



Analyzing Upstream Documents of Virtual Space With Content Analysis Method

Roya. Seddighi¹, Akbar. Nasrollahi^{2*}, Mastooreh. Ezzatzadeh³

¹ PhD Student, Department of Media Management, Central Tehran Branch, Islamic Azad University, Tehran, Iran

² Associate Professor, Department of Media Management, Faculty of Social Sciences, Communication and Media, Central Tehran Branch, Islamic Azad University, Tehran, Iran

³ Assistant Professor, Department of Media Management, West Tehran Branch, Islamic Azad University, Tehran, Iran

* Corresponding author email address: akbar.nasrollahi@gmail.com

Received: 2024-09-19

Revised: 2024-11-29

Accepted: 2024-12-08

Published: 2025-01-01

The role of cyberspace is so significant and fundamental that activities in all aspects of society are impossible without it. In this context, upstream policy documents in this industry play a crucial role in determining its trajectory. Accordingly, the present study was conducted with the aim of analyzing the content of upstream policy documents of the Supreme Council of Cyberspace. A total of four upstream and specific policy documents were selected and analyzed. Through data analysis, a total of 351 focal points and 66 categories emerged at different levels of the documents. The findings of this study indicate that 81 focal points and 30 categories emerged at various levels of the documents. Additionally, a communication map illustrating the relationships among multiple categories within the documents at different levels has been developed and presented in the form of a comprehensive diagram depicting key indicators related to the national cyberspace framework.

Keywords: Policy Documents, Cyberspace, Content Analysis.

How to cite this article:

Seddighi, R., Nasrollahi, A., & Ezzatzadeh, M. (2025). Content Analysis of Upstream Policy Documents in Cyberspace. *Interdisciplinary Studies in Society, Law, and Politics*, 4(1), 50-55. <https://doi.org/10.61838/kman.isslp.4.1.5>

1. Introduction

Upstream policy documents refer to documents that have been ratified by the highest legislative authorities of the country and possess legal status (A'Arabi, 2017). These documents serve as the foundation for long-term, medium-term, and short-term planning to achieve comprehensive development goals. The study of these documents clarifies the expectations of upstream institutions (Moradkhani & Taklu, 2021). In Iran, comprehensive and complete programs have been developed to advance goals in various fields (Hafez, 2009; Hamidzadeh, 2005). Once these programs are approved by relevant authorities, they are recognized as

upstream policy documents. In other words, these documents function as a roadmap for different sectors. This research examines upstream policy documents in response to the question: What are the perspectives of upstream institutions regarding the Supreme Council of Cyberspace?

2. Methodology

To address this question, upstream policy documents of the Supreme Council of Cyberspace were identified, and the content analysis method was employed to examine and model these documents.

The content analysis method in this study follows the stages outlined by Krippendorff (2019). The



implementation of content analysis was carried out as follows (Krippendorff, 2019):

Formulating content analysis-related questions:

- What are the key thematic issues emphasized in the upstream policy documents related to the Supreme Council of Cyberspace?
- How are the key themes interconnected at different levels of the documents?
- What focal points and categories exist in the upstream policy documents related to the Supreme Council of Cyberspace at various levels, including the national level and the Supreme Council of Cyberspace of Iran?

Defining the target population: All documents at different national levels and documents from the Supreme Council of Cyberspace of Iran.

Determining the unit of analysis: The entire text of each document was considered the unit of analysis, after which meaningful units were identified in the form of sentences.

Document analysis: Extracted statements in sentence format emphasize that a sentence refers to an expression containing at least one complete declarative or imperative sentence conveying an independent meaning.

In accordance with the research design, all data were reviewed, coded, categorized, and organized during the content analysis process. Initially, units of analysis were identified, followed by condensing meaningful units into

codes. These codes were then summarized, forming broader categories.

3. Findings

Upstream policy documents function as roadmaps for various sectors.

For the analysis of policy documents in the field of cyberspace and the Supreme Council of Cyberspace, the content analysis method was utilized.

The national level includes documents and statements issued by the Supreme Leader over the years, which must be incorporated into national policy.

The Supreme Council of Cyberspace level includes documents that encompass all sectors related to the council and its subsidiaries.

In accordance with the research design, all data were reviewed, coded, categorized, and organized during the content analysis process. Initially, units of analysis were identified, followed by condensing meaningful units into codes.

Initially, the following table provides a list of analyzed documents along with their respective levels and the codes assigned by the researcher for easy and quick identification. The document level refers to the issuing authority and the scope of the document. The national level includes documents issued by the Supreme Leader over the years that must be implemented at the national level.

Table 1

Names and Levels of Analyzed Documents with Assigned Codes

Document Level	Document Name	Document Code
National	Decree on the Formation and Appointment of Members of the Supreme Council of Cyberspace	M2
National	General Policies on Cybersecurity and Information Exchange Security (FATA)	M3
National	Vision Document of the Islamic Republic of Iran for 2025	M5

Table 2

Extracted Focal Points and Categories from Policy Documents

Source (Document)	Focal Point / Code	Category
M1	Manage cyberspace in favor of national values	Emphasis on values in cyberspace
M1	Cyberspace is as significant as the Islamic Revolution	-
M1	Strengthening cyberspace capabilities is vital for the country	Power in cyberspace
M1	Powerful countries set red lines in cyberspace	Observing red lines
M1	National Information Network implementation requires a timeline	Necessity of the National Information Network
M1	Continuous emphasis on forming the National Information Network	-
M1	Economic significance of cyberspace within the framework of national resilience policies	Knowledge-based economy in cyberspace

M1	Promoting Islamic-Iranian norms, values, and lifestyle, and countering cultural and social threats	Promotion of values in cyberspace
M1	Effective management of cyberspace is essential	Cyberspace governance
M1	National cybersecurity and protection of individual privacy	Comprehensive cybersecurity
M1	Cyberspace presents both opportunities and threats	Attention to cyberspace risks and opportunities
M1	Increasing digital literacy and responsible internet use	Enhancing digital literacy
M1	Strengthening domestic content production	Boosting digital content creation
M1	Cyberspace should be leveraged for social resilience and national security	Cyberspace resilience and security

According to the research design, all data were examined, coded, categorized, and organized. Initially, units of analysis were identified, followed by condensing

meaningful units into codes. These codes were then summarized to form broader categories.

Table 3

Focal Points and Categories Related to Iran's Cyberspace in the 20-Year Vision Document

Source (Document)	Focal Point / Code	Category
M1	A space extending the real world—healthy, secure, beneficial, and a driver of progress in other sectors—based on the country's endogenous capacities.	A space extending the real world—healthy, secure, beneficial, and a driver of progress in other sectors—based on endogenous national capacities.
M1	Active, innovative, strong, and goal-oriented presence in regional and international forums and institutions.	Active, innovative, strong, and goal-oriented presence in international institutions.
M1	An inspirational entity in the Islamic world and a key player on the global stage.	Inspirational in the Islamic world and a key player globally.
M1	Equipped with effective and efficient specialized human resources.	Equipped with specialized human resources, scientific, and research centers, and knowledge-based institutions.
M1	Equipped with scientific and research centers, knowledge-based companies, and advanced domestic industries.	-
M1	Possessing reliable, secure, sustainable, integrated, and widespread infrastructure across the country on the National Information Network and connected to the global network.	Possessing reliable and sustainable infrastructure on the National Information Network, connected to the global network, and ranking as the leading cyber power and top provider of cyberspace services in West and Southwest Asia.
M1	The leading cyber power and top provider of cyberspace services in West and Southwest Asia, with constructive and effective engagement in international relations and the peaceful use of cyberspace through the participation of all countries in its development.	-

Table 4

Decree on the Formation and Appointment of Members of the Supreme Council of Cyberspace

Source (Document)	Focal Point / Code	Category
M1	Comprehensive national commitment and serious investment in the creation and development of advanced and competitive technologies and industries.	Serious investment in the creation and development of various technologies.
M1	Elevating the Islamic Republic of Iran to the status of a global cyber power on par with influential world powers.	Elevating the Islamic Republic of Iran to a global cyber power on par with influential world powers.
M1	Developing and approving necessary security, legal, judicial, and regulatory frameworks for cyberspace.	Developing and approving security frameworks and ensuring comprehensive cybersecurity at the national level.
M1	Special attention to the purification and comprehensive security of national cyberspace.	-
M1	Protection of individual privacy.	Protection of individual privacy.
M1	Strengthening the position of the National Cyberspace Center as the executive arm of the Supreme Council of Cyberspace for implementing its decisions.	Strengthening the National Cyberspace Center and accelerating the establishment of the National Information Network.
M1	Accelerating the establishment of the National Information Network following its approval by the Supreme Council and ensuring continuous oversight.	-
M1	Promoting Islamic-Iranian norms, values, and lifestyle while preventing cultural and social threats.	Promoting Islamic-Iranian norms, values, and lifestyle.

M1	Securing an appropriate position and share for a knowledge-based economy in cyberspace within the framework of national resilience policies.	Securing an appropriate position and share for a knowledge-based economy in cyberspace.
M1	Developing efficient and competitive content and services aligned with Islamic-Iranian values and culture across all societal needs.	Developing efficient and competitive content and services aligned with Islamic-Iranian values and culture.

Table 5

Focal Points and Categories in the General Policies on Cybersecurity and Information Exchange Security (FATA)

Source (Document)	Focal Point / Code	Category
M1	Continuity of public services.	Securing critical and sensitive national IT and communication infrastructures and continuously enhancing the security of electronic networks and information systems.
M1	Sustainability of national infrastructures.	-
M1	Protection of national secrets.	-
M1	Preserving Islamic-Iranian culture and identity, and ethical values.	-
M1	Safeguarding privacy, legitimate freedoms, and material and intellectual assets.	-
M1	Monitoring, prevention, defense, and enhancing deterrence capabilities against threats in the IT and communications domain.	Monitoring, prevention, defense, and enhancing deterrence capabilities.
M1	Effective and constructive regional and global engagement, and joint cooperation and investment in knowledge, technology, and cybersecurity while safeguarding national interests and security.	International communication cooperation while maintaining national interests and security.
M1	Relying on indigenous technology and domestic expertise in developing scientific and technical infrastructures for cybersecurity.	Enhancing the level of knowledge and scientific, research, educational, and industrial capacities of the country.
M1	Development of IT and communication technologies while considering security measures.	-
M1	Enhancing the level of knowledge and scientific, research, educational, and industrial capacities of the country for the production of cybersecurity-related knowledge and technology (FATA).	-
M1	Assigning a designated authority under government oversight to guide, supervise, and establish necessary standards for maintaining and developing cybersecurity in information production and exchange.	Legislation and regulation.
M1	Raising public awareness, education, and increasing general skills in cybersecurity.	Awareness-raising and education.
M1	Adhering to religious and legal principles concerning the protection of individual and social rights in the implementation of these policies.	-

After extracting codes and categories from upstream policy documents, the frequency of identified categories was calculated based on the number of associated codes, resulting in a total of 81 codes. To determine reliability, Holsti's formula was applied. Holsti's reliability coefficient is used to assess the validity of qualitative content analysis. This index, introduced by Holsti, is a variation of the percentage agreement metric for cases where coders do not assign codes to exactly the same text segments. In other words, different excerpts from the text may be selected for a single code. Additionally, Holsti's index does not account for chance agreement.

The Holsti index ranges between 0 and 1. Generally, a Holsti index above 0.9 indicates a high level of reliability in qualitative content analysis. However, in various studies, a threshold above 0.8 is considered acceptable. For the reliability assessment, 20% of the coded textual content from the documents was randomly selected and provided to two expert coders, who were thoroughly briefed on the research subject. After receiving the coded data, Holsti's reliability coefficient was calculated, resulting in a value of 0.90 (90%), which indicates an acceptable level of reliability for the content analysis.

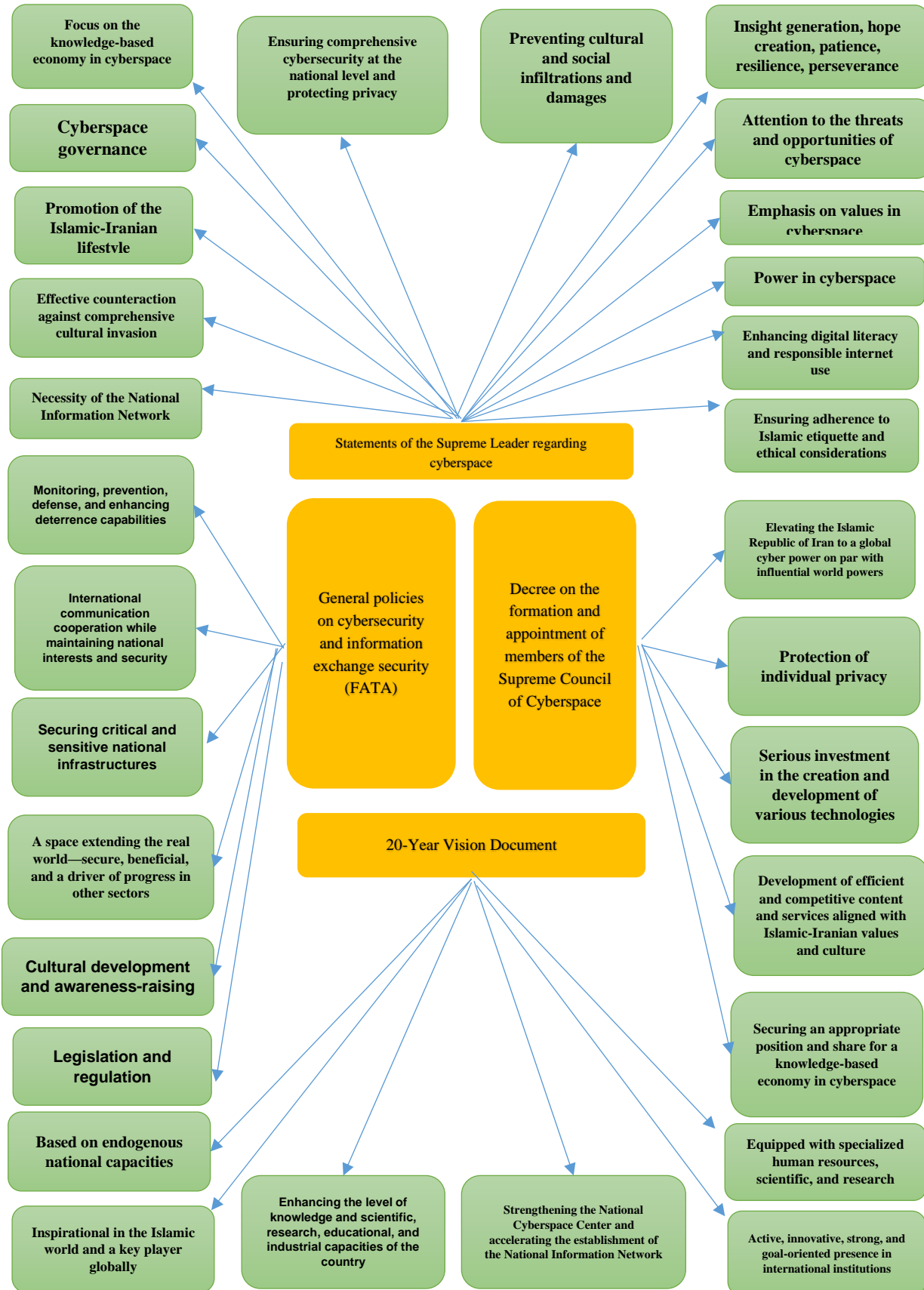
Table 6

Frequency of Codes Used for Reliability Calculation

Total Codes	Number of Codes Tested by Coder 1 (Approximately 20% of Total Codes)	Codes Tested by Coder 2	Codes Agreed Upon by Both Coders
81	17	16	15

Figure 1

Paradigm Model of Study



4. Conclusion

The findings of this study highlight the critical role of upstream policy documents in shaping the trajectory of cyberspace governance in Iran. Through content analysis of key documents issued by the Supreme Council of Cyberspace, fundamental focal points and categories were identified, providing a structured understanding of national priorities in this domain. The results indicate that cyberspace is positioned as a strategic and sovereign domain, necessitating comprehensive security frameworks, regulatory policies, infrastructure development, and international engagement.

One of the key takeaways from this analysis is the emphasis on national cybersecurity, digital sovereignty, and the integration of knowledge-based economic strategies. The study also underscores the importance of safeguarding cultural and ethical values, reinforcing the need for effective governance mechanisms to balance technological advancements with national security concerns and socio-cultural preservation.

Moreover, the application of Holsti's reliability coefficient confirmed a high level of reliability in the content analysis process, ensuring the validity of the extracted data. The 90% agreement rate between coders further affirms the robustness of the findings, making the conclusions drawn from this study highly credible for policy and decision-making.

Given the increasing complexities of cyberspace governance, future research should focus on evaluating the implementation of these upstream policy documents and their real-world impact on digital transformation, national security, and global engagement. Additionally, a comparative study of cyberspace policies in other countries could provide valuable insights for refining Iran's strategic approach to cyberspace governance.

In summary, the study demonstrates that Iran's cyberspace policies are evolving towards a secure, resilient, and innovative digital ecosystem, with a strong emphasis on technological independence, regulatory oversight, and international collaboration. These insights can contribute to a more cohesive and adaptive policy framework, ensuring that national cyberspace governance aligns with both domestic priorities and global digital advancements.

Authors' Contributions

Authors contributed equally to this article.

Declaration

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

Transparency Statement

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

Acknowledgments

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

Declaration of Interest

The authors report no conflict of interest.

Funding

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

Ethical Considerations

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

References

- A'Arabi, S. M. (2017). *Strategic Planning Guide (Step by Step)*. Cultural Research Office Publications.
- Hafez, M. (2009). Challenges and Prospects of Security in Cyberspace. *Bi-monthly Journal of Human Development of Police*(1).
- Hamidzadeh, M. R. (2005). *Strategic Planning*. Samt Publications.
- Krippendorff, K. (2019). *Content Analysis: An Introduction to Its Methodology* (Fourth Edition ed.) <https://doi.org/10.4135/9781071878781>
- Moradkhani, F., & Taklu, S. (2021). The Multiplicity of Legislative Institutions with Emphasis on the Position of the Supreme Council of Cyberspace Resolutions in Iran's Legal System. *Contemporary Legal Studies*, 12.