be associated with the concept of "energy management" in cyberspace. Preventive policy, akin to energy consumption management in a system, aims to reduce resource wastage (such as security, public trust, and privacy) and prevent abuse before it occurs (Esmaeilzadeh, 2018).

2.3. Situational Prevention and Its Relation to Energy Policy

Situational prevention, introduced in the text as a key measure, includes actions such as restricting access to crime-facilitating tools, enhancing system security, and monitoring user activities (Ebrahimi, 2012). This approach can be likened to "controlling energy flow" in a network. Just as energy systems prevent leakage or misuse through the installation of filters and regulators, cyberspace employs tools such as encryption, firewalls, and multi-factor authentication to prevent crimes. These measures contain destructive energy (criminal activities) and channel information flows in a secure direction (Amirian & Amin, 2022).

2.4. Energy Police

The concept of "Energy Police" in Iran refers to the government's supervisory and punitive measures for managing energy consumption and addressing violations such as waste, electricity or fuel theft, and unauthorized use of energy carriers (Botnarenko & Kryzhna, 2023). In recent years, particularly in response to crises such as widespread summer blackouts or winter gas shortages, these policies have become a government priority. However, their implementation faces multiple legal challenges rooted in conflicts between governmental authority, citizens' rights, and structural deficiencies in energy laws.

The Energy Police and legal challenges in Iran pertain to the complex regulatory framework governing environmental and energy laws in the Islamic Republic of Iran. The historical emphasis of the Iranian government on state control over energy resources, particularly in the oil and gas sector, has led to an administrative structure fraught with significant challenges in implementing effective energy policies and environmental regulations. The relationship between legal frameworks and energy governance has been further complicated by international sanctions, political factors, and socio-economic dynamics that limit the development of a sustainable energy sector.

3. Requirements and Obligations of the Energy Police

In Iran, the legal approach to enforcing energy laws, commonly referred to as the "Energy Police," encompasses various regulatory bodies responsible for ensuring compliance with environmental laws. The Department of Environmental Protection plays a crucial role in investigating violations, while the judiciary is responsible for imposing penalties for non-compliance. However, the effectiveness of these legal mechanisms is undermined by concerns regarding transparency and accountability, as past criticisms highlight a lack of trust in the judiciary's fair handling of environmental issues. Additionally, legal challenges are exacerbated by the government's deep involvement in the economy, which often hinders the growth of private enterprises in renewable energy initiatives (Aghababai, 2010).

Specifically, legal challenges in Iran extend beyond environmental concerns to human rights and civil liberties, as the judiciary has been scrutinized for using vague charges against activists and critics. These broader legal disputes reflect ongoing tensions between the government and civil society, creating an environment where legal measures sometimes hinder rather than promote sustainable development. The interaction between these legal frameworks and energy policies is critical in Iran's pursuit of a more diversified and efficient energy strategy, particularly in light of the country's ongoing transition towards renewable energy sources. While Iran grapples with these multifaceted challenges, the future of its energy governance will largely depend on resolving these issues. Enhancing public awareness, ensuring compliance with environmental regulations, encouraging community participation, and addressing the influence of political factors will be essential for establishing a more effective energy policy framework. The potential for reform exists, but such reforms will depend on overcoming entrenched interests and strengthening Iran's overall legal institutions.

On one hand, the government, citing laws such as Article 60 of the Energy Consumption Reform Act or resolutions of the Cabinet, takes measures such as cutting electricity to high-consumption subscribers, imposing fines on commercial units, or temporarily restricting gas distribution. However, ambiguities in defining terms like "unauthorized consumption" or "excessive consumption" have led to objections from citizens and even economic sectors. For instance, the disconnection of gas supplies to commercial units in the winter of 2021 triggered widespread complaints from businesses, which argued that the measure violated their economic right to survival (Article 46 of the Constitution) and, without offering a viable alternative, resulted in the bankruptcy of many enterprises.

On the other hand, outdated laws such as the Establishment Act of the Ministry of Energy (1974) or the Air Pollution Prevention Act (1995) do not align with modern energy policies, making the implementation of initiatives such as mandatory installation of smart meters or bans on high-consumption equipment challenging. Contradictions in Iran's overarching energy policies pose a fundamental challenge to energy management. While substantial energy subsidies keep the prices of carriers like electricity and gas artificially low, they also encourage irrational consumption patterns and wastefulness. A report by the Parliamentary Research Center (2022) indicates that low energy prices eliminate economic incentives for consumption optimization and even lead to the proliferation of luxury uses, such as residential swimming pools and inefficient cooling systems. However, the government, fearing widespread public backlash and constrained by legal mandates such as Article 4 of the Targeted Subsidies Act (2009), cannot abruptly reform these policies, as the sudden removal of subsidies could increase energy poverty among low-income groups and trigger civil unrest (Moslehi & Kalantari, 2022).

Furthermore, the outdated and inconsistent nature of energy laws has hindered the implementation of any new policies. For example, the Ministry of Energy Establishment Act (1974), which forms the foundation for managing the electricity and water sectors, does not provide clear mechanisms for penalizing high-consumption users or mandating the adoption of renewable energy sources. These legal inconsistencies have resulted in resistance to initiatives such as the "mandatory installation of solar panels in new buildings" or "penalizing high-consumption industrial units." Even the Energy Consumption Reform Act (2009), which prescribes financial penalties for excessive consumers, lacks precise benchmarks for "optimal consumption," leading to discretionary interpretations by government agencies during implementation. This situation not only creates legal uncertainty but also fosters corruption in energy consumption monitoring.

Innovative projects such as solar-powered control systems for police vehicles and energy-saving kiosks demonstrate the integration of renewable energy into law enforcement operations. These systems utilize solar panels to reduce reliance on traditional energy sources, enhance sustainability, and lower operational costs (Lobanov & Rostunova, 2022). In Europe, one of the mechanisms of the Energy Police includes a module designed for an electricity generation company to implement an intelligent management and control system (Pereira, 2015).

This module consists of five components: the energy consumption monitoring submodule, the security monitoring submodule, the measurement points monitoring submodule, the benchmarking monitoring submodule, and the dedicated monitoring submodule. During the startup and shutdown processes of machinery groups, this module provides operational staff with a controlled parameter range, guiding power plant personnel to precisely follow an optimized curve in machine operation. Additionally, by comparing pre- and post-maintenance performance parameters, it analyzes startup, operation, shutdown, and major maintenance indices, offers operational recommendations, evaluates performance levels, develops security and energy

consumption benchmarks for thermal power generation units, establishes a dynamic energy consumption target system, and implements an alert and closed-loop management process for unusual indicators (Tarnavsky, 2024).

This innovation has significant benefits, as the energy consumption management module can directly monitor abnormal parameters, enhance equipment reliability, efficiently reduce energy consumption in machinery groups, and provide a foundation for formulating consumption reduction strategies.

4. Strategies for Preventing Cybercrimes in the Energy Sector with an Emphasis on Reformative and Preventive Methods

4.1. Reformative Methods

With the advancement of Information and Communication Technology, energy infrastructures have become increasingly reliant on digital systems. While this dependency has improved efficiency and accessibility, it has also introduced threats such as cybercrimes. Power grids, fuel transmission systems, and power plants, due to their fundamental role in the economy and society, have become attractive targets for cyberattacks. Consequently, preventing such crimes through reformative and preventive strategies is an unavoidable necessity.

One of the primary pillars of prevention is the enactment of robust and reformative laws. Establishing precise security standards compels energy companies to continuously update their systems and reduce vulnerabilities. Additionally, mandating advanced encryption for data protection prevents cyber intrusions. Furthermore, strengthening criminal laws and imposing deterrent penalties weaken the incentives for offenders and create a safer environment for operations in this sector.

Emerging technologies also play a crucial role in mitigating cyber threats. Artificial intelligence enables rapid detection of abnormal patterns, allowing immediate responses to attacks. Blockchain technology enhances security and transparency by securing transactions and data. Moreover, conducting regular penetration tests and system updates helps identify and rectify weaknesses (Moradi et al., 2022). Cases such as the 2015 cyberattack on Ukraine's power grid underscore the importance of these measures.

The prevention of cybercrimes is not solely dependent on technical tools and legal frameworks; organizational preparedness is equally vital. Continuous training of personnel increases their awareness of cyber threats and reduces human errors. International cooperation between governments and energy companies facilitates the identification of emerging threats. Additionally, designing crisis management programs minimizes post-attack damages and strengthens institutional resilience.

Cybercrimes in the energy sector present a significant challenge due to the sector's increasing reliance on technology. The integration of robust legislation, advanced technologies, and organizational coordination ensures the security of critical infrastructures. These reformative and preventive strategies not only prevent attacks but also enhance resilience, paving the way for a safer future in energy management in the digital era.

4.2. Representation of Preventive Strategies for Cybercrimes

Utilizing Information and Communication Technology (ICT) tools as part of situational crime prevention strategies is one of the fastest and most effective methods for ensuring relative security and preventing severe damages caused by cybercrimes against energy infrastructures. In such crimes, both cyber offenders and criminal justice institutions employ the same technologies to achieve their objectives; however, the primary distinction lies in the ability to remain up-to-date and maximize the efficiency of these tools. The theory of situational crime prevention, introduced by the British Home Office in the late 1970s in response to the inefficiency of social prevention measures, adopts a proactive approach that focuses on restricting pre-crime opportunities. Rather than examining the offender's personality or the social, economic, and cultural causes of crime, this theory emphasizes altering the environmental and temporal conditions of crime commission and disrupting them to reduce the expected benefits for offenders. As Clarke states, "Situational crime prevention does not seek to reduce criminal motivations by improving society or its institutions; rather, its goal is to diminish opportunities and the attractiveness of crime through situational management" (Ghadir & Kazemi Foroushani, 2019).

In the field of energy infrastructures, implementing situational crime prevention measures using ICT can significantly reduce the occurrence of cybercrimes. For example, deploying intelligent monitoring systems, such as advanced sensors in power grids

or artificial intelligence algorithms to detect abnormal activities in data flows, can make unauthorized access to these facilities more challenging for offenders. These measures, by reducing the profitability of cyberattacks—such as disrupting energy supply or financial extortion—and increasing the risk of identification, decrease the attractiveness of crimes for perpetrators. Strengthening digital security through complex encryption, limiting system entry points via multi-layer authentication, and automatically severing suspicious communications minimize opportunities for misuse.

The practical application of this approach in protecting energy infrastructures can be observed in responses to past attacks. For instance, the 2021 cyberattack on the Colonial Pipeline demonstrated that the absence of situational crime prevention measures, such as timely system updates or active monitoring, can lead to widespread damage. Conversely, the use of technologies like blockchain for securing energy data exchanges and intrusion detection systems can prevent such incidents by intervening in vulnerable situations—such as high-risk periods or technical weaknesses (Savadkouhi Mahfarojaki & Asadi, 2022).

It can thus be argued that the use of ICT within the framework of situational crime prevention offers an effective solution for safeguarding energy infrastructures against cyber threats. This approach, by focusing on managing crime opportunities and reducing its ease and profitability, not only minimizes financial and operational damages but also ensures sustainable security for these critical facilities without necessitating extensive social or judicial transformations.

4.3. The Preventive Approach to Cross-Border Scrutiny of Energy Infrastructure

In the realm of criminal law, one of the fundamental challenges in cross-border scrutiny of cybercrimes is the absence of harmonized and unified international legislation, which makes intergovernmental cooperation complex and, at times, ineffective. The Energy Police, as a national-level institution, faces legal limitations when dealing with crimes originating beyond its borders. For example, if a cyberattack on a country's power grid is launched from a server in another country where such an act is not recognized as a crime, the Energy Police in the affected country is unable to directly prosecute the offenders or request the removal of criminal content from its source. This legal inconsistency, referred to in the text as the lack of consensus on cybercrime classifications, creates significant obstacles in criminal procedures such as evidence collection, extradition of suspects, or enforcement of judgments. The case of *Licra v. Yahoo!* exemplifies this challenge, where differences between French and U.S. laws resulted in a legal impasse in enforcing a criminal ruling.

In such circumstances, the Energy Police requires international legal instruments or bilateral agreements to effectively leverage its criminal jurisdiction (Bahremand et al., 2014). From a preventive perspective, aligning cross-border laws can serve as a key mechanism for reducing cybercrimes in the energy sector. By joining regional or global initiatives, such as drafting common protocols for filtering harmful cyber content, the Energy Police can engage in situational prevention. For example, collaborating with international service providers, such as web hosting companies, to block access to servers that act as cyberattack hubs targeting energy infrastructures can significantly reduce crime opportunities. This strategy is particularly critical in the energy sector, where infrastructures are highly vulnerable due to their reliance on information technology.

Furthermore, global awareness campaigns and the development of shared standards for identifying illegal content can aid in social prevention. This means that users worldwide become aware of the legal and ethical consequences of their cyber activities, thereby reducing their motivation to commit cyber offenses. However, the lack of a universal concept of "acceptable content," as cited from Cook (2007), remains a formidable barrier to cross-border scrutiny.

In the energy sector, this legal inconsistency may manifest as covert cyberattacks or the dissemination of misleading information about infrastructures—content that is deemed illegal in one country but permissible in another. In such situations, the Energy Police alone cannot effectively address the challenge and must collaborate with entities such as INTERPOL or regional organizations to align the global response to harmful content. The example of social media platforms mentioned in the text illustrates the complexity of this issue; users from various countries with conflicting legal systems interact on a single platform, and the discrepancy between the host country’s laws and those of the users’ nations makes filtering criminal content a difficult task. In the energy sector, this problem could lead to the publication of sensitive information or destructive instructions on social media, placing the Energy Police in a difficult position when attempting to prevent threats (Heydarinejad, 2018).

The *Licra v. Yahoo!* case, cited in the text as a compelling example, highlights the inefficacy of traditional criminal approaches in addressing cross-border cybercrimes. In this case, the French court sought to enforce domestic laws to filter illegal content, but Yahoo's resistance, supported by a U.S. court ruling based on freedom of expression, rendered the judgment ineffective.

If this scenario were applied to the energy sector, consider an instance where a country's Energy Police attempts to block access to a website that publishes instructions for attacking energy facilities. If the server hosting this website is located in a jurisdiction that considers such content lawful, criminal and preventive efforts would be unsuccessful. This example underscores the fact that the Energy Police, without the backing of bilateral or multilateral treaties, would be unable to effectively prevent and prosecute cross-border cybercrimes.

Cross-border scrutiny in preventing cybercrimes related to energy requires the integration of criminal and preventive approaches. From a criminal perspective, the Energy Police must enhance its international cooperation efforts and utilize legal mechanisms such as extradition and information exchange to strengthen its ability to prosecute transnational offenders. From a preventive standpoint, this institution can facilitate the alignment of global legal standards and criteria to simplify the process of filtering harmful content on an international scale, thereby preventing cybercrimes before they result in irreversible damages.

The primary challenge lies in overcoming legal and cultural inconsistencies among countries, which—without a global or at least regional agreement—would render the effectiveness of the Energy Police in this domain incomplete.

4.4. Representation of Preventive Strategies in the Iranian Criminal System

To address challenges in the energy sector, particularly cyber threats, several laws and regulations have been enacted in Iran that directly or indirectly pertain to legal and criminal issues in this domain. The Energy Consumption Reform Act (2009) was passed with the aim of reducing energy waste and optimizing energy consumption. This law seeks to lower overall energy consumption and prevent resource depletion through various policies, including improving energy efficiency and promoting the use of renewable energy sources.

The Renewable Energy Development Act (2016) supports the production and use of clean energy, aiming to enhance the generation of renewable energy sources such as solar and wind power to reduce dependence on non-renewable resources. This law, alongside other legislative measures, serves as a foundation for a fundamental transformation in sustainable energy supply while promoting environmental conservation.

The Regulation on the Protection of Critical Infrastructures was also enacted to counter security and cyber threats against energy networks. This regulation prioritizes energy facilities to protect the nation's critical infrastructures from cyber risks and other security threats by establishing mechanisms to ensure the security and stability of energy networks.

Collectively, these laws and regulations create a comprehensive legal framework for supporting renewable energy, optimizing energy consumption, and protecting critical infrastructures, effectively reducing threats and challenges in this sector, particularly cybercrimes.

An effective criminal policy system utilizes all available methods in addressing and combating cybercrimes rather than solely relying on punitive and repressive measures, as was the case in early societies. Evaluating the efficiency of a criminal policy requires examining the range of methods recommended within that system. The necessity of employing a comprehensive approach to crime prevention arises from the diverse and complex factors that contribute to the emergence and spread of cybercrimes, including individual and social factors. However, contemporary discourse increasingly emphasizes adopting preventive measures with a reformative and rehabilitative orientation, as such methods play a fundamental role in combating crime and delinquency.

5. Strengthening Cybersecurity in Infrastructures

Preventing unauthorized access to energy control systems requires the adoption of advanced security technologies. Utilizing security software and protocols such as firewalls, data encryption, and Intrusion Detection Systems (IDS) can significantly enhance the protection of these systems. Additionally, SCADA systems and other monitoring platforms must be regularly updated and reinforced to improve their resilience against emerging threats.

Alongside these technical measures, increasing employee awareness of cyber threats and providing training on best security practices are crucial in mitigating the risks of cyber intrusions. These training programs should cover topics such as phishing attack identification, countering online fraud, and secure information protection practices. Furthermore, implementing restricted access protocols, including multi-factor authentication (MFA) and access limitations based on job requirements, prevents unauthorized entry into sensitive networks and systems (Mirtorabi et al., 2020).

Continuous monitoring and control are also key pillars of cybercrime prevention in the energy sector. 24/7 surveillance of energy networks using intrusion detection and alert systems enables the immediate detection of suspicious activities. Given the increasing prevalence of cyber threats, conducting regular vulnerability assessments of energy networks and simulating cyberattacks can expose system weaknesses and facilitate the implementation of preventive measures. This approach enhances the resilience of systems against potential attacks.

International cooperation and information-sharing are essential in preventing transnational cybercrimes in the energy sector. Since many of these threats extend beyond geographical borders, collaboration with other nations and international organizations such as INTERPOL can aid in identifying and neutralizing shared threats. Additionally, participating in international cybersecurity agreements and protocols and adhering to global guidelines for protecting critical energy infrastructures enhance coordination between countries and promote a more unified approach to addressing these challenges. These measures collectively ensure the cybersecurity of energy infrastructures against cybercrimes.

5.1. Legislation and Establishing Legal Frameworks

Governments must enact comprehensive cybersecurity laws and regulations to safeguard energy infrastructures against cyber threats. These laws should specifically focus on protecting energy data, preventing the destruction of facilities, and securing sensitive information to provide a safe operational environment for this sector. Furthermore, to combat cybercriminals targeting energy infrastructures, it is essential to impose severe penalties, including substantial fines and imprisonment, to create a strong deterrent effect (Babaei & Najibian, 2011).

Preventing cybercrimes in the energy sector, particularly in today's digital and technology-driven world, is a critical priority for nations. Strengthening cybersecurity, implementing continuous monitoring, expanding international cooperation, and drafting effective laws are the four pillars of preventive policies. However, challenges such as a lack of expertise in this field and the rapid evolution of cyber threats present obstacles that must be carefully addressed to prevent severe damage to energy infrastructures (Razavi Asl & Darabi, 2019).

5.2. Challenges and Barriers to Preventing Cybercrimes in the Energy Sector

Many countries face a shortage of cybersecurity specialists in the energy sector, which limits their ability to detect and respond to cyber threats effectively. Additionally, insufficient coordination between governmental agencies, private sector companies, and international institutions weakens responses to cyber threats and leads to operational inefficiencies. The rapid advancement of technologies and the ever-evolving nature of cyber threats further complicate efforts, as many governments and corporations struggle to keep pace with these changes, increasing their vulnerability to new security risks.

5.3. Preventive Collaboration Between NGOs and the Energy Police

From a criminal law perspective, non-governmental organizations (NGOs) face significant challenges due to their lack of legal authority and dependence on government entities, such as the Energy Police and judicial authorities. In societies where the state exerts dominant control, NGO activities often slow down or cease entirely unless there is bilateral engagement with official institutions. For instance, if an NGO gathers evidence of a cyberattack against energy infrastructures but cannot swiftly coordinate with the Energy Police, criminal procedures such as offender prosecution or case initiation may be disrupted. While NGO independence and volunteer-driven operations are valuable aspects of their identity, they act as a barrier within the criminal justice system because these organizations lack punitive or executive authority and remain reliant on formal institutions. This dependency is especially problematic in cybercrimes, where rapid response is crucial, reducing the overall effectiveness of preventive efforts (Zolqi & Malmir, 2018).

From a preventive approach, external challenges can be turned into opportunities for collaboration between NGOs and the Energy Police. NGOs can contribute by providing analytical reports on cyber threats, such as phishing attacks or breaches of energy systems, thereby assisting the Energy Police in deploying advanced monitoring systems and strengthening situational prevention measures (Moghimi, 2016). Additionally, through public awareness campaigns and local community education initiatives on the risks of cybercrimes in the energy sector—such as hacking power grids—NGOs can help reduce crime incentives and opportunities, thus enhancing social prevention strategies.

However, financial constraints and bureaucratic delays, as referenced in the text, hinder the full realization of these objectives. The Energy Police can bridge this gap by establishing support mechanisms, such as providing financial and technical resources to NGOs, thereby strengthening preventive strategies in a more effective manner.

5.4. Preventive Institutional Cooperation and the Energy Police

From a criminal law perspective, obstacles such as lack of coordination among institutions, shortage of specialized personnel, and limited access to data significantly impact the effectiveness of criminal responses. For instance, if the Energy Police does not coordinate adequately with government or private sector organizations, processes such as collecting digital evidence or tracking cybercriminals may be delayed, which is particularly problematic in complex crimes such as DDoS attacks on power plants. The shortage of cybersecurity professionals also weakens the Energy Police's ability to detect and prosecute crimes, potentially leading to failure in presenting sufficient evidence in court. Furthermore, restricted access to data due to fragmented or inefficient information systems makes it difficult to identify the origins of cyberattacks and pursue criminal cases. Resistance to change and ineffective organizational culture further hinder the modernization of criminal justice methods; if the Energy Police remains reliant on traditional investigative approaches, it cannot effectively counter advanced cyber threats such as sophisticated malware.

From a preventive approach, these internal barriers can be addressed through structural reforms. To mitigate coordination deficiencies, the Energy Police can establish a shared platform for information exchange among institutions that provides early warnings about cyber threats and accelerates preventive actions. The shortage of specialized personnel can be resolved through continuous training of staff and collaborations with the private sector or universities to attract cybersecurity experts, thereby enhancing the preventive capacity of this institution (Khanealipour Vajarghah, 2011). Developing integrated information systems can also improve data accessibility and, by employing tools such as artificial intelligence, detect vulnerabilities before criminals exploit them.

Transforming organizational culture by encouraging the adoption of new technologies and promoting rapid reporting of cybercrimes helps institutionalize preventive approaches. Ultimately, formulating comprehensive security policies, such as encryption standards and crisis response protocols, prevents cybercrimes in energy infrastructures and enhances the effectiveness of security measures.

From a criminal justice perspective, internal and external challenges reflect structural limitations in informal responses to cybercrimes in the energy sector. The Energy Police can strengthen its legal authority and coordinate with NGOs and other institutions to transform these challenges into opportunities for effective crime detection and prosecution. However, from a preventive standpoint, emphasizing situational prevention—such as enhancing cybersecurity in infrastructures—and social prevention, such as public awareness and education, can be more effective. Internal barriers such as resource shortages and resistance to change require structural reforms within the Energy Police, whereas external challenges, such as government interactions, depend on macroeconomic policies and financial support.

The success of the Energy Police in combating cybercrimes in the energy sector depends on its ability to integrate both criminal justice and preventive approaches. Unless there is a comprehensive revision of energy laws and a gradual reform of subsidy policies, the contradiction between national energy management objectives and practical implementation will persist.

Another major challenge is violations of citizens' privacy due to energy consumption monitoring. While technologies such as smart meters are necessary for crisis management, the absence of clear laws on household energy consumption data protection raises concerns about potential misuse of this information. This issue is further complicated by the lack of explicit provisions in the Computer Crimes Act (2009) regarding digital privacy, particularly in the energy sector.

Additionally, implementing the Energy Police initiative under extensive energy subsidies, which artificially keeps electricity and gas prices low, presents a policy contradiction. On the one hand, the government encourages citizens to reduce consumption, but on the other hand, low prices eliminate the economic incentive for efficiency. A 2022 report by the Parliamentary Research Center indicates that gradually phasing out subsidies without harming low-income groups requires structural reforms, which have not yet been implemented.

The Energy Police has been focusing on adapting to domestic challenges and global trends in energy production and consumption. The Iranian government has made efforts to integrate renewable energy (RE) into the national energy mix; however, the current share of renewable energy remains minimal. According to the latest reports, only 823 megawatts (MW) of electricity is generated from renewable sources in Iran's power plants.

In recent years, these policies have led to the establishment of 134 new power plants, generating 5,035 million kilowatt-hours (kWh) of electricity and significantly contributing to the reduction of 3.417 million tons of greenhouse gases (CO_2). These actions indicate the government's attention to sustainable development and environmental conservation, although renewables still do not constitute a significant portion of the national energy portfolio.

6. Conclusion

The critical infrastructures of the energy sector, particularly renewable energy sources such as solar, wind, biomass, and hydrogen, are highly vulnerable to cybercrimes due to their dependence on advanced technologies and communication networks. These threats, ranging from hacking control systems to spreading false information, can jeopardize environmental sustainability and energy security.

In Iran, existing laws, such as the Computer Crimes Act, do not specifically address this sector, highlighting a legal gap that, given the growing importance of emerging energy technologies, underscores the need for legislative revisions. The Energy Police can play a key role in mitigating these threats by adopting situational prevention strategies, including enhancing cybersecurity measures through installing advanced systems (such as firewalls and encryption), restricting access to criminal tools, and continuously monitoring data traffic to identify suspicious patterns.

For instance, using artificial intelligence to predict and neutralize cyberattacks before they occur can minimize infrastructure vulnerabilities. Additionally, imposing stricter penalties for the unauthorized use of malicious software or unauthorized access to energy systems increases the cost of crime for offenders and enhances deterrence.

One of the main challenges in this field is determining judicial jurisdiction in cyberspace. Unlike physical spaces, where geographical borders define jurisdiction, cyberattacks are often transnational, making it difficult to identify the origin or destination of the crime. This uncertainty complicates processes such as evidence collection and extradition. Here, the Energy Police can collaborate internationally and leverage the experiences of countries such as Germany or the United States, which have advanced systems for combating cybercrimes, to localize successful models.

The rapid pace of technological advancements poses another significant challenge. Laws drafted today to combat cyber threats may quickly become outdated as new technologies emerge. Therefore, continuous legal flexibility and periodic legislative reviews, along with coordination between the Energy Police, legislators, and technology experts, are essential.

Integrating situational measures (such as strengthening technical security) with social measures (such as employee training and public awareness campaigns) offers a comprehensive approach to cybercrime prevention. Cybercrimes targeting energy infrastructures, particularly in the renewable energy sector, are a growing threat that demands multifaceted preventive strategies.

The Energy Police, by focusing on increasing the risks associated with committing cybercrimes, strengthening security infrastructures, and fostering international cooperation, can play a crucial role in reducing these threats. However, the success of these strategies depends on aligning laws with technological advancements, clarifying judicial jurisdiction, and utilizing global best practices.

A preventive approach not only reduces crime rates but also alleviates the burden on the judicial system and ensures the stability of energy infrastructures.

Ultimately, cybercrime prevention in energy infrastructures requires actions on two levels.

At the strategic level, national planning and policymaking, such as drafting comprehensive cybersecurity laws and strengthening technical infrastructures, can eliminate the root causes of cybercrimes. The Energy Police, at this level, analyzes threats and proposes policies to decision-makers.

At the operational level, immediate actions, such as installing advanced security systems, training personnel, and enforcing stricter penalties, are implemented by the Energy Police to prevent the rapid spread of cybercrimes. This combination ensures the security of energy infrastructures.

Ethical Considerations

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

Acknowledgments

Authors thank all participants who participate in 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

Aghababai, H. (2010). *The Scope of Security in Criminal Law*. Institute of Culture and Islamic Thought.

Amirian, F., & Amin. (2022). Situational Prevention Measures for Cybercrimes in the Context of Its Governing Pathologies. *Quarterly Journal of Legal Studies in Cyberspace*.

Babaei, M.-A., & Najibian, A. (2011). Challenges of Situational Crime Prevention. *Judiciary Legal Journal*, *75*, 147-172.

Bahremand, H., Korepaz, H. M., & Salimi, E. (2014). Strategies for Situational Prevention of Cybercrimes. *Criminal Law Teachings*, *7*, 147-176.

Botnarenko, I., & Kryzhna, V. (2023). Energy market manipulation: Criminal law analysis and signs. *Naukovij Vìsnik Nacìonal'noï Akademìï Vnutrìšnìh Sprav*, *28*(2), 30-40. https://doi.org/10.56215/naia-herald/2.2023.30

Davoodi Dehaqani, E. (2019). Major Barriers to Crime Prevention in Cyberspace. *Journal of Police Order and Security Research*, *12*(2), 53-82.

Ebrahimi, S. (2012). *Criminology of Crime Prevention* (Fourth Edition ed., Vol. 1). Mizan.

Esmaeilzadeh. (2018). The Role of Cyberspace in Committing Crimes with a Preventive Approach. *Islamic Human Sciences Studies*, *21*(4), 64-74.

Ghadir, M., & Kazemi Foroushani, H. (2019). A Comparative Study of Iranian Criminal Law and International Documents on Combating and Preventing Cyberterrorism. *International Legal Journal*, *36*(60), 237-267.

Heydarinejad, N. (2018). Situational Prevention of Cybercrimes from the Perspective of Iranian and International Criminal Law. *Ghanoun Yar*, *2*(6), 29-43. https://www.sid.ir/paper/259670/fa

Khanealipour Vajarghah, S. (2011). *Technical Crime Prevention* (First Edition ed.). Mizan.

Mirtorabi, H. S., Shirzad, H., & Aghakashi, V. (2020). The Role of Police in Preventing Cybercrimes with an Emphasis on National Legislation. *International Police Studies*, *11*(44), 90-113. https://www.sid.ir/paper/404900/fa

Moghimi, M. (2016). *UN Policies and Measures for Cybercrime Prevention* Doctoral Dissertation, Shahid Beheshti University, Tehran].

Moradi, S., Shokarchizadeh, M., Naghshe, A., & Masoud, G. (2022). Cyber Threats and Crimes Against Security and the Challenges Ahead. *Comparative Criminal Jurisprudence*, *2*(1), 37-50. https://www.sid.ir/paper/1036291/fa

Moslehi, A., & Kalantari, I. (2022). The Crisis of Iran's Criminal Policy in the Field of Cybercrimes and Preventive Solutions for Its Aggravation. *Police Criminology Research*, *11*(4), 104-126.

Pereira, R. (2015). *Environmental Criminal Liability and Enforcement in European and International Law*. https://doi.org/10.1163/9789004195882

Razavi Asl, S. M. J., & Darabi, S. (2019). Functions and Preventive Achievements of Electronic Litigation and Cybercrime Procedural Laws. *Legal Researches*, *18*(40), 369-387.

Savadkouhi Mahfarojaki, S., & Asadi. (2022). Iran's Criminal Policy Against Cybercrimes. *Legal Studies*, *65*(7), 395-410.

Tarnavsky, O. A. (2024). Legal Regulation of Compensation of Damage Caused by a Crime in the Energy Sphere. *Ûridičeskij Mir*, 35-40. https://doi.org/10.18572/1811-1475-2024-8-35-40

Zolqi, A., & Malmir, M. (2018). The Role of Law Enforcement Officers in Preventing and Controlling Cybercrimes in Iranian and English Law. *Medical Law Research Journal*, *12*, 93-106.