The Optimal Model of Oversight for Institutions and Executive Bodies Utilizing Cyberspace in Light of Iranian Laws

1. Pezhman Ghafoori: Department of Public Law, Shiraz Branch, Islamic Azad University, Shiraz, Iran
2. Kourosh Ostovar Sangari*: Department of Public Law, Shiraz Branch, Islamic Azad University, Shiraz, Iran
3. Seyyed Reza Alemohammad: Department of Public Law, Shiraz Branch, Islamic Azad University, Shiraz, Iran

***Correspondence: e-mail: Kourosh_ostovar_s@yahoo.com**

Abstract

Oversight of the performance of institutions and executive bodies governing society has long been a crucial issue in preventing corruption, curbing the concentration of power, and improving existing conditions. With the evolution of oversight mechanisms, various types of supervision have emerged, with oversight through cyberspace being a relatively recent approach. This study aims to examine the optimal model of oversight through cyberspace over executive bodies and institutions from the perspective of Iran's domestic laws. The central question is: What responsibilities does the optimal oversight model through cyberspace assign to the general public and the officials of institutions and governmental bodies? This study employs a descriptive-analytical method. The findings of the study indicate that fostering interaction and accountability, establishing a transparent and glass-like government, promoting criticism and open discourse, and enabling public oversight by elites and experts are among the key contributions of cyberspace in shaping an optimal oversight model. The optimal model of oversight for institutions and executive bodies can be realized through Article 24 of the Constitution, the Cyberspace Strategic Document ratified in 2022 as a framework for oversight in forming an ideal Islamic society, and the Computer Crimes Act ratified in 2009 as a legal foundation for criminalizing offenses in cyberspace. Achieving effective oversight through cyberspace by the public necessitates a rational, professional approach that is free from defamation and destructive discourse while considering media literacy. Additionally, managers and officials must prioritize digital responsibility and shift their perspective on cyberspace from a threat-oriented outlook to an opportunity-driven approach.

Keywords: Oversight, Executive Bodies, Cyberspace, Constitution.

Received: 10 June 2024
Revised: 26 June 2024
Accepted: 05 July 2024
Published: 23 August 2024

Citation: Ghafoori, P., Ostovar Sangari, K., & Alemohammad, S. R. (2024). The Optimal Model of Oversight for Institutions and Executive Bodies Utilizing Cyberspace in Light of Iranian Laws. *Legal Studies in Digital Age*, 3(3), 126-133.

1. Introduction

Oversight is a crucial and vital factor in the stability and sustainability of a political system and its acceptance by the people. If oversight is not pursued using efficient, effective, and up-to-date tools, corruption, injustice, discrimination, and

dissatisfaction with political systems may emerge, ultimately jeopardizing the foundations of the social order and the legitimacy of the political system. Historically, oversight through civil institutions, such as political parties, organizations, professional associations, and media outlets, was the most common method before the advent and widespread use of the Internet. However, the emergence of the Internet and the proliferation of various programs, platforms, and software derived from it have introduced a new mode of oversight, which surpasses previous methods in terms of speed, efficiency, scope of supervision, and the ability to receive feedback from those being monitored.

Cyberspace, enabled by the Internet, has created new opportunities not only by altering the nature and form of communications and interactions among individuals but also by establishing mechanisms for improving oversight in governance. With the rapid transformation of digital platforms and programs, cyberspace has played a significant role in amplifying the voice of the people to officials and policymakers, transcending geographical borders and promoting global accountability and collective responsibility. This transformation has also occurred in Iranian society, particularly since the early 2000s, when the Internet was gradually introduced in Iran, paving the way for its use in e-government initiatives and administrative reforms. Over the past decade, with the emergence of various digital platforms reliant on the Internet, the potential for public oversight of political and social affairs, environmental issues, administrative governance, anti-corruption efforts, decentralization, and the promotion of citizens' rights has gained attention.

Although the Constitution, having been drafted before the Internet era, does not explicitly address cyberspace, various articles emphasize oversight, the role of media and press, and other related matters, demonstrating the Constitution's potential to provide a framework for governance oversight, in which cyberspace has become a modern manifestation. Despite the advantages and disadvantages of cyberspace, its widespread and routine integration into global and Iranian society necessitates the establishment of appropriate legal and regulatory frameworks. This means that, given the current conditions, the potential weaknesses of civil and grassroots institutions, and the inadequacy of certain oversight laws, cyberspace can be leveraged as a tool for monitoring institutions, executive bodies, and governance processes. Existing laws concerning cyberspace require thorough examination to identify their limitations, unintended consequences, and adverse effects while utilizing their benefits to establish an oversight framework aligned with the actual needs and expectations of the public.

Recognizing the critical role of oversight in preventing corruption, curbing the concentration of power, protecting citizens' rights, and fostering constructive engagement between the people and the political system, this study aims to propose an optimal oversight model for executive bodies and governing institutions by examining constitutional principles, regulatory frameworks, and specialized laws in the domain of cyberspace. This article adopts a theoretical framework in which cyberspace is conceptualized as a mechanism for oversight, specifically applied to the supervision of Iran's executive institutions.

2. Literature Review

Several studies have examined the role of cyberspace in overseeing political and social domains, including:

Rouhani and Rouhani (2023), in their article "The Role of Cyberspace in National Governance of the Islamic Republic of Iran," concluded that cyberspace, if its threats and vulnerabilities are mitigated, can serve as a medium for fostering national engagement within the framework of shared discourses. In this governance model, cyberspace functions as a key instrument, similar to tools in the physical domain, in linking the people with national identity. However, this study is largely idealistic and does not extensively analyze cyberspace's role within existing laws and governance structures (Rouhani & Rouhani, 2023).

Khalasi et al. (2019), in their study titled "Challenges, Opportunities, and Political Impacts of Cyberspace in the Islamic Republic of Iran," found that cyberspace is an inescapable aspect of modern human life, necessitating specialized skills for effective utilization. Their research recommends that policymakers and cyberspace administrators adopt a strategic perspective on cyberspace rather than viewing it solely as a threat. This study, however, focuses on governance approaches to cyberspace rather than its functional applications (Khalasi et al., 2019).

Khaniki and Khajir (2018), in their research on "The Role of Social Networks in the Development of Civil Society in Iran," explored certain functions of social networks in the realm of civil society. They concluded that the primary use of social networks is for communication and news tracking by citizens, while public opinion assessment and transparency are

among the least utilized functions. This study employed a quantitative field research approach and did not extend its analysis to broader social and political implications (Khaniki & Babaei, 2011).

Salami (2013), in a study titled "Opportunities and Threats of Cyberspace," analyzed the necessity of legal frameworks that identify and criminalize cyber-related offenses to facilitate effective participation in this domain. However, much of this study reiterates general discussions on cyberspace's opportunities and threats, without examining its function as an oversight tool for constructing an ideal society through digital governance (Salami, 2013).

In light of the critical review of existing studies, this research aims to investigate the role of cyberspace in the oversight of executive bodies and institutions, while avoiding redundant discussions on cyberspace applications, implications, risks, and opportunities. Instead, the focus will be on examining existing legal provisions and developing a mechanism for utilizing cyberspace in governance oversight, considering both the role of citizens and the responsibilities of managers and officials.

3. Cyberspace and Its Significance

Cyberspace is an environment built upon information and communication technology, where content production, data filtering, data processing, and information distribution occur. This space functions as a networked domain where individuals with unique and diverse characteristics can interact in various ways (Firouzabadi, 2019). In cyberspace, without the constraints of location and time, social interactions across different cultures are facilitated through modern technologies within a short timeframe (Khaniki & Babaei, 2011). However, like any technological advancement, cyberspace has both advantages and disadvantages. Its primary function is to enhance communication and interactions while reducing communication costs among individuals. Nonetheless, it has also introduced social threats, including shifts in lifestyle and societal norms (Fahimifar & Heydari, 2014). The excessive use of cyberspace may lead to dependency and psychological issues, such as depression, which have become increasingly prevalent with the rising trend of Internet engagement. Furthermore, in the social realm, social networks and cyberspace have facilitated the formation of terrorist groups and cyber threats.

4. Cyberspace and Oversight of Executive Bodies

Various constitutional principles, including Article 24, regulate the operation of press and media, which can be extended to activities in cyberspace. Other constitutional articles emphasize freedom of expression, the right to criticism, and accountability. In particular, the Computer Crimes Act of 2009 outlines the regulatory framework governing cyberspace activities and their limitations. Additionally, the Cyberspace Strategic Document, ratified in 2022, provides a specialized approach to cyberspace governance.

At the institutional and organizational levels, Article 174 of the Constitution of the Islamic Republic of Iran establishes the General Inspection Organization as a judiciary entity responsible for monitoring governmental activities. This institution can utilize cyberspace tools to detect certain offenses and uncover the truth. Judicial support orders may grant inspectors, experts, or their designated representatives the authority to conduct investigations and disclose information (Jalali Farahani, 2010).

Furthermore, within the oversight framework of cyberspace, mechanisms should be developed where specialized committees composed of experts and elites in different sectors conduct precise and technical evaluations. This would prevent the oversight process from becoming superficial and ineffective. Such an approach could involve engaging scholars and experts from both domestic and international contexts to utilize their insights in predicting future trends and analyzing developments (Sadati, 2014, p. 108). Addressing economic issues, domestic and foreign policies, managerial performance, and governmental accountability through expert-driven cyberspace oversight can contribute to an intelligent and strategic monitoring framework for executive institutions in Iran.

5. Establishing Digital Responsibility

Accountability through cyberspace, facilitated by available digital tools, can create a system of continuous and ongoing responsiveness, made possible by instant access to the latest information. This means that cyberspace enables rapid access to

both general and specialized information in the most efficient manner (Abbasi Dareh Bidi et al., 2016). This characteristic allows for the daily operationalization of oversight mechanisms for executive bodies, ensuring that regulatory institutions, in collaboration with the public, can effectively implement such measures.

Achieving this objective requires that citizens, as users who engage with cyberspace to improve societal conditions, engage in fair and constructive criticism while avoiding bias and focusing on the principle of gradual improvement. This capability appears to be attainable through cyberspace, as the Internet has a profound influence on individual and societal thought processes. Through continuous interaction in cyberspace, barriers such as coercion, hostility, lack of confidence, and low levels of understanding can be mitigated (Mashayekh & Hajizadeh, 2023). Conversely, this interaction also allows individuals to cultivate their expertise and ideas, fostering creativity and enhancing personal capabilities (Nye, 2011). The outcome of this engagement is the development of a healthy critical environment, devoid of personal biases, which refines human thought through broad and inclusive interactions. This, in turn, promotes a fair and rational approach, replacing prejudice, negligence, and hostility with informed discourse. In this manner, a significant component of the optimal oversight model for executive bodies emerges, shaped by rational and unbiased criticism.

A crucial requirement for overseeing executive bodies is the reinforcement and support of "digital responsibility" by institutions and governmental organizations. This entails that management strategies in the contemporary era, which is significantly shaped by the presence of media and cyberspace, must be adapted to enhance institutional performance. The emphasis on digital responsibility arises because the widespread influence of digital technology in modern life has introduced a novel dimension to social responsibility, recognizing individuals' online activities as an extension of their broader obligations (Guping et al., 2021).

Digital responsibility implies that the administrators of executive bodies and governing institutions must acknowledge their duty to remain accountable to the public in a new digital environment shaped by the expansive reach of cyberspace. Thus, digital social responsibility can be established as a modern strategy that leverages the advantages of emerging digital conditions (Puriwat & Tripopsakul, 2021). However, the realization of digital social responsibility requires the interpretation of constitutional principles to ensure the acceptance of oversight, the necessity of public supervision over executive bodies, and the establishment of appropriate legal and infrastructural conditions for harnessing the benefits of this widespread digital space.

Auditing and oversight through institutions such as the Court of Audit, the General Inspection Organization, the Article 90 Commission, and even extraordinary inspections by the Judiciary and regulatory agencies can be effectively conducted using digital tools and citizen engagement. However, the application of cyberspace-based oversight over executive bodies necessitates a tailored and localized model. Current policymaking by state agencies remains passive and lacks comprehensive, systematic, and inclusive planning. Furthermore, the existing regulatory frameworks, content production standards, and national digital content models are fragmented, lack a strategic roadmap, and often rely on Western frameworks while neglecting the challenges and opportunities posed by unhealthy digital content. There is also a failure to capitalize on positive aspects and a lack of a distinguished, strategic, and indigenous oversight model (Firoozi et al., 2022).

Thus, it is essential to integrate digital social responsibility with existing legal and regulatory frameworks to adopt an opportunity-driven perspective. This approach would address the challenges associated with digital access while fostering a system in which citizens, experts, and intellectuals can participate in supervising executive bodies. Such an initiative would pave the way for a sustainable, expert-driven, and localized model for improving governance.

6. Establishing a Transparent Government through Cyberspace

Effective oversight requires mechanisms that facilitate a transparent and citizen-centered governance structure. Given that Iranian society has widely embraced smartphones, cyberspace, and various domestic and international digital platforms, utilizing cyberspace for the development of an optimal oversight model is imperative. The widespread adoption of cyberspace highlights its role as a fundamental aspect of both individual and social life (Salami, 2013).

Moreover, maintaining constant oversight over employees, their performance, and their activities through in-person monitoring within complex bureaucratic processes is challenging and demands significant time and financial resources.

Therefore, establishing a modern electronic inspection and monitoring system utilizing information technology infrastructure is both necessary and vital. Such a system enhances oversight efficiency, offering extensive and precise monitoring with minimal time and cost investment (Poornagdi, 2015).

This model could also lay the groundwork for the formation of a "transparent government", in which the activities and performance of managers and employees in executive institutions are fully visible to the public. This would enable citizens to engage interactively in evaluating governmental operations and expressing their perspectives.

The realization of a transparent government requires a specific type of critical oversight—one that is facilitated through cyberspace and built upon constructive and solution-oriented accountability, rather than unprecedented criticism, the dismissal of achievements, or undue pessimism. To achieve this, enhancing and expanding media literacy is crucial. Media literacy ensures that individuals can use digital platforms effectively and intelligently (Najafi & Vahedi, 2017).

According to Article 24 of the Constitution of the Islamic Republic of Iran, the scope of press, publications, and media activities is clearly defined, ensuring that these activities do not disrupt public order or undermine Islamic values and norms. Additionally, the Cyberspace Strategic Document (2022) states:

"The cyberspace of the Islamic Republic of Iran, by 2031, will be an extension of the real-world space—healthy, useful, secure, and a driving force for progress in other sectors. It will be based on the country's endogenous capacities, supported by specialized, skilled, and effective human resources, benefiting from academic and research institutions, knowledge-based enterprises, and advanced domestic industries, while maintaining an innovative and proactive stance."

Achieving a healthy, beneficial, and secure cyberspace requires empowering the public and grassroots institutions and ensuring legal mechanisms that facilitate public participation and oversight while preventing excessive dominance by governmental agencies. It appears feasible to transfer power to the people through cyberspace, as digital platforms and their derivatives, such as social networks, have significantly transformed various dimensions of human life, including political, economic, security, cultural, social, and legal systems (Rouhani & Rouhani, 2023). This transformation aligns with Joseph Nye's conceptualization of soft power, which he identified as the key form of power in the 20th century (Nye, 2011).

If cyberspace and the Internet are sources of power, transferring this power to the people can play a vital role in oversight mechanisms across various governance sectors, including executive institutions. The contemporary public no longer accepts a governance model in which laws are enacted, implemented, and adjudicated solely by governmental bodies without broader accountability.

Cyberspace not only empowers citizens but also grants them diverse tools for oversight. Consequently, cyberspace bridges the gap between the public and the government, eliminating many traditional barriers to oversight. Various domestic legal frameworks, including Article 24 of the Constitution, the Computer Crimes Act (2009), and the Cyberspace Strategic Document (2022), emphasize the significance of oversight and responsible use of cyberspace.

The legal support for cyberspace-based oversight suggests that digital communications can enhance public scrutiny over governance through political organizations, pressure groups, parties, and associations. This, in turn, strengthens political culture and improves governance quality (Khalasi et al., 2019). Consequently, leveraging cyberspace for political and cultural development can help advance political affairs and facilitate the formation of a transparent and efficient government, ensuring the long-term sustainability and effectiveness of the Islamic Republic of Iran's governance system.

7. Effective and Interactive Accountability

Cyberspace, by fostering widespread awareness, contributes to the establishment of mechanisms that enhance accountability and transparency (Azadi et al., 2020). Accordingly, the utilization of cyberspace by citizens should be structured in a way that influences public opinion both domestically and internationally (Bashir & Rezaei, 2015, p. 46). However, this influence should not be limited to raising awareness alone; rather, it is essential to establish a supervisory infrastructure backed by public opinion and create executive domains to ensure the effectiveness of public oversight.

Electronic oversight through cyberspace accelerates decision-making processes and provides organizations with the necessary information from various sources. Additionally, within this oversight framework, certain events can be predicted, including potential violations or breaches of the law (Hosseini & Noorozian, 2010). Consequently, media outlets, by

increasing awareness and exposing different dimensions of decision-making by elites and policymakers, elevate public knowledge regarding political intricacies. The power generated through cyberspace places pressure on elites, leading to heightened demands, greater transparency, and enhanced accountability (Azadi et al., 2020).

To achieve this goal, domestic legal frameworks are also significant. For instance, the Cyberspace Strategic Document includes provisions such as the "Plan to Enhance the Capacity for Public Participation and Civil Society Organizations in Cyberspace". This legal foundation facilitates the establishment of accountability by enabling oversight of the performance of government officials. Social networks, as tangible manifestations of cyberspace, possess the capability to provide users with equal opportunities to engage in content creation and opinion-sharing. Unlike traditional mass media with hierarchical structures, social media platforms do not enforce rigid gatekeeping mechanisms; instead, they serve as facilitators, enablers, and hosts for public discourse (Gillespie, 2012, p. 353).

This direct interaction presents a valuable opportunity for overseeing executive bodies, ensuring that citizens' perspectives are neither censored nor disregarded by higher authorities. A major outcome of cyberspace in the realm of effective accountability is its role in decentralizing power, leading to a "polyarchy" within political and social structures, where power is distributed among diverse societal groups rather than being concentrated in a few elite institutions. This shift has significantly transformed classical power mechanisms (Firouzabadi, 2019).

Social networks, emerging from cyberspace, have decentralized power across various domains and disseminated it throughout society at the grassroots level. Given the legal frameworks and mechanisms embedded in constitutional law and the Cyberspace Strategic Document, cyberspace can be leveraged as a mechanism for shaping an ideal society. If the Executive Branch (through its regulatory bodies in various ministries), the Judiciary (via the General Inspection Organization), and the Legislature (through the Article 90 Commission) intend to utilize cyberspace for oversight, the Cyberspace Strategic Document (2022) outlines specific measures that serve as a roadmap for implementing public oversight through digital means.

In this regard, the Executive Branch can focus on designing a digital economic system and a legal framework for cyberspace, while the Judiciary can develop a judicial system for cyberspace. Consequently, transitioning from a centralized governance model to a decentralized and participatory governance framework through cyberspace becomes both feasible and essential. Governance, in this context, implies responding to public demands and utilizing the capabilities of non-governmental institutions and organizations alongside governmental institutions to facilitate the realization of governance objectives (Rouhani & Rouhani, 2023).

Achieving an oversight model that integrates non-governmental organizations with governmental institutions requires removing barriers that hinder civil society participation while reducing the government's overwhelming influence across various sectors. This is because the state alone cannot comprehensively manage executive, legislative, oversight, and judicial affairs, nor can it consider public participation a threat to its authority. With the rise of cyberspace as a supervisory tool, new power dynamics and relationships are emerging that foster greater societal cohesion. If these evolving relationships gain legitimacy, they will serve as a model for social action and mutual understanding (Abdollahi et al., 2020).

In this context, a culture of criticism and discourse fosters the identification of optimal strategies for supervising executive bodies, leading to the development of a "methodical collective understanding" that aligns with societal expectations and actions (Praetorius, 2000). Therefore, the establishment of a shared societal understanding for mapping out an oversight framework necessitates an opportunity-driven approach to cyberspace governance. Restrictions that weaken public oversight and hinder participatory development should be avoided. However, achieving this goal requires legal incentives and governmental support.

Accordingly, the establishment of a "Ministry of Cyberspace" at the macro-policy level is essential to mitigate the current disarray in cyberspace governance and fully utilize its potential for oversight. Implementing such an approach would signify a shift towards media and cyberspace governance as an official government function (Azadi et al., 2020). The creation of a Cyberspace Ministry would further support the formation of specialized supervisory communities across various sectors, maximizing the benefits of structured, legally compliant oversight mechanisms.

The ultimate goal of oversight over executive bodies is to establish a sustainable, widespread, and discourse-driven system in which public engagement in monitoring governance structures becomes a permanent fixture of society.

8. Conclusion

Oversight, as a mechanism for monitoring the actions of managers, officials, institutions, and executive bodies, is a recognized principle under Article 24 of the Constitution. In alignment with this principle and related provisions concerning accountability and freedom of expression, a series of legal frameworks, including the Islamic Republic of Iran Cyberspace Strategic Document (2022) and the Computer Crimes Act (2009), have been enacted.

While these laws impose certain restrictions and criteria for cyberspace use within the media domain and include measures for prosecuting cybercriminals, they also present opportunities for the general public. If utilized properly and rationally, these legal provisions can enhance oversight over executive bodies and institutions in a structured and efficient manner.

The oversight model facilitated by cyberspace involves leveraging legal and regulatory mechanisms to achieve objectives such as the formation of a transparent government. Within this framework, cyberspace serves as a platform for improving the performance of managers and officials while simultaneously empowering citizens. In this sense, cyberspace should not be viewed as a threat but rather as an opportunity to distribute power among the people.

This perspective positions the public as active agents of oversight, granting them access to monitoring mechanisms within governance structures. However, for public oversight through cyberspace to be effective, a balanced and rational approach is necessary from both the government and the citizens. The integration of expert opinions and specialized insights is crucial in ensuring the effectiveness of cyberspace-based oversight.

Moreover, the acceptance of digital responsibility by managers and government officials plays a fundamental role in shaping an optimal oversight model. Digital responsibility signals a governmental commitment to embracing public scrutiny and constructive criticism in a manner that enhances governance efficiency in the digital era.

Based on the findings of this study, the following recommendations can be proposed:

- Facilitating specialized digital oversight tools by establishing transparent infrastructure in cyberspace.
- Developing information security strategies to distinguish legitimate oversight from disruptive activities.
- Promoting trust-building measures in cyberspace to ensure low-cost and accessible oversight for citizens.
- Adopting an opportunity-driven approach to cyberspace governance, rather than perceiving it solely as a threat.
- Establishing a Ministry of Cyberspace at the governmental level to ensure top-down strategic oversight.
- Prioritizing an expert-driven and elite-centric approach to digital oversight.

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

Abbasi Dareh Bidi, A., Yousefi, S., & Mahmoudi, F. (2016). Cyber technology and progress. In Proceedings of the Tenth Congress of Progress Pioneers,

Abdollahi, H., Mohseni Moshtagh, A., & Elahi Manesh, H. (2020). The impact of cyberspace on the development approach in Iran based on international interdependence. *Quarterly Journal of Political Sociology in Iran*, *4*(4), 833-857.

Azadi, A., Torabi, M., & Heydarpoor, M. (2020). The Islamic Republic of Iran and cyberspace: Solutions to challenges. *Quarterly Journal of Sacred Defense Studies*, *6*(3), 149-180.

Fahimifar, S., & Heydari, E. (2014). Examining the economic dimensions of electronic book publishing from the perspective of Iranian publishers. *Quarterly Journal of National Studies in Librarianship and Information Organization*.

Firoozi, M. H., Ghorbani, M., Taghipour, R., & Alidadi, R. (2022). A strategic model for producing high-quality content based on national security approaches in cyberspace. *Quarterly Journal of National Security*, *12*(44), 105-134.

Firouzabadi, S. A. (2019). *Cyberspace and its developments*. Mashhad: Astan Quds Razavi Publishing.

Guping, C., Cherian, J., Sial, M. S., Mentel, G., Wan, P., Álvarez-Otero, S., & Saleem, U. (2021). The relationship between csr communication on social media, purchase intention, and e-wom in the banking sector of an emerging economy. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(4), 1025-1041. https://doi.org/10.3390/jtaer16040058

Hosseini, M. H., & Noorozian, A. (2010). Implementing electronic monitoring in the country's supervisory organizations and its effect on reducing corruption. *Journal of Supervision and Inspection*, *4*(14), 1-19.

Jalali Farahani, A. H. (2010). *The Cybercrime Convention and its additional protocol*. Tehran: Khorsandi Publishing.

Khalasi, P., Babaei, M. B., & Mazaheri, M. H. (2019). Challenges, opportunities, and political effects of cyberspace in the Islamic Republic of Iran. *Quarterly Journal of Political Research in the Islamic World*, *9*(4), 165-188.

Khaniki, H., & Babaei, M. (2011). Cyber and social networks: Concepts and functions. *Quarterly Journal of the Iranian Society for Information Studies*, *1*(1), 1-24.

Mashayekh, F., & Hajizadeh, H. (2023). Opportunities and harms of cyberspace. *Quarterly Journal of New Ideas in Educational Research*, *2*(2), 91-113.

Najafi, F., & Vahedi, M. (2017). Opportunities in cyberspace: A religious-educational approach. *Journal of Pure Life*, *6*(20), 31-49.

Nye, J. S. (2011). *The future of power*. New York: Public Affairs.

Poornagdi, B. (2015). Challenges and solutions for establishing electronic monitoring in the General Inspection Organization. *Journal of Evaluation Knowledge*, *7*(23), 5-23.

Praetorius, N. (2000). *PRINCIPLES OF COGNITION LANGUAGE AND ACTION (Essays on the Foundation of a science of Psychology)*. University of Copenhagen, Denmark: Kluwer Academic Publishers. https://doi.org/10.1007/978-94-011-4036-2

Puriwat, W., & Tripopsakul, S. (2021). The impact of digital social responsibility on preference and purchase intentions: The implication for open innovation. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(1), 24. https://doi.org/10.3390/joitmc7010024

Rouhani, A. F., & Rouhani, M. (2023). The role of cyberspace in national governance of the Islamic Republic of Iran. *Quarterly Journal of Interdisciplinary Strategic Studies*, *13*(53), 61-84.

Salami, M. H. (2013). *Opportunities and threats of cyberspace*. Tehran: Tazieh Distribution Publishing.