Journal of Cyberspace Studies
eISSN: 2588-5502
http://jcss.ut.ac.ir
University of Tehran

Co-creating cyberspace governance: A boundary critique perspective on digital participation and policy legitimacy

Seyed Mohammad Sobhani[1]*, Mohammad Reza Fathi[2], Shima Ghadimi[3]

1. Department of Business Policy Making at SR.C., Islamic Azad University, Science and Research Branch, Tehran, Iran. (*Corresponding author: mohammad.sobhanii@iau.ac.ir, https://orcid.org/0000-0003-2977-8791)
2. Department of Management and Accounting, College of Farabi, University of Tehran, Qum, Iran.
3. Department of Accounting, Daneshestan Institute of Higher Education, Saveh, Iran.

Article Info

Original article

Main Object: Business & Economics

Received: 12 July 2026
Revised: 07 August 2026
Accepted: 28 August 2026
Published online: 12 September 2026

Keywords:
boundary critique,
critical systems heuristics,
cyberspace governance,
digital participation,
policy legitimacy.

Abstract

Background: Cyberspace governance has become a complex socio-technical field where sovereignty, cybersecurity, digital participation, and policy legitimacy intersect. Although previous studies have extensively examined digital sovereignty, e-participation, and co-creation, limited attention has been paid to how boundary judgments shape stakeholder inclusion, decision authority, knowledge recognition, and legitimacy in cyberspace governance, particularly in the Iranian context.
Aims: This study aims to examine how Critical Systems Heuristics (CSH) can reveal and reconstruct the boundary judgments shaping co-created cyberspace governance, digital participation, and policy legitimacy in Iran.
Methodology: A qualitative exploratory case study design was adopted, drawing on semi-structured interviews with 26 experts and analysis of policy, regulatory, and strategic documents. Data were analyzed using Ulrich and Reynolds' CSH framework by distinguishing current "is" conditions from desirable "ought to be" arrangements across the dimensions of motivation, control, knowledge, and legitimacy.
Findings: The analysis indicates that current cyberspace governance is primarily bounded by security, sovereignty, infrastructural control, regulatory authority, and technical expertise. However, affected stakeholders, including citizens, digital businesses, educators, researchers, civil society actors, vulnerable groups, and future generations, remain weakly represented in governance processes.
Conclusion: The study argues that legitimate cyberspace governance requires a transition from primarily control-oriented arrangements toward structured co-creation based on stakeholder inclusion, plural knowledge, transparent accountability, and participatory boundary governance.

Cite this article: Sobhani SM, Fathi MR, Ghadimi S. (????). "Co-creating cyberspace governance: A boundary critique perspective on digital participation and policy legitimacy". *Cyberspace Studies*. ?(?): 1-35. doi: https://doi.org/10.22059/jcss.2026.418413.1260.

Creative Commons Attribution-NonCommercial 4.0 International License
Website: https://jcss.ut.ac.ir/| Email: jcss@ut.ac.ir |
EISSN: 2588-5502
Publisher: University of Tehran

in press

Cyberspace Studies, Vol ?, No ?, ????

1. Introduction

Cyberspace has become a strategic domain in which questions of public administration, sovereignty, security, economic development, cultural regulation, citizen participation, and institutional legitimacy increasingly converge. Contemporary digital governance is no longer reducible to the technical management of information systems or the digitization of public services; rather, it concerns the organization of power, coordination, trust, accountability, and value creation across complex socio-technical environments (Hanisch et al., 2023; Sharma et al., 2024). In this context, governments are required not only to provide digital services but also to justify how digital infrastructures, platforms, data flows, cybersecurity arrangements, and participatory mechanisms are governed. This has made cyberspace governance a deeply political and systemic field, shaped by competing claims over control, expertise, inclusion, sovereignty, and public legitimacy (Hofmann & Pawlak, 2023; Pohle & Santaniello, 2024).

Recent scholarship shows that cyberspace governance is increasingly shaped by boundary conflicts. These conflicts emerge from competing claims over authority, infrastructure control, interest representation, and the recognition of legitimate actors in digital policymaking (Hofmann & Pawlak, 2023; Pierucci, 2025). At the same time, the global shift from multistakeholder internet governance toward digital sovereignty has intensified tensions between state authority, public participation, platform power, cybersecurity, economic innovation, and digital rights (Pohle & Santaniello, 2024; Pierucci, 2025). Such tensions are especially significant in countries where cyberspace is simultaneously viewed as a developmental infrastructure, a security domain, a cultural field, and a space of social mobilization.

Iran provides a particularly important context for examining these tensions. Cyberspace governance in Iran is shaped by the simultaneous pursuit of digital sovereignty, national security, cultural governance, domestic platform development, e-government expansion, and efforts to manage information environments, which may create tensions with participation and legitimacy objectives. These priorities are not analytically separable from broader challenges of public trust, fragmented institutional authority, sanctions-related technological constraints, platform restrictions, digital business uncertainty, uneven access, and limited channels of citizen participation. From an institutional-capacity perspective, sustainability-oriented organizational practices also show that legitimacy depends not only on external stakeholder engagement but also on internal human, cultural, and managerial infrastructures capable of supporting long-term public value (Khosravi et al., 2022). Prior research on e-participation in Iran has identified barriers related to administrative culture, institutional structure, attitudes toward participation, and limited staff capacity for engaging the public through digital mechanisms (Shahab et al., 2021).

UT PRESS

These conditions suggest that the main problem is not merely the absence of digital tools, but the deeper governance question of how participation is defined, authorized, limited, or excluded.

The concept of co-creation is therefore central to this study. In public governance, co-creation refers to the collaborative production of public value through interaction among public institutions, citizens, experts, private actors, and civil society stakeholders (Voorberg et al., 2015; Osborne et al., 2016). However, in cyberspace governance, co-creation cannot be treated as a simple invitation for citizens to use digital platforms or provide feedback after policy decisions have already been made. Genuine co-creation requires affected stakeholders to participate in defining policy problems, evaluating governance alternatives, identifying risks, and shaping legitimacy criteria. This also makes co-creation a knowledge-governance problem: participation becomes meaningful only when stakeholder knowledge is institutionally collected, interpreted, incorporated and reviewed (Fathi et al., 2021). This distinction is crucial in the Iranian context, where digital participation may exist at the level of service use or administrative interaction while remaining weak at the level of agenda setting, deliberation, policy design, and accountability. To address this problem, the present study adopts Critical Systems Heuristics (CSH) as a conceptual and analytical framework, drawing particularly on Ulrich and Reynolds' boundary critique approach. CSH is appropriate because it treats governance problems as boundary problems: every policy system rests on judgments about what is included, what is excluded, whose purposes matter, who controls resources, whose knowledge counts, and who represents those affected but not involved (Ulrich & Reynolds, 2010). CSH further distinguishes between the existing "is" situation and the normatively desirable "ought to be" situation, enabling researchers to critically compare current institutional arrangements with more inclusive and legitimate alternatives (Ulrich & Reynolds, 2010; Hutcheson et al., 2024). Recent systematic work confirms that CSH is especially useful for examining power asymmetries, coercive conditions, marginalized stakeholders, and emancipatory possibilities in complex governance settings (Hutcheson et al., 2024). Recent applications of Critical Systems Heuristics demonstrate its usefulness for examining complex governance and reliability challenges across organizational contexts (Fathi et al., 2026).

Accordingly, this study argues that the legitimacy deficit in cyberspace governance cannot be adequately understood through technical, legal, or administrative analysis alone. It must be examined through the boundary judgments that organize digital governance: who is treated as a beneficiary, who controls decisions, what knowledge is recognized as valid, and how affected but excluded groups are represented. In Iran, these questions are especially consequential because cyberspace policies affect not only state institutions and

In Press

Cyberspace Studies, Vol ?, No ?, ????

infrastructure providers but also citizens, students, digital entrepreneurs, online businesses, educators, researchers, content creators, women, vulnerable groups, and future generations.

This article therefore asks:

RQ1. How are boundary judgments constructed in cyberspace governance in Iran?

RQ2. How do these boundary judgments influence digital participation and policy legitimacy?

RQ3. How can Critical Systems Heuristics support the development of a co-created cyberspace governance model?

In doing so, the study positions boundary critique as a necessary methodological bridge between critical systems thinking and the practical reform of digital governance.

2. Literature review

2.1. The digital domain as a contested socio-technical field and digital sovereignty

Recent cyberspace governance literature increasingly treats the digital domain as a contested socio-technical field rather than a neutral infrastructure. A central debate concerns digital sovereignty, which has moved from a narrow concern with jurisdiction and data localization toward a broader policy discourse about control, autonomy, resilience, rights, and institutional accountability. Falkner et al. (2024) show that digital sovereignty has become a dominant policy vocabulary but does not always translate coherently into policy change. Santaniello (2026) further conceptualizes digital sovereignty as a discursive resource shaped by adversariality, multiversity, instrumentality, and contradictory political uses.

Similarly, Fratini et al. (2024) identify multiple sovereignty models, including rights-based, market-oriented, centralization-based, and state-based models, concluding that none fully resolves the challenge of combining regulatory control with responsiveness to technological and social change. These studies are highly relevant to Iran, where cyberspace governance is shaped by national sovereignty, security concerns, domestic infrastructure development, platform control, sanctions related constraints, and public trust tensions. The Iranian context therefore requires an analytical frame that does not reject sovereignty concerns but asks how sovereignty can be bounded by participation, accountability, and legitimacy.

2.2. Digital participation and e-participation

Recent studies caution that digital participation should not be equated with the mere existence of digital platforms. Shin et al. (2024), in a systematic analysis of 116 digital citizen participation tools, show that many tools facilitate the flow of information from citizens to

In Press

governments but remain weak in communicating accountability information back to citizens. This is critical for cyberspace governance because participation without feedback, traceability, or responsiveness can become symbolic rather than legitimate. Lai and Beh (2025) similarly argue that e-participation studies have often fallen into "technological solutionism" by emphasizing adoption models while neglecting political efficacy and citizens' psychological capacity to believe that participation matters. Escher and Rottinghaus (2024) show that online participation can strengthen legitimacy beliefs, but not automatically; legitimacy gains depend on process quality, expectations, trust, and perceived policy effects. These findings are directly applicable to Iran, where digital participation must be studied not only as access to e-services but as meaningful influence over agenda setting, consultation, policy design, evaluation, and correction.

2.3. Co-creation and co-production

Co-creation is increasingly presented as a response to complex public problems because it mobilizes dispersed knowledge, strengthens ownership, and enables cross-boundary problem solving. Evidence from Iranian educational services similarly indicates that value co-creation produces reciprocal outcomes for both participants and institutions, including relationship development, capability formation, identity strengthening, brand improvement, market learning, and financial sustainability (Zargaran Khouzani et al., 2022). Ansell et al. (2024) argue that the democratic quality of co-creation lies in empowering lay actors to participate in shared problem solving and joint agreement over public value outcomes. Edelmann and Virkar (2023) show that sustainable co-creation of digital public services requires more than technological mediation; it depends on institutional learning, resource integration, stakeholder knowledge, and long-term governance capacity. Pauluzzo et al. (2024) similarly find that research on digital technology and public sector co-creation remains underdeveloped from a governance perspective and needs greater attention to public value generation, the whole service cycle, comparative designs, and risk mitigation. For the present study, this means that co-creating cyberspace governance should not be reduced to citizen feedback mechanisms. It should involve reconstructing the boundaries of who participates, whose knowledge is recognized, which institutions control digital decisions, and how policy legitimacy is assessed. This is consistent with Iranian evidence from foreign language institutions, where value co-creation was found to depend on sustained interaction, participant engagement, customer knowledge, and mutually reinforcing mechanisms rather than one-way service provision (Sobhani et al., 2023).

In Press

Cyberspace Studies, Vol ?, No ?, ????

2.4. Digital governance in politically constrained or state-centered contexts

Comparative work on e-participative governance in China shows that digital participation may emerge through different pathways, including disclosure, consultation, and deliberation, while still operating within state-managed boundaries (Xin & Huang, 2025). This literature is useful for analyzing Iran because it avoids a simplistic binary between participation and control. Instead, it shows that participation can be institutionally opened, selectively channeled, or strategically limited depending on the state society relationship. Related evidence from sustainability governance shows that coercive and non-coercive drivers operate through different pathways, with coercive mechanisms strengthening monitoring and non-coercive mechanisms supporting collaboration, suggesting that legitimacy-oriented governance cannot rely solely on command-and-control arrangements (Nasrollahi et al., 2021). In Iran's case, cyberspace governance is shaped by tensions among national security, cultural regulation, domestic platform policy, technological autonomy, public demand for access, and the needs of digital businesses. Therefore, the literature suggests that the key research problem is not whether participation exists, but what type of participation is institutionally possible, whose participation is authorized, and which affected groups remain outside the governance boundary.

2.5. Critical Systems Heuristics and boundary critique

Finally, the literature on Critical Systems Heuristics and boundary critique provides the methodological bridge. Recent systems research has extended CSH into information systems and governance settings by emphasizing that system boundaries define not only what is technically included but also who is affected by consequences and who can influence design choices. Goede and Goede (2025) argue that poorly designed information systems generate unintended consequences and that CSH can help reveal conditioned realities, feedback loops, and the position of affected but uninvolved actors. This is directly aligned with the present article because Iranian cyberspace governance is not simply a technical policy system; it is a boundary system involving beneficiaries, decision makers, experts, witnesses, affected groups, and competing worldviews. The unresolved gap is not the absence of studies on digital sovereignty, e-participation or co-creation separately, but the absence of a boundary critique that explains how these domains are institutionally connected, who is included or excluded, and how legitimacy is constructed in Iran's cyberspace governance system. To provide a more systematic and critical synthesis of the reviewed literature, Table 1 compares the selected studies in terms of their research context, analytical focus, methodological design, empirical basis, principal findings, unresolved limitations, and relevance to the present study.

In Press

Table 1. Comparative and critical mapping of the literature underpinning the study

Study	Context and research focus	Methodological design and data	Principal findings	Unresolved limitation or research gap	Relevance to the present study
Falkner et al. (2024)	European Union digital policymaking; relationship between digital-sovereignty discourse and actual policy change	Conceptual and comparative synthesis of contributions to a special issue on EU digital sovereignty	Digital sovereignty has become a central policy discourse, but its meaning and translation into policy vary across institutions and policy domains	Focuses predominantly on the EU and does not examine affected stakeholders, participatory legitimacy, or boundary judgments in state-centred contexts	Demonstrates that sovereignty must be examined as a contested governance concept rather than as a neutral policy objective
Santaniello (2026)	Geopolitics and competing political uses of digital sovereignty	Constructivist conceptual analysis and development of a multidimensional framework for digital-sovereignty discourse	Digital sovereignty is shaped by adversariality, multiple meanings, instrumentality, and contradictory political uses	Provides a conceptual framework but does not empirically examine how sovereignty discourses affect stakeholder participation and policy legitimacy	Supports the analysis of competing security-, sovereignty-, rights-, and participation-oriented worldviews
Fratini et al. (2024)	National approaches to digital sovereignty across different political and institutional settings	Systematic review and coding of 271 peer-reviewed publications; comparative construction of four sovereignty models	Identifies rights-based, market-oriented, centralization-based, and state-based models; none fully combines comprehensive regulation with adaptability to technological and societal change	Compares sovereignty models at a broad level but does not analyze who benefits, who controls resources, or who represents affected groups	Provides a typology against which Iran's predominantly state- and control-oriented governance arrangements can be critically assessed
Shin et al. (2024)	Digital citizen-participation tools used in public policymaking	Systematic supply-side analysis of 116 digital tools collected from three public	Many tools enable citizens to submit information or preferences, but fewer	Focuses on technological functionalities rather than the institutional	Supports the distinction between digital access or feedback and meaningful

i.Press

Study	Context and research focus	Methodological design and data	Principal findings	Unresolved limitation or research gap	Relevance to the present study
		repositories	provide accountability information, feedback, or traceability of policy impact	power structures determining whether citizen input influences decisions	participation in policy formation and accountability
Lai & Beh (2025)	Citizens' willingness to participate through digital-government channels	Quantitative survey of 388 respondents analyzed using partial least squares structural equation modelling	Internal and external political efficacy strongly influence citizens' willingness to engage in digital participation	Concentrates on individual behavioral intention and gives limited attention to institutional exclusion, decision authority, and policy responsiveness	Shows that participation depends not only on technology but also on whether citizens believe their involvement can influence governance
Escher & Rottinghaus (2024)	Online citizen-participation platforms in three German municipalities	Comparative municipal study using survey-based assessment of participation processes and legitimacy beliefs	Online participation may improve legitimacy beliefs, but outcomes depend on process quality, expectations, trust, and perceived policy influence	Findings arise from local democratic settings and do not explain participation under centralized, security-sensitive, or institutionally constrained governance	Establishes the theoretical connection between participation quality and perceived policy legitimacy
Shahab et al. (2021)	E-participation within the Iranian planning system	Qualitative interviews with Iranian public- and private-sector planning actors	Major barriers include institutional structure, administrative culture, attitudes toward public participation, trust, knowledge, staff capacity, infrastructure, leadership, and cost	Focuses on urban planning rather than national cyberspace governance and does not use a systemic boundary critique	Provides direct Iranian evidence that weak participation is rooted in institutional and cultural conditions, not merely technological limitations
Ansell et al. (2024)	Democratic implications of co-creation in public governance	Theoretical comparison of co-creation with established forms of democracy	Co-creation has democratic value when it empowers lay actors, facilitates cross-	Primarily normative and theoretical; does not specify how excluded	Supplies the democratic rationale for moving from one-way service provision

in press

Study	Context and research focus	Methodological design and data	Principal findings	Unresolved limitation or research gap	Relevance to the present study
			boundary collaboration, and enables shared influence over public-value outcomes	stakeholders can be identified and institutionally represented	toward shared problem definition and policy formation
Edelmann & Virkar (2023)	Sustainability of co-created digital public services in public administration	Qualitative expert workshop involving 30 participants, followed by grounded-theory-oriented coding	Sustainable co-creation requires continuity, stakeholder knowledge, institutional learning, resource integration, funding, technical capacity, and long-term commitment	Focuses on digital public-service development rather than contested national cyberspace policy and sovereignty	Shows that co-creation requires permanent institutional capacities rather than temporary consultation mechanisms
Pauluzzo et al. (2024)	Digital technologies, co-production, and co-creation in public administration	Structured literature review of 128 records published up to 2022	Digital technologies can reshape citizen–government relationships, but governance-oriented research, risk analysis, and whole-cycle co-creation remain underdeveloped	Does not provide a critical framework for examining power asymmetries, exclusion, or the legitimacy of governance boundaries	Justifies examining co-creation across the complete policy cycle, including problem definition, design, implementation, evaluation, and correction
Xin & Huang (2025)	Digital participatory policymaking and state–society relations in China	Longitudinal fieldwork and comparative analysis of pathways of disclosure, consultation, and deliberation	Digital participation can be institutionally enabled while remaining selectively channeled within state-managed boundaries	Does not systematically examine the normative justification of inclusion and exclusion or compare current and desirable governance boundaries	Offers a relevant comparison for analyzing participation within a state-centred governance system without assuming a simple control–participation binary
Hutcheson et al. (2024)	Applications and conceptual	Systematic review of 77 peer-reviewed articles	CSH is valuable for examining boundary	Existing applications are dispersed across	Provides the methodological basis

In Press

Study	Context and research focus	Methodological design and data	Principal findings	Unresolved limitation or research gap	Relevance to the present study
	development of Critical Systems Heuristics across multiple policy and organizational fields	selected from 111 Scopus records	critique, coercion, emancipation, and "is" versus "ought to be" judgments, but remains underused relative to other systems approaches	sectors, with limited application to cyberspace governance and digital-policy legitimacy	for examining beneficiaries, purposes, decision makers, expertise, affected groups, and competing worldviews
Goede & Goede (2025)	Critical Systems Heuristics and information-systems governance	Conceptual extension of CSH informed by critical realism and problems arising from poorly designed information systems	Formal system designs may generate workarounds and unintended governance consequences; analysis should consider realities and actors extending beyond formally designed boundaries	Focuses mainly on organizational information systems rather than national-level digital governance and public legitimacy	Strengthens the treatment of cyberspace as a socio-technical system whose formal rules may produce resistance, adaptation, and unintended outcomes
Present study	Iranian cyberspace-governance ecosystem, including state institutions, regulators, digital businesses, experts, citizens, and affected groups	Qualitative exploratory case study based on 26 expert interviews, policy documents, inductive coding, and mapping onto the twelve CSH boundary questions	Identifies discrepancies between current and desirable arrangements across motivation, control, knowledge, and legitimacy, and develops a model of co-created cyberspace governance	Addresses the absence of an integrated boundary critique connecting digital sovereignty, participation, co-creation, and legitimacy in Iran	Extends CSH into national cyberspace governance and converts the identified boundary gaps into context-sensitive governance reforms

in Press

As shown in Table 1, although previous research has separately examined digital sovereignty, e-participation, co-creation, policy legitimacy, and Critical Systems Heuristics, limited attention has been paid to integrating these perspectives within a unified boundary critique of cyberspace governance in Iran.

3. Methodology

This study employed a qualitative, exploratory case-study design to examine how boundary judgments shape digital participation and policy legitimacy within cyberspace governance in Iran, with Critical Systems Heuristics (CSH) serving as the principal analytical framework.

Data collection was conducted during 2025, a period in which cyberspace governance debates, regulatory developments, and digital policy challenges provided a relevant context for examining boundary judgments, participation, and policy legitimacy.

The empirical material comprised semi-structured expert interviews and publicly available policy, regulatory, and strategic documents concerning cyberspace governance, digital participation, e-government, platform regulation, digital business, cybersecurity, and public-sector digital transformation in Iran. The case was defined as the Iranian cyberspace governance ecosystem, understood as the institutional and socio-technical field in which state institutions, regulatory authorities, ICT organizations, digital businesses, experts, civil-society actors, and other affected social groups interact around digital policy formation, implementation, and evaluation.

A purposive expert-sampling strategy was adopted to ensure disciplinary, professional, and institutional diversity. The final sample comprised 26 experts, all of whom participated in the semi-structured interviews conducted for this study. As detailed in Table 2, the sample included five public policy and cyberspace governance experts, five ICT and e-government managers, four cyberlaw and regulatory experts, four digital economy and platform actors, five academic researchers, and three civil-society, media, and digital-participation observers. The final sample size was determined based on data saturation. Interviews continued until additional interviews did not generate substantially new themes, boundary judgments, or analytical insights relevant to the CSH framework.

Participants were selected according to three criteria: direct professional experience relevant to cyberspace governance, demonstrable expertise in digital policy, regulation, technology, digital economy, or participation, and representation of diverse perspectives from the public, private, academic, legal, technical, and civil-society domains. This diversity enabled the study to incorporate policy, managerial, technical, legal, economic, academic, and experiential forms of knowledge and to avoid examining cyberspace governance exclusively from an institutional or technical perspective.

IHU Press

Table 2. Detailed composition, expertise, and analytical contribution of the expert interview sample

Expert group	Number	Institutional or professional domain	Relevant expertise and experience	Basis for inclusion in the sample	Principal contribution to the study	Main interview focus	Main CSH dimensions informed
Public policy and cyberspace governance experts	5	Public policy institutions, strategic policymaking, governance advisory, and cyberspace policy analysis	Experience in policy formulation, institutional design, strategic planning, inter-organizational coordination, and national cyberspace governance	Direct professional involvement in cyberspace policymaking or demonstrable expertise in institutional governance and digital policy	Clarified the formal purposes of cyberspace governance, the structure of decision authority, institutional priorities, coordination problems, and desirable governance reforms	Policy purposes; institutional authority; distribution of decision-making power; policy coordination; sovereignty; security; accountability	Motivation and Control
ICT and e-government managers	5	Public-sector ICT management, e-government, digital transformation, infrastructure, and electronic service delivery	Practical experience in digital infrastructure, public platforms, information systems, service delivery, data management, implementation constraints, and technical capacity	Direct managerial or implementation experience in ICT, e-government, digital platforms, or public-sector digital transformation	Explained how policies are implemented in practice, which technological and organizational resources are controlled, and what infrastructural or operational constraints affect	Infrastructure; digital services; platform management; implementation capacity; data governance; technical standards; institutional resources	Control and Knowledge

inPress

Expert group	Number	Institutional or professional domain	Relevant expertise and experience	Basis for inclusion in the sample	Principal contribution to the study	Main interview focus	Main CSH dimensions informed
					governance outcomes		
Cyberlaw and regulatory experts	4	Cyberlaw, digital regulation, platform governance, legal compliance, and digital rights	Expertise in regulatory authority, cybercrime, platform responsibilities, legal mandates, compliance mechanisms, data-related rules, rights, and legal accountability	Specialized knowledge of the legal and regulatory dimensions of cyberspace governance	Identified legal boundaries of authority, tensions between regulation and rights, weaknesses in accountability, and the legal position of affected stakeholders	Regulatory authority; legal legitimacy; platform regulation; rights and responsibilities; compliance; appeal and review mechanisms	Control and Legitimacy
Digital economy and platform actors	4	Private digital businesses, online platforms, startups, entrepreneurship, and the digital economy	Practical experience with platform regulation, online markets, business uncertainty, restrictions, innovation, technological dependence, and sanctions-related constraints	Direct experience of the economic and operational consequences of cyberspace policies	Provided evidence about how regulatory instability, access restrictions, platform policies, and governance decisions affect innovation, investment, business continuity, and	Regulatory predictability; digital business constraints; innovation; market access; platform stability; sanctions; economic consequences of policy	Motivation, Control, and Legitimacy

in press

Expert group	Number	Institutional or professional domain	Relevant expertise and experience	Basis for inclusion in the sample	Principal contribution to the study	Main interview focus	Main CSH dimensions informed
Academic researchers	5	Universities and research institutions in public administration, cyberspace studies, information systems, law, governance, and participation	Research-based knowledge of digital governance, public policy, social consequences of technology, participation, institutional legitimacy, and systems thinking	Demonstrable research expertise relevant to cyberspace governance, participation, public administration, or digital policy	user relations Contributed interdisciplinary, theoretically informed, and comparatively independent interpretations of governance problems and possible reforms	Valid knowledge; policy evidence; social impact; public trust; participation; comparative governance; evaluation criteria; unintended consequences	Knowledge and Legitimacy
Civil society, media, and participation observers	3	Civil society, media, public communication, digital participation, and observation of citizen–state relations	Experience in monitoring public concerns, communication processes, citizen participation, digital exclusion, stakeholder representation, and public trust	Ability to represent or observe perspectives that are less institutionally powerful and more weakly represented in formal policymaking	Highlighted the experiences of citizens and affected but weakly involved groups, limitations of existing participation channels, trust problems, and representation gaps	Citizen voice; access; public trust; exclusion; vulnerable groups; consultation mechanisms; feedback; representation; accountability	Legitimacy and Motivation

In Press

The interviews lasted approximately 40-60 min and focused on participants' experiences and assessments of current governance arrangements, institutional authority, participation mechanisms, stakeholder inclusion, digital rights and responsibilities, policy legitimacy, implementation constraints, and desirable reform pathways. All interviews were conducted in Persian, which was the preferred language of the participants. The interviews were transcribed in the original language and translated into English for analytical presentation. To maintain conceptual accuracy, the translated materials were reviewed against the original transcripts during the analysis process.

The interview guide covered six main domains: institutional authority and decision-making processes; existing participation mechanisms; inclusion and representation of affected stakeholders; digital rights and responsibilities; criteria of policy legitimacy; and desirable governance reforms. These domains were designed to generate evidence relevant to the four CSH dimensions of motivation, control, knowledge, and legitimacy and to support comparison between existing "is" conditions and desirable "ought to be" arrangements.

In addition to expert interviews, documentary materials were analyzed to contextualize cyberspace governance arrangements. The documentary corpus consisted of official policy documents, regulatory frameworks, strategic plans, and institutional reports related to cyberspace governance, digital participation, e-government, platform regulation, cybersecurity, and digital transformation in Iran. Documents were selected based on three criteria: (1) direct relevance to cyberspace governance and digital policy issues; (2) official status and institutional significance; and (3) their capacity to reveal assumptions regarding authority, knowledge, participation, and legitimacy.

3.1. Ethical considerations

Ethical considerations were carefully addressed due to the sensitive nature of cyberspace governance research and the involvement of human participants. Participation was voluntary, and participants were informed about the purpose of the study before the interviews. Participants provided consent to participate, and their identities were anonymized to protect confidentiality. No personally identifiable information was reported in the findings, and the collected data were used exclusively for academic research purposes.

Data familiarization began with repeated and systematic reading of the interview transcripts and relevant policy, regulatory, and strategic documents. At this stage, the purpose was to develop a comprehensive understanding of the language, assumptions, and institutional perspectives through which cyberspace governance was described, rather than to impose predetermined analytical categories on the data. Particular attention was paid to recurring references to institutional

In Press

control, regulatory restriction, citizen participation, public trust, national security, digital sovereignty, accountability, recognized expertise, institutional fragmentation, regulatory uncertainty affecting digital businesses, and citizens' limited influence over policy decisions. Analytical memos were prepared during and after the review of each transcript and document to record emerging patterns, contradictions, institutional tensions, stakeholder positions, and potential boundary judgments. The coding process was conducted manually using a structured qualitative coding framework aligned with Critical Systems Heuristics. The analysis involved identifying statements related to purpose, beneficiaries, authority, resources, knowledge claims, stakeholder participation, and legitimacy concerns. These codes were subsequently organized according to the twelve CSH boundary questions.

The first cycle of coding followed an inductive and data-driven thematic approach. Interview transcripts and documentary materials were examined line by line, and statements were coded when they referred to policy purposes, beneficiaries, actors, interests, institutional resources, decision-making authority, constraints, knowledge claims, affected stakeholders, legitimacy concerns, or proposed governance reforms. At this stage, the codes were kept close to the language and meaning of the empirical material in order to minimize premature theoretical abstraction. Examples of the initial codes included "centralized policy authority", "citizens treated as service users rather than policy participants", "priority of security over participation", "limited institutional feedback loops", "regulatory uncertainty for digital businesses", "weak public consultation", and "need for accountable platform governance".

During the first-cycle analysis, the codes were also classified according to whether they described existing governance arrangements or expressed desirable alternatives. Statements concerning current institutional practices, power relations, participation mechanisms, and policy consequences were categorized as "is" judgments, whereas statements proposing more inclusive, accountable, or participatory governance arrangements were categorized as "ought to be" judgments. For example, the statement that "citizens are mainly treated as users of digital services rather than as co-designers of cyberspace policy" was coded as an "is" judgment. In contrast, the proposition that "citizens and affected stakeholder groups should participate in policy design, implementation review, evaluation, and accountability mechanisms" was categorized as an "ought to be" judgment.

3.2. Trustworthiness of the study

The trustworthiness of the qualitative analysis was addressed through credibility, dependability, and confirmability procedures. Credibility was enhanced through triangulation between expert interviews and

In Press

documentary materials, as well as through systematic comparison of different stakeholder perspectives. Dependability was supported by maintaining a transparent analytical process, documenting coding decisions, and applying the same CSH framework consistently across the empirical materials. Confirmability was strengthened by linking interpretations to interview evidence and documentary sources rather than relying solely on researcher assumptions.

4. Research findings

This distinction operationalized the central CSH comparison between existing and normatively desirable system arrangements. It also provided the analytical foundation for the subsequent mapping of the empirical codes onto the twelve CSH boundary questions and their aggregation within the four dimensions of motivation, control, knowledge, and legitimacy, as summarized in Table 3.

As shown in Table 3, the four CSH dimensions were analytically interconnected. A narrow definition of system purpose influenced which actors were recognized as beneficiaries; concentrated control affected which stakeholders could participate; dominant forms of technical and regulatory expertise shaped what counted as valid knowledge; and weak representation limited the ability of affected groups to question or revise existing governance boundaries. The comparison between the "is" and "ought to be" conditions therefore revealed not twelve isolated problems, but a mutually reinforcing pattern of institutional control, restricted knowledge inclusion, and limited participatory legitimacy.

4.1. Responses to boundary questions

Boundary question 1. What is the purpose of cyberspace governance, and what ought it to be?

In Critical Systems Heuristics (CSH), system purpose is a boundary judgment because it defines which objectives are treated as legitimate and which concerns are pushed outside the policy agenda. In Iranian cyberspace governance, this boundary determines whether digital policy is framed mainly around control, security, sovereignty, and service delivery, or around broader public purposes such as participation, trust, innovation, accountability, and social inclusion.

a) "What is"

Interview-based coding showed that the current purpose of cyberspace governance was primarily framed through four logics: national security, digital sovereignty, infrastructural control, and cultural regulation.

In Press

Table 3. Mapping of interview evidence onto the twelve CSH boundary questions

CSH boundary question	Current "is" condition	Illustrative participant quotation	Analytical interpretation	Desired "ought to be" condition
1. Who ought to be the beneficiaries of cyberspace governance?	The current governance approach mainly defines beneficiaries through institutional priorities, national interests, security objectives, and regulatory stability. Citizens are often positioned as users rather than active beneficiaries and co-creators.	"In many digital policies, the main focus is on protecting the system and managing risks. The everyday needs and expectations of citizens are usually considered after institutional priorities are defined." (P4, policy expert)	The boundary of beneficiaries is narrowly defined around institutional objectives, limiting the recognition of broader public value.	Beneficiaries should include citizens, digital communities, businesses, researchers, and all groups affected by cyberspace decisions.
2. What is the purpose of cyberspace governance?	Governance purposes are primarily associated with security, sovereignty, infrastructure protection, regulation, and institutional control.	"Security is an essential concern in cyberspace governance, but governance cannot be sustainable if it only focuses on control and does not consider trust, participation, and innovation." (P7, governance expert)	The current purpose boundary prioritizes protection and control while giving less attention to social value creation.	The purpose of governance should balance security and sovereignty with public trust, innovation, participation, and inclusion.
3. What measures should be used to evaluate improvement?	Improvement is mainly assessed through regulatory compliance, security performance, infrastructure development, and institutional effectiveness.	"A policy may achieve its regulatory objectives, but this does not necessarily mean that people accept it or feel that their concerns have been considered." (P12, academic expert)	Evaluation criteria emphasize institutional outcomes rather than legitimacy and stakeholder experience.	Improvement should include security, effectiveness, transparency, user satisfaction, trust, and legitimacy.
4. Who ought to be the decision makers?	Decision-making authority is concentrated among governmental institutions, regulatory bodies, and formal technical organizations.	"Most stakeholders are invited when the main framework is already determined. Their role is usually to provide comments rather than participate in defining the	Decision-making boundaries limit meaningful participation and reinforce centralized authority.	Decision-making should involve government, private sector, academia, civil society, and users through participatory mechanisms.

in Press

CSH boundary question	Current "is" condition	Illustrative participant quotation	Analytical interpretation	Desired "ought to be" condition
		direction of policy." (P15, digital policy expert)		
5. Who controls the resources required for governance?	Critical resources, including infrastructure, regulatory authority, and implementation mechanisms, are controlled mainly by formal institutions.	"Those who control infrastructure and regulatory tools naturally have more influence over cyberspace decisions compared with other actors." (P9, ICT expert)	Control boundaries shape unequal influence among stakeholders.	Resource control should be accompanied by transparency, accountability, and collaborative governance arrangements.
6. What expertise is considered legitimate?	Technical and institutional expertise dominates cyberspace governance, while social and experiential knowledge has limited influence.	"Technical expertise is necessary, but technology alone cannot explain how people experience digital policies in society." (P18, researcher)	The knowledge boundary privileges technical knowledge over socio-technical perspectives.	Legitimate knowledge should integrate technical, social, cultural, economic, and experiential forms of knowledge.
7. Who generates and validates knowledge?	Knowledge production is mainly conducted by governmental agencies, technical experts, and formal organizations.	"Users experience the consequences of digital policies every day, but their experiences are rarely considered as a source of policy knowledge." (P6, civil society participant)	Knowledge generation remains institution-centered and limits participatory learning.	Knowledge production should include citizens, users, researchers, businesses, and affected communities.
8. What knowledge perspectives are excluded?	Informal knowledge, user experiences, social impacts, and community perspectives are often marginalized compared with formal technical knowledge.	"Many practical problems become visible only when people use digital services, but these experiences are not always included in policy discussions." (P20, digital service expert)	Excluded knowledge creates gaps between policy assumptions and real-world experiences.	Governance should recognize multiple knowledge sources and challenge dominant assumptions.
9. Who ought to participate in cyberspace governance?	Participation is mainly indirect and consultative. Stakeholders often have limited influence over agenda-setting and policy	"Participation should not begin after decisions are made. Stakeholders need opportunities to contribute when problems and	Existing participation mechanisms provide limited opportunities for co-creation.	Stakeholders should participate throughout problem definition, policymaking, implementation, and

In Press

CSH boundary question	Current "is" condition	Illustrative participant quotation	Analytical interpretation	Desired "ought to be" condition
	design.	priorities are being defined." (P11, governance researcher)		evaluation.
10. What values should guide cyberspace governance?	Governance values are mainly shaped by security, sovereignty, order, and institutional responsibility.	"Security is important, but legitimacy also depends on whether people understand decisions, trust institutions, and feel represented." (P3, policy analyst)	The value boundary requires expansion from control-oriented values toward legitimacy-oriented values.	Governance values should combine security with transparency, accountability, trust, inclusion, and responsiveness.
11. Who represents affected stakeholders?	Representation is primarily indirect through formal institutions. Many affected groups lack direct channels for influencing governance.	"Citizens are affected by cyberspace decisions, but they often do not have effective mechanisms to express their concerns before policies are implemented." (P14, academic expert)	Indirect representation creates legitimacy gaps between decision makers and affected communities.	Representation should move toward substantive participation and stakeholder inclusion.
12. How can cyberspace governance decisions achieve legitimacy?	Legitimacy is mainly derived from institutional authority, legal procedures, and administrative justification.	"People are more likely to accept digital policies when they understand the reasons behind them and have some opportunity to contribute." (P22, digital governance expert)	Legitimacy requires more than formal authority; it depends on participation, transparency, and trust.	Policy legitimacy should be achieved through accountable institutions, meaningful participation, transparency, and co-created governance.

in press

Cyberspace is treated as a strategic domain that must be protected from external threats, foreign platform dependency, harmful content, cybercrime, and uncontrolled information flows. E-government and digital service delivery are also emphasized, but participation is mostly understood as access to services rather than involvement in policymaking. Thus, current success is largely narrated as maintaining control over digital infrastructures, expanding domestic platforms, improving cyber security, regulating online behavior, and ensuring institutional compliance.

b) "What ought to be"

Interviewees argued that security and sovereignty should remain important but should be embedded in a broader public governance purpose. Four desirable purposes emerge: legitimate digital participation, public trust, inclusive digital development, and accountable cyberspace governance. In this view, cyberspace governance should protect national interests while also enabling citizens, businesses, educators, researchers, vulnerable groups, and future generations to benefit from digital transformation. The purpose should shift from governing cyberspace mainly as a domain of control to governing it as a shared public infrastructure for security, innovation, participation, cultural development, and social trust.

Boundary question 2. Who is the intended beneficiary of cyberspace governance, and who ought to be?

In CSH, identifying the beneficiary reveals whose improvement the system is designed to serve. This is a critical question because governance systems may claim to serve society while practically prioritizing institutional, regulatory, or security interests.

a) "What is"

The current beneficiary boundary appears to privilege formal state institutions, regulatory bodies, security actors, infrastructure authorities, and domestic platform policy agendas. Citizens are recognized as users of services and subjects of regulation, but not always as co-creators of cyberspace policy. Digital businesses benefit when policies support domestic platforms, but they may also experience uncertainty, restrictions, and unstable access conditions. Ordinary users, students, women, small online businesses, content creators, civil society actors, and rural or marginalized groups often remain secondary beneficiaries rather than central stakeholders.

b) "What ought to be"

The beneficiary boundary should be widened. Cyberspace governance ought to serve not only institutional security and sovereignty but also citizens' digital capabilities, public service quality, entrepreneurial

In Press

activity, academic access, social communication, digital rights, and future technological resilience. Beneficiaries should include state institutions, but also ordinary users, students, educators, researchers, startups, online businesses, content producers, vulnerable communities, and future generations. This broader beneficiary boundary is essential for policy legitimacy because those who bear the consequences of digital policies should also be recognized as legitimate recipients of governance value.

Boundary question 3. What counts as improvement in cyberspace governance, and what ought to count as improvement?

In CSH, improvement is not neutral. It depends on the values and criteria used to judge whether the system is working well. In cyberspace governance, improvement may be defined narrowly as control and compliance or more broadly as legitimacy, trust, participation, and resilience.

a) "What is"

Current improvement is often understood in instrumental and institutional terms: stronger cyber security, more domestic infrastructure, expanded e-government services, greater platform regulation, higher compliance, better monitoring capacity, and reduced exposure to external digital threats. Such criteria are important, but they tend to privilege measurable institutional outputs over lived user experience, public trust, civic participation, and accountability. As a result, policy success may be claimed even when affected stakeholders experience reduced agency, limited consultation, or uncertainty in digital life and digital business.

b) "What ought to be"

Improvement should be defined through a multidimensional public value lens. It should include secure infrastructure, but also meaningful participation, transparent policymaking, predictable regulation, user trust, digital inclusion, innovation capacity, accessibility, accountability, and responsiveness to affected groups. A legitimate cyberspace governance system should not be evaluated only by whether it controls risks, but also by whether it enables society to participate safely, productively, and fairly in digital life.

Boundary question 4. Who makes the decisions in cyberspace governance, and who ought to make them?

In CSH, decision makers are those who control the system's direction and define its practical boundaries. This question is central to co-creation because participation is impossible if decision authority remains entirely closed.

ID Press

a) "What is"

Decision making in Iranian cyberspace governance is largely concentrated among formal state institutions, high-level cyberspace policymaking bodies, regulatory authorities, security organizations, legal institutions, and technical infrastructure actors. These actors define policy priorities, platform rules, access conditions, enforcement mechanisms, and digital transformation strategies. Non-state actors may be consulted occasionally, but their influence over agenda setting, policy design, implementation, and evaluation appears limited. Citizens and affected groups are more often positioned as recipients of decisions rather than participants in decision formation.

b) "What ought to be"

Decision making should become more structured, consultative, and co-created without eliminating the legitimate role of the state. A desirable model would include formal channels for universities, digital businesses, civil society organizations, professional associations, educators, youth representatives, user communities, and vulnerable groups. The state would remain a central guarantor of security and public order, but policy design would become more open to plural knowledge, public consultation, and stakeholder review. Co-creation here means shared influence over defined parts of the policy cycle, not uncontrolled fragmentation of authority.

Boundary question 5. What resources and conditions are controlled by decision makers, and what ought to be controlled or shared?

CSH treats resources as part of the control boundary because those who control key conditions shape what the system can become. In cyberspace governance, resources include infrastructure, data, platforms, legal authority, technical standards, and participation channels.

a) "What is"

Current decision makers control major governance conditions: internet infrastructure, licensing, regulatory enforcement, platform access, cyber security standards, filtering mechanisms, data governance rules, digital identity systems, and e-government platforms. These resources give formal actors significant influence over public communication, digital business activity, service delivery, and access to global information flows. However, participation mechanisms, public feedback systems, impact assessments, and transparency tools are less developed as shared governance resources.

b) "What ought to be"

Critical resources should remain secure, but their governance should become more transparent, accountable, and participatory. Certain

IN Press

resources such as policy consultation platforms, public data dashboards, regulatory impact assessments, digital rights review mechanisms, and complaint systems should be opened to wider stakeholder participation. Data, infrastructure, and platform governance should be supported by clear rules, independent evaluation, and feedback loops. The aim is not to weaken control over sensitive infrastructure but to ensure that control is exercised with public justification and stakeholder accountability.

Boundary question 6. What conditions are outside the control of decision makers, and how ought these constraints to be handled?

In CSH, no system is fully self-contained. The environment includes external constraints and uncertainties that decision makers cannot completely control. Recognizing these limits prevents unrealistic governance designs.

a) "What is"

Iranian cyberspace governance operates under significant external and internal constraints: international sanctions, dependency on foreign technologies, global platform dominance, cyber threats, geopolitical conflict, rapid technological change, VPN use, user resistance, digital business adaptation, and shifting public expectations. These factors limit the effectiveness of purely command-based governance. Even when formal actors attempt to regulate digital flows, users and businesses often develop informal workarounds, which may reduce transparency and weaken trust.

b) "What ought to be"

Governance should become more adaptive and learning oriented. Instead of seeking total control over a highly dynamic digital environment, cyberspace policy should build resilience, trust, institutional learning, and flexible regulation. External constraints should be addressed through domestic capacity building, digital literacy, transparent risk communication, regulatory predictability, and adaptive consultation with affected stakeholders. A realistic "ought" model recognizes that legitimacy and cooperation may produce more sustainable governance than rigid control alone.

Boundary question 7. Who is considered an expert, and who ought to be considered an expert?

In CSH, expertise is a boundary judgment because it determines whose knowledge is authorized to shape policy. Cyberspace governance requires technical knowledge, but technical expertise alone cannot capture social consequences.

In Press

a) "What is"
Recognized expertise is mainly concentrated among technical specialists, cyber security professionals, legal authorities, ICT managers, regulatory officials, and administrative decision makers. These forms of expertise are necessary for infrastructure security, cybercrime prevention, legal compliance, and platform regulation. However, social scientists, public administration scholars, digital rights specialists, educators, user communities, entrepreneurs, women's groups, rural communities, and vulnerable users may be less visible in formal expertise structures.

b) "What ought to be"
Expertise should be pluralized. A legitimate cyberspace governance system should integrate technical, legal, administrative, economic, social, cultural, ethical, and experiential knowledge. Users' lived experiences, entrepreneurs' operational knowledge, educators' academic needs, civil society's rights-based concerns, and researchers' evidence-based analysis should all inform policy. This does not undermine technical expertise; it completes it. Cyberspace is a socio-technical system, so its governance requires socio-technical expertise.

Boundary question 8. What kind of knowledge is considered relevant, and what knowledge ought to be considered relevant?
This CSH question moves from who the experts are to what kinds of knowledge count as valid. In digital governance, the knowledge boundary can determine whether policy is designed around enforcement or around broader public consequences.

a) "What is"
Current relevant knowledge appears to emphasize cyber security, legal regulation, infrastructure management, platform control, public order, technical standards, and compliance requirements. Evidence about user trust, economic disruption, digital exclusion, gendered consequences, youth experience, academic access, business uncertainty, and public legitimacy may be less systematically incorporated into decision making. As a result, policy may become technically rational but socially incomplete.

b) "What ought to be"
Relevant knowledge should include social impact assessment, user experience, digital inclusion data, public trust indicators, economic effects on startups and online businesses, educational consequences, accessibility requirements, rights-based analysis, and evidence from affected communities. Policy knowledge should be generated through mixed sources: expert analysis, stakeholder consultation, public feedback, academic research, and evaluation of implemented policies.

UT Press

Cyberspace Studies, Vol ?, No ?, ????

This wider knowledge boundary would help prevent unintended consequences and improve policy legitimacy.

Boundary question 9. What guarantees successful cyberspace governance, and what ought to guarantee it?

In CSH, the "guarantor" refers to what gives confidence that the system will achieve its purpose. In many governance systems, success is assumed to follow from authority, technical capacity, or compliance. CSH asks whether these guarantees are sufficient.

a) "What is"

The data associate current guarantees of success with institutional authority, legal enforcement, technical infrastructure, cybersecurity capacity, regulatory compliance and formal coordination among responsible bodies. These mechanisms are important, but they do not automatically guarantee legitimacy, trust, or effective participation. A policy can be implemented and enforced while still being contested, bypassed, or distrusted by affected groups.

b) "What ought to be"

Successful cyberspace governance should be guaranteed by a broader set of mechanisms: transparent policymaking, evidence-based regulation, independent evaluation, public consultation, stakeholder feedback, periodic policy review, accountability mechanisms, and measurable indicators of trust and inclusion. Compliance should be complemented by learning. Enforcement should be complemented by responsiveness. Technical capacity should be complemented by legitimacy. These combined guarantees would make governance more durable and publicly justifiable.

Boundary question 10. Who represents those affected but not involved, and who ought to represent them?

This is one of the most important CSH questions for the present study. It addresses the legitimacy problem of affected groups who experience policy consequences but lack direct influence over policy design.

a) "What is"

Affected but weakly involved groups include ordinary internet users, students, online sellers, startups, content creators, educators, researchers, women, rural communities, persons with disabilities, civil society actors, and future generations. Their interests are often represented indirectly through formal institutions or broad public interest claims. However, indirect representation may not capture the specific effects of restrictions, regulatory uncertainty, weak access, platform instability, or limited participation mechanisms.

in press

b) "What ought to be"

These groups should be represented through institutionalized mechanisms: stakeholder councils, public consultation procedures, digital participation platforms, civil society channels, academic advisory panels, business associations, youth and student forums, accessibility representatives, and independent review bodies. Representation should not be symbolic. It should allow affected groups to influence problem definition, risk assessment, policy design, implementation review, and reform proposals. This is essential for transforming cyberspace governance from top-down administration into co-created public governance.

Boundary question 11. What opportunities exist for emancipation, and what ought to exist?

In CSH, emancipation means giving affected actors the opportunity to question, challenge, and revise boundary judgments. It does not merely mean receiving services or submitting complaints.

a) "What is"

Current opportunities for emancipation appear limited when participation is reduced to service use, complaint registration, or post-decision feedback. Citizens may interact with e-government systems, but this does not necessarily mean they can influence cyberspace policy. Digital businesses may comply with regulations but may not meaningfully shape regulatory design. Civil society and expert communities may comment on policies but may lack stable institutional channels to affect decisions.

b) "What ought to be"

Emancipatory opportunities should include agenda-setting participation, pre-policy consultation, deliberative forums, transparent appeal mechanisms, participatory impact assessment, public reporting of consultation outcomes, and periodic boundary review. Affected groups should be able to ask: Why is this policy necessary? Who benefits from it? What alternatives were considered? What harms may result? How will unintended consequences be corrected? In this sense, emancipation means enabling stakeholders to participate in defining the boundaries of legitimate cyberspace governance.

Boundary question 12. How are competing worldviews reconciled, and how ought they to be reconciled?

In CSH, worldviews shape how actors interpret the same system differently. Cyberspace governance is especially worldview-dependent because it involves security, freedom, sovereignty, culture, economy, innovation, and rights.

In Press

a) "What is"

Competing worldviews in Iranian cyberspace governance include security-centered, sovereignty-centered, cultural-protection, economic-development, innovation-oriented, rights-based, user-centered, and global-connectivity perspectives. At present, security, sovereignty, and regulatory worldviews appear to hold stronger institutional authority. Other perspectives particularly those emphasizing user experience, digital entrepreneurship, open knowledge access, and participatory legitimacy may be present but less influential in final policy decisions.

b) "What ought to be"

Competing worldviews should be reconciled through structured boundary dialogue, transparent trade-off analysis, multi-stakeholder policy forums, and public justification of decisions. The aim is not to eliminate conflict, because cyberspace governance will always involve value tensions. Rather, the aim is to make these tensions visible, discussable, and accountable. A legitimate model should allow security, sovereignty, cultural concerns, innovation, digital rights, and public participation to be negotiated through explicit governance procedures rather than being resolved implicitly by the most powerful actors.

4.2. Boundary of motivation: From institutional control to public value

The first major finding concerns the purpose and beneficiary structure of cyberspace governance in Iran. The analysis indicates that the current "is" situation is largely shaped by a security, sovereignty, and control-oriented logic. Cyberspace is primarily framed as a strategic domain requiring protection, regulation, infrastructural autonomy, cultural oversight, and institutional coordination. Within this boundary, the main beneficiaries are formal governing institutions, regulatory authorities, security actors, infrastructure providers, and domestic platform policy agendas. However, the "ought to be" situation emerging from the CSH analysis requires a wider public value orientation. Cyberspace governance should not only protect national security and digital sovereignty but also serve citizens, digital businesses, students, researchers, educators, vulnerable users, content creators, and future generations. The key boundary gap is therefore between institutional benefit and societal benefit. Current policy purposes appear narrower than the range of actors affected by cyberspace governance.

4.3. Boundary of control: Concentrated authority and limited co-creation

The second finding concerns decision authority. The current governance structure is characterized by concentrated control among formal policymaking institutions, regulators, legal authorities, security bodies, and technical infrastructure actors. These actors control major governance conditions, including platform access, licensing, filtering, cyber security standards, digital infrastructure, data governance rules,

In Press

and regulatory enforcement. The desired situation points toward a more structured co-creation model. This does not imply weakening the state's legitimate role in security, public order, or infrastructure protection. Rather, it suggests that selected stages of the policy cycle problem definition, consultation, design, implementation review, and evaluation should include universities, digital entrepreneurs, civil society actors, professional associations, user groups, educators, youth representatives, and vulnerable communities. The central gap is between closed authority and participatory authority.

4.4. Boundary of knowledge: Dominance of technical and security expertise

The third finding concerns the knowledge base of cyberspace governance. Current governance appears to privilege technical, legal, administrative, security, and infrastructural expertise. These forms of knowledge are necessary but incomplete. They are well suited to addressing cyber threats, infrastructure protection, compliance, and platform regulation, but they are less able to capture the social, economic, ethical, cultural, and lived consequences of digital policy.

The "ought to be" boundary requires plural knowledge. Cyberspace governance should include user experience, digital business evidence, public administration knowledge, social impact analysis, digital rights expertise, accessibility concerns, gender-sensitive perspectives, youth experience, academic access, and civil society knowledge. The key finding is that legitimacy requires not only better technical decisions but better knowledge inclusion.

4.5. Legitimacy: Participation, representation, and policy acceptance

The legitimacy dimension revealed that cyberspace governance challenges are not limited to institutional capacity or regulatory effectiveness; they also concern whether affected stakeholders perceive governance processes as fair, transparent, and inclusive. Interview evidence indicated that existing arrangements rely predominantly on institutional authority and indirect representation, while citizens, digital communities, and other affected groups have limited opportunities to influence policy formulation and evaluation.

5. Discussion and conclusion

This study examined Iranian cyberspace governance through the twelve boundary questions of Critical Systems Heuristics (CSH), comparing existing "is" conditions with desirable "ought to be" arrangements. The findings show that the main challenge of cyberspace governance is not merely technological, regulatory, or administrative. It is fundamentally related to the boundaries through which governance purposes, beneficiaries, decision makers, resources, expertise, and legitimacy are defined.

IKI Press

Cyberspace Studies, Vol ?, No ?, ????

Across the four CSH dimensions, an interconnected pattern emerged. In the motivation dimension, cyberspace governance was primarily framed around national security, digital sovereignty, infrastructural control, cultural regulation, and institutional compliance. In the control dimension, decision-making authority and strategic resources were concentrated among formal policymaking, regulatory, legal, security, and technical institutions. In the knowledge dimension, technical, legal, administrative, and cybersecurity expertise received greater recognition than social, economic, ethical, participatory, and experiential knowledge. In the legitimacy dimension, citizens, digital businesses, researchers, educators, civil-society actors, vulnerable groups, and other affected stakeholders were more often positioned as users, regulated subjects, or indirect beneficiaries than as meaningful participants in policy formation and evaluation.

These four dimensions reinforce one another. A narrow definition of system purpose affects who is recognized as a legitimate beneficiary; concentrated authority determines who can influence policy decisions; dominant forms of expertise shape what counts as relevant knowledge; and weak representation limits the ability of affected groups to question or revise existing governance boundaries. The legitimacy deficit identified in this study should therefore not be attributed to a single institutional weakness, but to the combined effects of restricted participation, concentrated decision-making, limited knowledge diversity, and indirect stakeholder representation.

These findings support the argument that cyberspace governance is a form of boundary politics involving competing claims over authority, sovereignty, expertise, inclusion, and accountability (Hofmann & Pawlak, 2023). They are also consistent with studies showing that digital sovereignty is not a politically neutral or internally coherent concept and may be interpreted in ways that emphasize either public autonomy and resilience or centralized institutional control (Fratini et al., 2024; Pohle & Santaniello, 2024). The present study extends this discussion by showing that the legitimacy of sovereignty depends on how governance boundaries are constructed and justified.

In the Iranian context, concerns relating to national security, cultural protection, international sanctions, technological dependency, foreign platforms, and cybersecurity threats are genuine and cannot be ignored. The findings therefore do not imply that the state should abandon its responsibility for security, regulation, and critical infrastructure. Rather, they suggest that the exercise of this authority should be more transparent, accountable, participatory, and informed by plural forms of knowledge. Sovereignty and participation should not be treated as mutually exclusive. Participation can strengthen sovereignty by increasing public trust, cooperation, policy responsiveness, institutional learning, and the ability to identify unintended consequences. By contrast, governance based predominantly on control may encourage

Under Review

distrust, informal workarounds, regulatory avoidance, and uncertainty among users and digital businesses.

The findings also highlight the need to distinguish between e-government, digital participation, and co-created cyberspace governance. E-government mainly concerns digital service delivery and administrative efficiency, while digital participation may allow citizens to submit information, register complaints, or provide feedback. Co-created governance goes further by involving stakeholders in defining problems, assessing risks, comparing policy alternatives, evaluating implementation, and revising existing arrangements. The existence of digital tools alone does not guarantee meaningful participation. As Shin et al. (2024) observe, many digital participation tools facilitate the transfer of information from citizens to government but provide limited evidence regarding how this input affects decisions. Similarly, the present findings indicate that interaction with digital services should not be confused with influence over policy.

Co-created governance should not be interpreted as unrestricted public decision-making or the weakening of formal authority. It refers to structured and differentiated stakeholder involvement in appropriate stages of the policy cycle. Security-sensitive matters may require specific institutional safeguards, but policies affecting digital access, online businesses, education, platform regulation, accessibility, user rights, and public services can still include systematic consultation, impact assessment, stakeholder review, and transparent explanation of policy choices.

The study contributes theoretically in three ways. First, it conceptualizes cyberspace governance as a boundary system in which cybersecurity, digital sovereignty, participation, platform regulation, and public-sector digital transformation are connected through judgments about purpose, authority, knowledge, and representation.
Second, it links digital participation to policy legitimacy by showing that participation should be evaluated not only through platform availability or citizen input, but through the actual capacity of stakeholders to influence problem definition, policy design, evaluation, and accountability.

Third, it extends CSH into national cyberspace governance and demonstrates how the distinction between “is” and “ought to be” conditions can connect normative critique with institutional reform.

The findings also have practical implications. Major cyberspace policies should be accompanied by participatory impact assessments examining their effects on citizens, businesses, education, research, accessibility, digital inclusion, innovation, and public trust. Stakeholder consultation should become an institutionalized part of the policy process rather than an occasional or symbolic activity. Public institutions should also explain which groups were consulted, how their input was considered, and why particular recommendations were

JM Press

accepted or rejected. Technical and security expertise should be complemented by social, economic, ethical, and experiential knowledge. In addition, independent or semi-independent mechanisms should periodically evaluate policy outcomes and unintended consequences. Public dashboards, consultation reports, stakeholder councils, academic panels, business associations, and civil-society channels could strengthen transparency, representation, and accountability without requiring the disclosure of security-sensitive information.

This study has several limitations. Its findings are based on expert interviews and publicly available policy, regulatory, and strategic documents. Although the sample included participants from public, private, academic, technical, legal, business, and civil-society domains, it cannot fully represent all citizens and affected communities. Groups such as ordinary users, students, rural communities, persons with disabilities, small online sellers, and other vulnerable stakeholders were mainly represented through expert interpretations rather than direct participation. Moreover, the qualitative case-study design was intended to provide contextual and analytical depth rather than statistical generalizability. Publicly available documents may also fail to reveal informal decision-making processes, internal institutional disagreements, or non-public security considerations. Future research should therefore include direct interviews with affected groups, participatory workshops, comparative international studies, and quantitative examination of the relationships among participation, trust, regulatory predictability, and policy legitimacy.

In conclusion, the central challenge of cyberspace governance in Iran lies in how governance boundaries are defined, justified, and potentially reconstructed. The application of Critical Systems Heuristics revealed that existing governance arrangements are primarily shaped by security, sovereignty, infrastructure, regulation, and technical expertise, while affected stakeholders have limited influence in policy formation and evaluation. Through the CSH analysis, four interconnected boundary gaps were identified: between institutional purposes and broader public value, concentrated authority and participatory influence, dominant technical expertise and plural socio-technical knowledge, and indirect representation and policy legitimacy. These findings demonstrate that co-created cyberspace governance requires reconstructing boundary judgments toward greater stakeholder inclusion, knowledge plurality, accountability, and legitimate participation. The study does not argue that security, sovereignty, cultural concerns, or infrastructural control should be abandoned. Instead, it concludes that these objectives become more legitimate and sustainable when combined with transparency, knowledge pluralism, stakeholder inclusion, accountable decision-making, and institutional learning. Legitimate cyberspace governance therefore requires more than policy enforcement or digital service

In Press

delivery. It requires clear and publicly defensible answers to who benefits, who decides, whose knowledge counts, who bears the consequences, and how affected stakeholders can question or revise governance arrangements. Boundary critique provides a systematic foundation for developing a more participatory, adaptive, and legitimate model of cyberspace governance in Iran.

Conflict of interest

The authors declared no conflicts of interest.

Ethical considerations

The authors have completely considered ethical issues, including informed consent, plagiarism, data fabrication, misconduct, and/or falsification, double publication and/or redundancy, submission, etc. This article was not authored by artificial intelligence.

Data availability

The dataset generated and analyzed during the current study is available from the author on reasonable request.

Funding

This research did not receive any grant from funding agencies in the public, commercial, or non-profit sectors.

References

Ansell, C.; Sørensen, E. & Torfing, J. (2024). "The democratic quality of co-creation: A theoretical exploration". *Public Policy and Administration*. 39: 149-170. https://doi.org/10.1177/09520767231170 71.

Edelmann, N., & Virkar, S. (2023). "The impact of sustainability on co-creation of digital public services". *Admnistrative Sciences*. https://doi.org/10.3390/admsci13020043.

Escher, T. & Rottinghaus, B. (2024). "Effects of online citizen participation on legitimacy beliefs in local government: Evidence from a comparative study of online participation platforms in three German municipalities". *Policy & Internet*. 16(1): 173-208. https://doi.org/10.1002/poi3.371.

Falkner, G.; Heidebrecht, S.; Obendiek, A. & Seidl, T. (2024). "Digital sovereignty: Rhetoric and reality". *Journal of European Public Policy*. 31: 2099-2120. https://doi.org/10.1080/13501763.2024.2358984.

Fathi, M.R.; Sobhani, S.M.; Khosravi, M. & Khakpour, F. (2026). "Enhancing safety and reliability policies in gas pressure reduction stations: A Critical Systems Heuristics approach". *International Journal of Reliability, Risk and Safety: Theory and Application.* e243255. https://www.ijrrs.ir/article_243255.html.

Fathi, M.R.; Sobhani, S.M.; Nasrollahi, M. & Abdollahi Nejat, M. (2021). "The effect of structured knowledge on the performance of an organization". *Health Management and Information Science*. 8(4): 242-247. https://doi.org/10.30476/JHMI.2022.91363.1084.

Fratini, S.; Hine, E.; Novelli, C.; Roberts, H. & Floridi, L. (2024). "Digital sovereignty: A descriptive analysis and a critical evaluation of existing models". *DISO*. 3: 59. https://doi.org/10.1007/s44206-024-00146-7.

Goede, R. & Goede, H. (2025). "Introducing Critical Systems Heuristics 2.0: A third

No Press

boundary extending CSH from reflections on critical realism in information systems research". *Systems Research and Behavioral Science*. 42(5): 1424-1438. https://doi.org/10.1002/sres.3187.

Hanisch, M.; Goldsby, C.; Fabian, N. & Oehmichen, J. (2023). "Digital governance: A conceptual framework and research agenda". *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2023.113777.

Hofmann, S.C. & Pawlak, P. (2023). "Governing cyberspace: Policy boundary politics across organizations". *Review of International Political Economy*. 30: 2122-2149. https://doi.org/10.1080/09692290.2023.2249002

Hutcheson, M.; Morton, A. & Blair, S. (2024). "Critical systems heuristics: A systematic review". *Systemic Practice and Action Research*. 37: 499-514. https://doi.org/10.1007/s11213-023-09665-9.

Khosravi, A.; Fathi, M.R.; Habibi, M.J.; Sobhani, S.M. & Younessi, A. (2022). "The role of sustainable human resource management typologies in marketing: A case study of hospitals in Tehran". *Health Management and Information Science*. 9(3): 129-138. https://doi.org/10.30476/JHMI.2022.94599.1119.

Lai, R. & Beh, L.S. (2025). "The impact of political efficacy on citizens' e-participation in digital government". *Administrative Sciences*. 15(1): 17. https://doi.org/10.3390/admsci15010017.

Nasrollahi, M.; Fathi, M.R.; Sanouni, H.R.; Sobhani, S.M. & Behrooz, A. (2021). "Impact of coercive and non-coercive environmental supply chain sustainability drivers on supply chain performance: Mediation role of monitoring and collaboration". *International Journal of Sustainable Engineering*. 14(2): 98-106. https://doi.org/10.1080/19397038.2020.1853271.

Osborne, S.P.; Radnor, Z. & Strokosch, K. (2016). "Co-production and the co-creation of value in public services: A suitable case for treatment?". *Public Management Review*. 18(5): 639-653. https://doi.org/10.1080/14719037.2015.1111927.

Pauluzzo, R.; Fedele, P.; Dokalskaya, I. & Garlatti, A. (2024). "The role of digital technologies in public sector coproduction and co-creation: A structured literature review". *Financial Accountability & Management*. 40: 613-640. https://doi.org/10.1111/faam.12391.

Pierucci, F. (2025). "Sovereignty in the digital era: Rethinking territoriality and governance in cyberspace". *Digital Society*. 4: 27. https://doi.org/10.1007/s44206-025-00189-4.

Pohle, J. & Santaniello, M. (2024). "From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance?". *Policy & Internet*. 16: 672-691. https://doi.org/10.1002/poi3.426.

Santaniello, M. (2026). "Attributes of digital sovereignty: A conceptual framework". *Geopolitics*. 31(2): 788-809. https://doi.org/10.1080/14650045.2025.2521548.

Shahab, S.; Bagheri, B. & Potts, R. (2021). "Barriers to employing e-participation in the Iranian planning system". *Cities*. 116: 103281. https://doi.org/10.1016/j.cities.2021.103281.

Sharma, S.; Kar, A.K. & Gupta, M. (2024). "Untangling the web between digital citizen empowerment, accountability and quality of participation experience for e-government: Lessons from India". *Government Information Quarterly.* 41. 101964. https://doi.org/10.1016/j.giq.2024.101964.

Shin, B.; Floch, J.; Rask, M.; Bæck, P.; Edgar, C.; Berditchevskaia, A.; Mesure, P. & Branlat, M. (2024). "A systematic analysis of digital tools for citizen participation". *Government Information Quarterly*. 41: 101954. https://doi.org/10.1016/j.giq.2024.101954.

Sobhani, S.M.; Soltani, M. & Fathi, M.R. (2023). "Identifying the fields and mechanisms of value co-creation in foreign language institutions using fuzzy DEMATEL ranking approach: Case study Tehran, Iran". *Iranian Journal of Educational Research*. 2(4): 58-74. https://doi.org/10.22034/2.4.58.

Ulrich, W. & Reynolds, M. (2010). "Critical systems heuristics". In M. Reynolds & S. Holwell (Eds.). *Systems Approaches to Managing Change: A Practical Guide*

Proof

(pp. 243-292). Springer. https://doi.org/10.1007/978-1-84882-809-4_6.

Voorberg, W.H.; Bekkers, V.J.J.M. & Tummers, L.G. (2015). "A systematic review of co-creation and co-production: Embarking on the social innovation journey". *Public Management Review*. 17(9): 1333-1357. https://doi.org/10.1080/14719037.2014.930505.

Xin, G. & Huang, J. (2025). "Making the people's voice heard: Pathways of e-participative governance in China". *Journal of Chinese Governance*. 10: 33-56. https://doi.org/10.1080/23812346.2024.2400634.

Zargaran Khouzani, F.; Rahmanseresht, H.; Sobhani, S.M. & Fakhri, F. (2022). "Consequences of value co-creation strategy in educational services". *Journal of New Approaches in Educational Administration*. 12(6): 122-136. https://doi.org/10.30495/JEDU.2022.25429.5059.

Cyberspace Studies, Vol ?, No ?, ????

in Press