Opportunities of Virtual Social Networks for Critical Infrastructure of National Security

(From the Point of View of Political and Virtual Media Experts)

Marjan Karami[1], Garineh Keshishyan Siraki[2]*, Mohammad Tohidfam[3]

[1, 2]*Department of Political Science, South Tehran Branch, Islamic Azad University, Tehran, Iran
[3]Department of Political Science, Central Tehran Branch, Islamic Azad University, Tehran, Iran

Abstract:
Virtual space and the associated social networks, like many other emerging phenomena, have both positive and negative consequences in various aspects of life. The undeniable impact of this space is particularly significant in the national security of countries, as it can create numerous opportunities for national security along with the changes and developments it brings about. This research aims to identify the opportunities that social networks create for the infrastructure of national security. Data were collected through grounded theory and in-depth interviews with 16 experts in the fields of politics and virtual space. The data were analyzed using open, axial, and selective coding methods, employing the Strauss and Corbin approach. The research results indicate that virtual social networks can provide unique opportunities for national security by strengthening the infrastructures of social, political, cultural, economic, and environmental security. The research results are presented in the form of a paradigm model of opportunities.

*Corresponding Author's Email: G_Keshishyan@azad.ac.ir

Introduction

Based on Maslow's hierarchy of needs theory (Maslow, 1981), security is a fundamental human need, and the level at which members of a society experience it reflects in the trust and security of that society. As governmental institutions worldwide seek sustainable solutions for national security and disaster management, they face challenges in dealing with the puzzle of managing social media influence.

Social media, its access, influence, and potential in the globalized world are no longer debatable. Instead, considering its use and misuse, it has impacted people's lives (Wanja, 2021). The extraordinary increase in internet usage with related multi-layered social media platforms is globally recognized as one of the most significant opportunities for security at local, regional, national, and global levels. The role of social media as a mechanism for stabilizing intellectual beliefs, ideological stability, and strengthening ethical and social virtues to create balance in society, enhance national security, and create opportunities is widely acknowledged in contemporary literature (Innes et al., 2019).

The presented research in this article aims to understand the impact of social media on elements contributing to national security experienced in Iran. Al-Huwaish (2017) suggests that security encompasses various elements, and their priorities differ for each individual. These security elements include social, political, economic, criminal, food, water, cultural, environmental, and informational (newer aspects of security) security, all interconnected. The mutual dependence of these security elements, when one is disrupted, leads to disturbances in the overall security of the society.

The internet has brought significant changes to communication, expanding its scope and creating new opportunities. It has allowed the voices of the silent to be heard and broken the boundaries set by traditional media. Before the internet, those unable to afford the costs of expressing their opinions in traditional media would remain silent. Expressing opinions, beliefs, and awareness of societal issues and others' thoughts used to belong to the wealthy and specific groups (Asogwa, 2020). However, with the emergence of internet-based social networks, everything has changed. People can now express their ideals, beliefs, and thoughts through social media platforms like Facebook, Twitter, Telegram, WhatsApp, and others with little or no cost. Asogwa (2017) notes that internet-based media are a significant part of media preferences and consumer behavior in the 21st century. The Internet has also expanded the advertising scope, allowing small and medium-sized companies that cannot afford the financial burden of traditional media advertisements to do so with a single click (Asogwa, 2017).

These networks are recognized as one of the most important factors in fostering free interaction among users. They encourage users with weak connections to expand their communications and experience new cultures, news, information, knowledge, and more. The openness of communication spaces on social media networks has led to increased interactions, enhanced identity, and increased participation, and potentially created a global pandemic in the realm of privacy and national security.

These networks, with their diverse technological capabilities, support a wide range of interests, thoughts, and affiliations. Some networks

help users connect based on common interests, shared culture, political views, or activities. Some respond to various audiences, while others attract individuals based on common language or shared racial, political, sexual, religious, or national identities. Moreover, during the protests of 2022 in the Islamic Republic of Iran, internet restrictions on social media were imposed to protect national security.

Based on this, Martin Libicki in his book titled "Victory in Cyberspace: National Security and Information Warfare" argues that information technology and communication have created a new space alongside the real and tangible world, known as cyberspace or virtual space. The most important feature of this new space is the uncontrollability of interactions and the changing nature of many concepts such as power and threat (Libicki, 2014).

In such conditions, the best option for dealing with cyberspace and social networks is a precise understanding of these phenomena in all dimensions, especially their opportunities and threats to national security, to approach them knowingly and increase national power and security.

Cyberspace, especially social media, and the information flows present in it, are among the most important and influential power streams. Mismanagement of this space can lead to the destruction and collapse of a political system. Therefore, advanced countries try, in various ways, to manage and govern cyberspace and not allow hostile countries to take control of its management. Thus, cyberspace and social networks can provide opportunities for exercising and expanding power, but if neglected, they can become a serious threat to power. As previously mentioned, cyberspace and social networks, especially social media, have opportunities that, with awareness and proper planning, can be utilized. Opportunities for education, messaging, cultural development, national unity, economic exploitation, and political uses.

This study focuses on addressing this key question: What opportunities do social media offer for national security from the perspective of experts and specialists? The findings of this study help understand the views of political and media experts on the opportunities of social media in key areas, including political, cultural, economic, security, social, ethical, and religious aspects, in contributing to the security level of Iran. Additionally, the study considers considerations related to social media on national security to reduce the negative characteristics of social media.

Theoretical

In an article titled "Internet-Based Communications: Threat or Strength for National Security," Asogwa (2020) concludes that internet-based communication media such as Facebook, Gmail, YouTube, Yahoo email, and Twitter are significantly related to national security. The study identifies specific ways in which negative internet usage can adversely affect national security. It emphasizes that internet-based media can be useful in raising awareness about national security threats, issuing warnings about national security issues, and alerting people to national security concerns. Based on the study results, the researcher recommends traditional media like radio, television, newspapers, and magazines to collaborate with security agencies in Nigeria to create awareness for national security vigilance. Although the article does not focus on national security in Iran, we are exploring opportunities in cyberspace for national security in Iran.

Joseph Nye (2011), a prominent professor at Harvard University, discusses cyber power in today's world in an article published on the Harvard Kennedy School's Center for Science and International Affairs website. He states that cyberspace is a new and important domain of power, and even countries like the United States, with vast hard and soft power interests, face challenges in controlling their borders in the cyber domain. While the article does not classify national security, it highlights cyberspace, and we are seeking opportunities in cyberspace for national security in Iran.

In his book "The Information Revolution, Security, and New Technologies," Rezvanav (1924) expresses the goal of familiarizing with information technology and its impact on empowering elites and people. The book gathers examples, such as "Information Revolution, Security, and International Relations," "Information, Artificial Intelligence, and Development of Analytical Skills," and "Evaluation of Information Technology and Security Theories for the Middle East." The study extensively examines information technology and communication, focusing on its potential impact on national security, a topic that this research specifically addresses.

Naderi, Bakhshayeshi, Darabi, and Moghaddasi (2018) conclude in their study that social media networks, like a double-edged sword, can create both positive and negative actions in the political-security environment of the Islamic Republic of Iran. Due to the unregulated nature and island-style policymaking in the cyberspace of the Islamic Republic of Iran, social networks have highlighted the country's vulnerability in certain aspects of national security. These networks actively engage in activities such as subversion, delegitimizing the political system, weakening national cohesion, and creating a rift between society and government.

They also operate in the security domain through espionage, monitoring user information, disseminating destructive teachings on social networks, and transferring classified information to disrupt national security. Establishing a powerful and comprehensive structure for policymaking organizing the country's cyberspace and launching a national information network can effectively address many problems in this area. This study, using the grounded theory approach, focuses on national security opportunities in social media networks.

As observed in the research background, most studies in the cyberspace and national security domain either focus on one variable or broadly examine each area. In this research, efforts are made to categorize and study national security opportunities at the infrastructure level. Despite the negative roles and functions of social media networks, they also have positive functions. According to theoretical perspectives, social media networks can have positive implications for their audiences, such as increased communication, control of information flow, reduction of national, cultural, and gender gaps, participation enhancement, ideological strengthening, and the creation of new political demands.

While previous theoretical discussions may have provided a foundation for the study, the reality is that the concepts and foundations discussed are specific to other societies and may not fully align with Iranian society. The theoretical concepts presented express broad and pervasive global realities, but they may

not cover the existing differences in various societies.

The technological determinism theory proposed by Thorstein Veblen (1857-1929), an American sociologist, suggests that technology has significant effects on our lives. McLuhan developed this idea in 1960 (McQuail, 2005). Technological determinism, in simple terms, is the idea that technology has important influences on our society. McLuhan argues that changes in technology affect society as a whole, which is prominent in political and imaginative terms. For example, the idea that the Internet is transforming the economy and society is highlighted in political and imaginative terms (Asogwa, 2020).

Before the emergence of new technologies, addressing security issues was easier. At least, the issue of cybersecurity was not a problem that security experts faced. However, with current conditions, it is plausible that a country's security architecture is at risk, but opportunities can be created for national security amidst these risks.

Therefore, in this study, we use these concepts to increase theoretical sensitivity. Our goals include discovering related concepts and relationships between them to reach a theory that explains the dominant pattern of relationships between variables in Iranian society. In the end, the pattern and framework obtained may have connections with previous theories and studies. Still, our goal, which is studying the phenomenon in question within the framework of foundational theory, does not create doubt and difficulty, as the phenomenon emerged during the study, not testing previous theories.

Research methodology

This practical study, conducted with a qualitative approach and the theoretical framework of "Grounded Theory," utilizes Grounded Theory as a form of qualitative research that involves a systematic, inductive, and adaptive approach to construct theory (Charmaz, 2006). Primarily designed to encourage continuous interaction between the researcher and the data through ongoing engagement in emergent analyzes throughout the study, this method facilitates the simultaneous collection and analysis of data, easing the workflow

Grounded Theory generates empirical research during the analysis process, as the researcher is obliged to test all theoretical explanations against empirical findings. The forward and backward movement between research data leads to a gradual focus on the collected data, making the theoretical analysis more successful (Alqahtani, 2014). The process of conducting Grounded Theory is illustrated in Figure 1. In this study, information was initially gathered through library research, including books, journals, online sources, theses, articles, and databases, determining the indicators and components of national security and cyberspace.

In Grounded Theory, theoretical sampling is employed, where participants are selected based on criteria defined by the researcher and preliminary results. The targeted interviewees in this study, meeting the needs of 16 experts and professionals in the fields of politics and media with doctoral qualifications and activities in the cyberspace and national security domain, provided data through in-depth interviews. Given the study's timing during the COVID-19 pandemic, all interviews were conducted via telephone and WhatsApp, followed by the analysis phase.
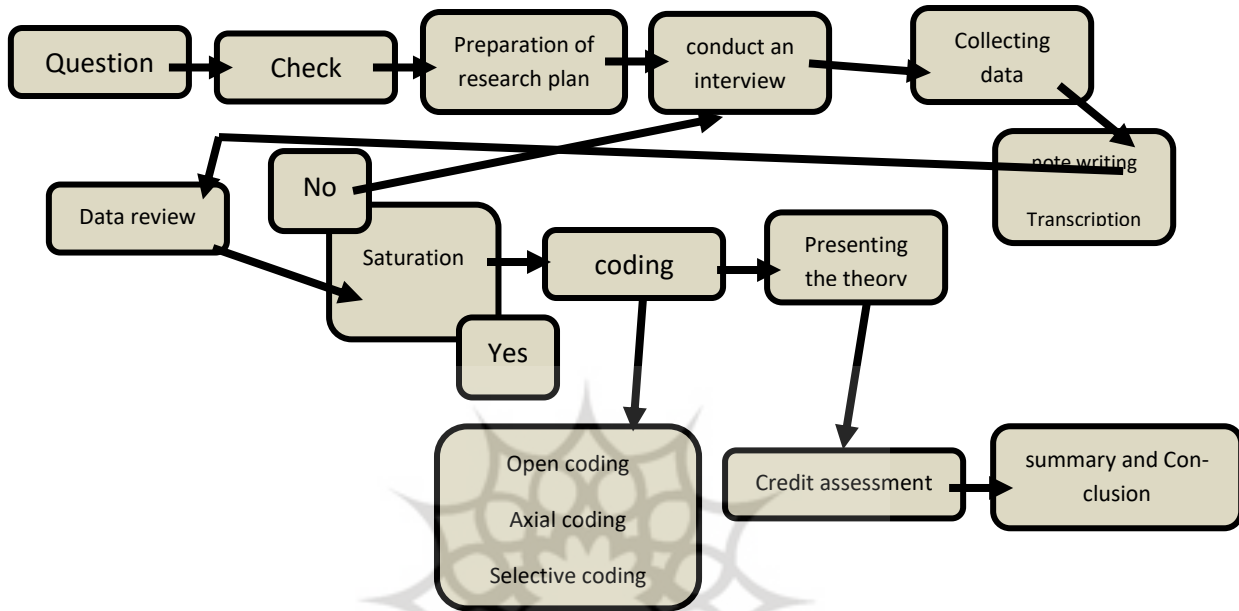
Table 1: Distribution of people in groups participating in the interview and the codes used

Row	Interviewee code	gender	Age	education	Expertise
1	1 p	Male	24	PH.D	Researcher
2	2 p	Male	40	PH.D	Professor
3	3 p	Male	34	PH.D	University lecturer and researcher
4	4 p	Male	34	PH.D	Researcher
5	5 p	Male	55	PH.D	Researcher
6	6p	Male	-	PH.D	Security
7	7p	Male	65	PH.D	Former cultural and media employee
8	8p	Female	42	PH.D	Researcher
9	9p	Female	42	PH.D	Active in the field of women, family and media
10	10p	Female	32	MA	Researcher
11	11p	Male	54	PH.D	Research faculty
12	12p	Male	35	PH.D	Commercial employee
13	13p	Male	47	PH.D	Azad University faculty member
14	14p	Male	36	PH.D	R&D expert at Hamrah-e Aval
15	15 p	Male	48	PH.D	An employee of the IRI Broadcasting Organization
16	16p	Male	-	PH.D	-

In the first step of the grounded theory analysis, the interviews are coded. In this study, a three-phase coding system proposed by Strauss and Corbin, namely open coding, axial coding and selective coding, was used. Atlas.ti software was used for data coding and analysis.

Figure 1- Grounded theory implementation process

```
Question → Check → Preparation of research plan → conduct an interview → Collecting data

No → Data review
Saturation → coding → Presenting the theory
Yes
note writing / Transcription

Open coding
Axial coding
Selective coding

Credit assessment → summary and Conclusion
```

In the present study, various aspects were considered to achieve research validity. First, two university professors in the field of national security were consulted about interview questions and how to follow up on the answers. Then, for the validity of the research at a higher level during the analysis process, the participants were consulted to ensure that the obtained model was consistent with their point of view.

For credibility, interviews and conversations close to the desired issue were examined during the implementation of the research to reach a more comprehensive and complete analysis and results. For verifiability, the final analysis was given to two university professors to express their opinions, and their desired corrections were applied.

Analysis of Findings

After completing all encoding stages for all questions, the research findings are presented in the form of concepts, major themes, and the identification of core issues for each question separately. In open coding, naming, description, and classification of data were performed. In axial coding, concepts and themes identified in the previous stage were linked and associated with a new categorization. In selective coding, an attempt was made to extract an analytical model from the data and codes.

In this research, after analyzing interviews using content analysis, line-by-line and phrase-by-phrase examination, concept elaboration, categorization, and then, based on coherence,

conceptual relations, and common features among open codes, concepts, and themes were specified. In the data analysis process, 369 open codes were extracted. In axial coding, the process of linking themes to their sub-themes and connecting themes at the level of features and dimensions took place (Lee, 2001). In this coding, a theme is selected from open coding and placed in the center of the process under investigation. Other themes are then linked to it. Other themes include:

Casual Condition: Themes related to conditions that influence the core theme and are considered the main cause of the phenomenon's existence. The causal conditions in the final model pattern were 24 cases, including:

1- Social security opportunity, 2- Media literacy, 3- Social relationships, 4- Social justice, 5- Decentralized information, 6- Economic security opportunity, 7- Economic development, 8- Satisfaction with the current situation, 9- Increased sales, 10- Economic progress, 11- Cultural security opportunity, 11- Social cohesion, 12- Media literacy, 13- Soft power, 14- Development, strengthening social identity 15- Cultural convergence, 16- Political security opportunity, 17- Increased accuracy and speed, 18- Social justice, 19- Increased legitimacy and power 20- Information exploitation and 21- Environmental security opportunity, 22- Economic development, 23- Innovation facilitation, adaptation, and progress, 24- Increase in biological participation, all contribute to each other and create a foundation for strengthening national security, leading to national security empowerment.

In this regard, it must be said that studies have shown that media, especially social media networks, have significant effects on cultural and ethical beliefs, politics, and the economy. These media can enable society to continue its social, economic, political, cultural, and environmental features to cope with changing threats and changes. Weakness and change in these features are considered the basis for weakening the national security of any country. Control over published information and the extensive volume of this information create awareness, insight, and enlightenment for users. Given that efforts are being made for media literacy in the dominant society, this space strongly governs the thoughts and feelings of society, can become the basis for cohesion and coherence in society, and can strengthen national security in all dimensions. Government control over information and news published and the control of this space by governments and authorities can achieve their goals. All of these factors intensify the phenomenon of strengthening national security, and the main reasons mentioned as causal conditions are recognized as the main reasons.

Contextual Condition: Background conditions are conditions under which strategies and actions are taken to manage the phenomenon. Contextual conditions in this research include 1- High volume of information, 2- Decentralized information, 3- National security enhancement, 4- National identity enhancement, 5- Economic improvement, 6- Social cohesion, 7- Increased accuracy and speed, 8- Media democracy, 9- Economic development, 10- Environmental protection, which creates a basis for enhancing national security.

Given that various types of information are produced on social media networks without any restrictions and spread rapidly among different users, it is natural that useful information and informative and real data,

combined with false data and information, are disseminated. With the strengthening of media literacy, a favorable environment is created for users and the body of this space. Government control over social media can improve the economy by creating virtual jobs and virtual entrepreneurship, increasing speed and accuracy in this space, strengthening national identity, and providing a platform for enhancing culture and increasing national security.

Main Concept or Axis: The central concept is a phenomenon that forms the foundation and axis of the process. The chosen central concept must be abstract enough to relate to other main concepts. The phenomenon studied in this research is national security opportunities in social media networks.

Intervention Conditions: Intervention conditions, such as culture and space, act as facilitators or constraints for strategies. In this research, intervention conditions include 1- Increasing the power of media democracy, 2- Information exploitation, 3- Empowering movements, 4- Soft power capability, 5- Increasing sustainable development, and 6- Cultural engineering.

Strategies: Specific actions or reactions resulting from the central concept. Strategies in this research include 1- Media literacy development, 2- Utilizing experts in social media networks, 3- Transparency and uncensored government access to information, 4- Economic development with a focus on cyberspace, 5- Expansion of advertising and government presence in the virtual space, 6- Defense of domestic values and convincing citizens, 7- Creating laws in the realm of social media networks, 8- Increasing biological participation, 9- Cultural diplomacy focus.

Today, for governments to maintain security, they must strive to achieve media power because media, especially social media, holds immense power in the age of communication and information. Therefore, governments should identify opportunities and threats created in social media networks and strengthen national security by increasing the media literacy of their citizens. Media literacy is so important that, according to Hougart (1390), it depends on the assessment of media literacy. When governments prioritize transparency in their activities and provide information and news to the audience without censorship, they create a platform for countering misinformation and incorrect information in the virtual space.

Governments can use experts in social media networks to produce suitable content aligned with their culture and society and establish native platforms for development and government legitimacy. By focusing on advertising and defending their domestic values, governments can persuade public opinion, leading to independence from external influences through internal production and economic development. In the realm of virtual space, governments can formulate relevant laws, and reduce confusion and misuse in social media networks by establishing institutions and organizations with specialized forces in cyberspace. These specialized forces can have effective awareness campaigns on social networks and contribute to the governance of the virtual space. Additionally, governments, through cultural diplomacy, can create cultural bridges in international relations, gaining relative dominance among other countries by promoting their culture and having a stronger soft power.

Consequences: Consequences include visible and invisible impactful outcomes resulting from the design of a place-based brand model based on the sense of belonging to the brand in society. The outcomes of implementing strategies in this research are as follows: 1- Media literacy awareness, 2- Rapid

information dissemination, 3- Information management, 4- Promotion of cultural communications, 5- Bridging ethnic and religious differences, 6- Strong cultural diplomacy, 7- Economic efficiency, 8- Strengthening national security, 9- Closer ties between different cultures, 10- Legitimacy, 11- Increased people's influence.

Selective Coding (theorizing stage): The presented diagrammatic model for the national security opportunity in virtual social networks is displayed in the paradigm model. The paradigm model is a formal model in which the main major categories are depicted (Qaderi, 2011).

Figure 2- The final codes of virtual social network opportunities for national security
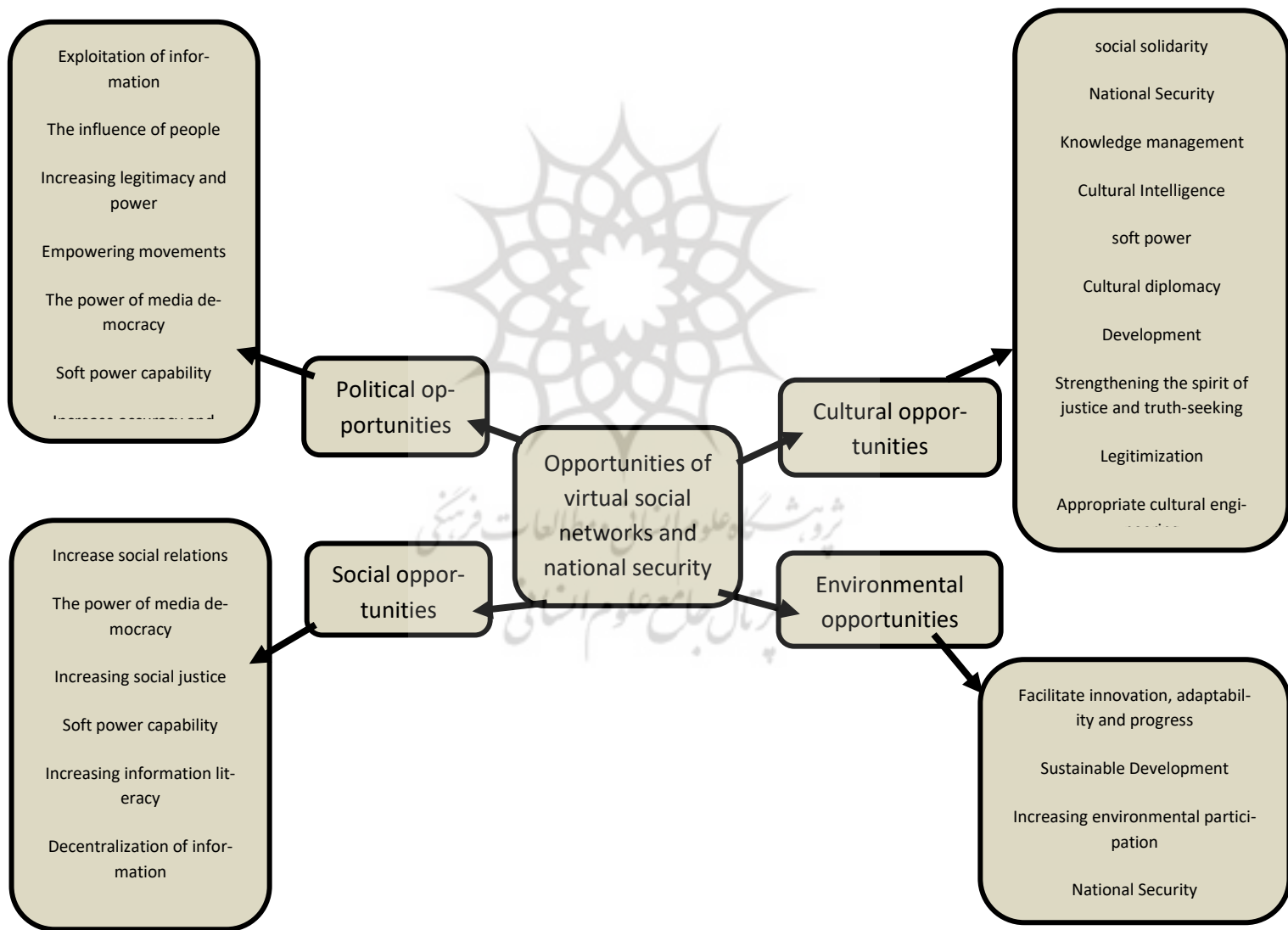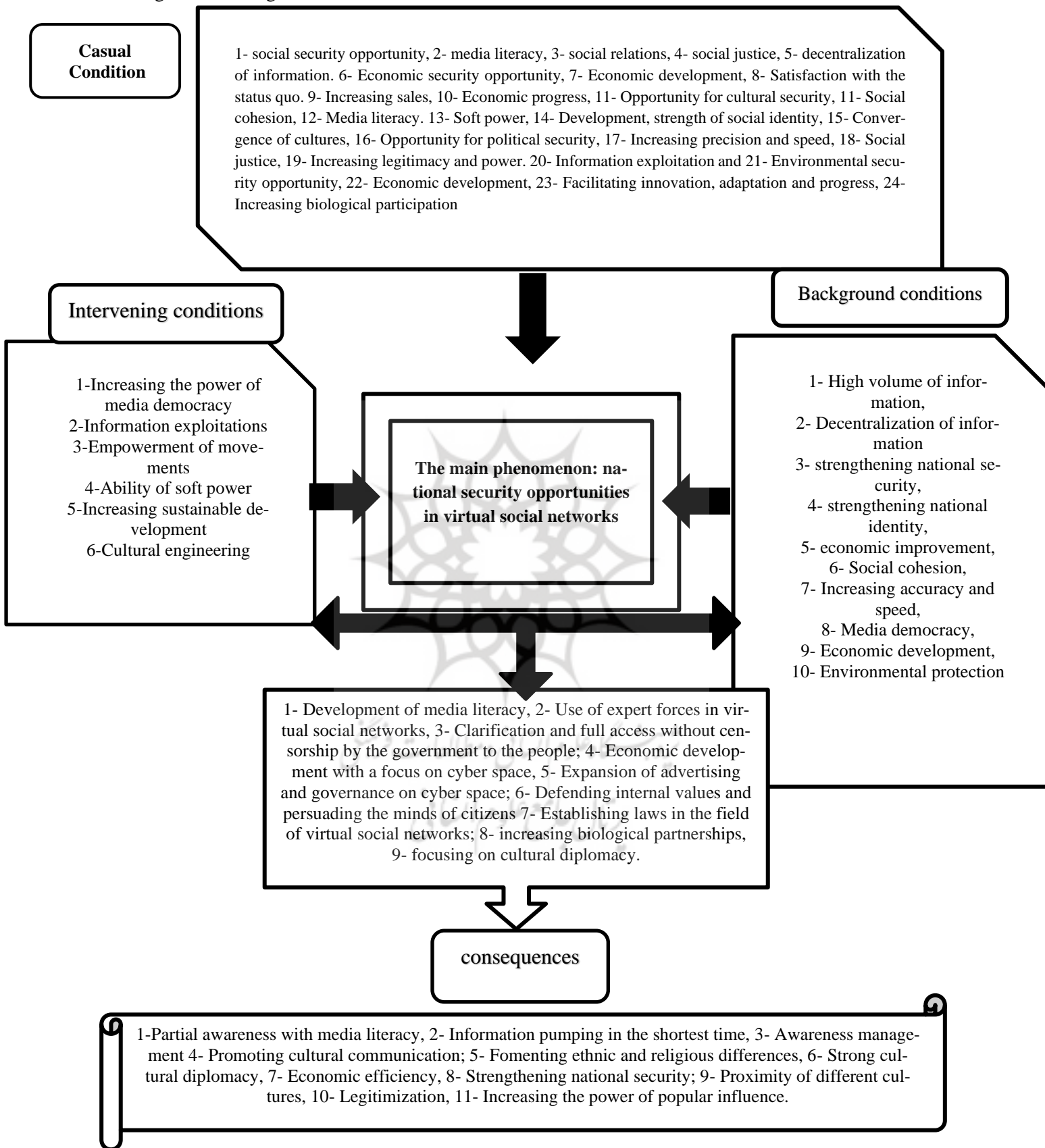
Figure 3: Paradigm model

Casual Condition

1- social security opportunity, 2- media literacy, 3- social relations, 4- social justice, 5- decentralization of information. 6- Economic security opportunity, 7- Economic development, 8- Satisfaction with the status quo. 9- Increasing sales, 10- Economic progress, 11- Opportunity for cultural security, 11- Social cohesion, 12- Media literacy. 13- Soft power, 14- Development, strength of social identity, 15- Convergence of cultures, 16- Opportunity for political security, 17- Increasing precision and speed, 18- Social justice, 19- Increasing legitimacy and power. 20- Information exploitation and 21- Environmental security opportunity, 22- Economic development, 23- Facilitating innovation, adaptation and progress, 24- Increasing biological participation

Intervening conditions

1-Increasing the power of media democracy
2-Information exploitations
3-Empowerment of movements
4-Ability of soft power
5-Increasing sustainable development
6-Cultural engineering

Background conditions

1- High volume of information,
2- Decentralization of information
3- strengthening national security,
4- strengthening national identity,
5- economic improvement,
6- Social cohesion,
7- Increasing accuracy and speed,
8- Media democracy,
9- Economic development,
10- Environmental protection

The main phenomenon: national security opportunities in virtual social networks

1- Development of media literacy, 2- Use of expert forces in virtual social networks, 3- Clarification and full access without censorship by the government to the people; 4- Economic development with a focus on cyber space, 5- Expansion of advertising and governance on cyber space; 6- Defending internal values and persuading the minds of citizens 7- Establishing laws in the field of virtual social networks; 8- increasing biological partnerships, 9- focusing on cultural diplomacy.

consequences

1-Partial awareness with media literacy, 2- Information pumping in the shortest time, 3- Awareness management 4- Promoting cultural communication; 5- Fomenting ethnic and religious differences, 6- Strong cultural diplomacy, 7- Economic efficiency, 8- Strengthening national security; 9- Proximity of different cultures, 10- Legitimization, 11- Increasing the power of popular influence.

In the foundational theory of data, the discussed problem begins with platforms and challenging domains and concludes with consequences and solutions. Our research's main issue starts from the point where the expansion and revolution of information and communication in virtual social networks have created opportunities for the national security of the country. The virtual space and the information flows within it are considered the most important and influential power streams, requiring careful management of this space. Social media networks have complex opportunities that create security infrastructures, including social, economic, cultural, political, and environmental security.

According to experts and researchers in the virtual space, social networks like WhatsApp and Telegram have provided golden opportunities to introduce cultural capabilities, enhance social capital through improving and maintaining individuals' social relationships, raising awareness, social education, and producing soft power for the country. to strengthen national security. Virtual social networks in the realm of social security increase accuracy and speed, empowering the country socially to dominate societies, enhancing people's influence, giving power to the media for democracy, enabling various movements, and increasing the exploitation power of information. In the political domain, they increase entered information and essentially provide the government with informational power, non-centralized information allows individuals to access extensive and diverse information, social justice increases through social networks' widespread dissemination of information and news. In the cultural domain, interactions and communications can create a form of cultural unity due to extensive cultural interactions, manage collective awareness, strengthen dominant ideologies in society, and have cultural legitimacy along with strengthening cultural intelligence.

Cultural intelligence helps enhance the ability to deal appropriately with multicultural situations. It contributes to social cohesion as one of the key dimensions of social capital, which can be considered as indicators of social, cultural, and political development in the country. As mentioned, empowering people's governance leads to accountability and questioning of the government regarding the legitimate demands of the people, which is a kind of enlightenment. This issue can cultivate a spirit of justice and truth-seeking in society. In the environmental field, it can lead to creativity, innovation in the environmental field, and environmental preservation as a foundation for progress and development in society. Sustainable development is accompanied by the ability to participate in the environmental field due to the various groups' activities in this space. Finally, based on the obtained results, several strategies and suggestions are proposed to strengthen national security infrastructures in virtual social networks:

Increase the media literacy level of the general public, especially active adolescent and young groups in virtual social networks. This can be achieved by organizing educational classes, introducing work methods and activities in the online space as a source of study at various educational levels, and identifying and introducing the main functions of the cyber space without restrictions through the publication of books, articles, films, and promotional teasers. Monitor information on virtual social networks with the help of experienced and specialized cyber and virtual space experts.

Establish and strengthen domestic platforms in the cyber space and strive to produce internal content.

References

Qaderi, Salahuddin. (2011). Examining the consequences and results of crime prevention programs in the public spaces of the city with an emphasis on the plan to improve social security. PhD Thesis, Faculty of Social Sciences, University of Tehran.

Libicki, Martin C., (2014). Cyber warfare and cyber deterrence. Translated by Faraji Astana, Payman; Shirmohammadi, Javad, Publications of Imam Ali University (AS), research assistant.

Al Huwaish, Y. (2017). Enhancing Intellectual Security in Light of Contemporary Global Models and Experiences; King Abdulaziz Center for National Dialogue: Riyadh, Saudi Arabia, 2017.

Alqahtani, Abdulrahman. (2014). Awareness of the Potential Threat of Cyberterrorism to the National Security. Journal of Information Security, Vol.5 No.4, October 2014.

Asogwa C. E. (2017). Media preference and usage pattern among diabetes patients in Enugu State, Nigeria. Global Media Journal, 15(29), 1–7.

Asogwa, Chika Euphemia (2020). Internet-Based Communications: A Threat or Strength to National Security? SAGE Open Volume 10, Issue 2, April-June 2020.

Charmaz, K. (2006) Constructing Grounded Theory. Sage Publications, London.

Innes, M.; Dobreva, D.; Innes, H. (2019). Disinformation and digital influencing after terrorism: Spoofing, truthing and social proofing. Contemp. Soc. Sci. 2019, 16, 241–255.

Lee, J. (2001). A grounded theory: Integration and Internalization in ERP adoption and use, Unpublished Doctoral Dissertation, University of Nebraska, In Proquest UMI Database.

Mathes, E.W. (1981). Maslow's Hierarchy of Needs as a Guide for Living. J. Humanist. Psychol. 1981, 21, 69–72. [CrossRef].

McQuail D. (2005). Mass communication theory. Sage.

Wanja, S.W.; Muna, W. Effects of social media on Security-Agenda Setting in Nairobi City County, Kenya. Int. J. Curr. Asp. 2021, 5, 64–77.