DIGITAL TRANSFORMATION AND ADMINISTRATION INNOVATION

Citation: Karimi Saleh, R., Taghipour, F., & Peykari, H. (2026). The Role of Combat Information Dissemination in Cognitive Deterrence and Strengthening the National Security of the Islamic Republic of Iran. *Digital Transformation and Administration Innovation*, 4(1), 1-10.

Received date: 2025-06-11 Revised date: 2025-09-01 Accepted date: 2025-09-09 Published date: 2026-01-01

The Role of Combat Information Dissemination in Cognitive Deterrence and Strengthening the National Security of the Islamic Republic of Iran

Reza Karimi Saleh[1], **Faezeh Taghipour**[1]*, **Hamidreza Peykari** [1]

1. Department of Communication Sciences, IsF.C.,, Islamic Azad University, Isfahan, Iran

*Correspondence: f.taghipour58@iau.ac.ir

Abstract

In the era of hybrid and cognitive warfare, the national security of states is profoundly influenced by narrative construction, psychological operations, and the management of public perception. Despite utilizing media capacities during the Sacred Defense and regional crises, the Islamic Republic of Iran lacks an institutionalized and indigenous model for combat information dissemination—one that can play a deterrent and coordinating role in confronting perceptual threats and misinformation. This study, aiming to design and explain a conceptual model for combat information dissemination, examines the media mechanisms effective in enhancing defensive soft power, psychological resilience, and legitimization of military actions within the framework of the national security of the Islamic Republic of Iran. The main research question is: What components, conditions, and consequences does the optimal model of combat information dissemination for cognitive deterrence and strengthening national security of the Islamic Republic of Iran include? The research method is qualitative, based on grounded theory, and relies on the analysis of data collected from 34 semi-structured interviews with media experts, military commanders, and security analysts using MaxQDA software. The findings indicate that effective combat information dissemination depends on six key components: real-time information management, strategic narrative construction, on-the-ground presence of military journalists, pre-emptive psychological operations, intelligent utilization of digital media, and institutional coordination between media and military organizations. Moreover, causal, contextual, and intervening conditions influencing this model, along with its strategies and consequences, were identified, and the final conceptual model was designed. Implementation of this model can lead to the reinforcement of cognitive deterrence, preservation of the psychological cohesion of forces, counteraction against enemy psychological operations, and enhancement of media–military synergy during crises.

Keywords: Combat information dissemination, Cognitive deterrence, National security, Hybrid warfare.

1. Introduction

In the contemporary security environment, the boundaries between war, peace, communication, and governance have become increasingly blurred. The rise of hybrid and cognitive warfare has placed information at the center of conflict, where narratives, perception management, and psychological influence often carry greater strategic weight than conventional military force (Pomerantsev, 2019; Rid, 2020). Disinformation campaigns, psychological operations, and propaganda have evolved into sophisticated instruments of political warfare, shaping public opinion, undermining trust in institutions, and altering the strategic balance of power (Geers, 2015; Paul & Matthews, 2016). In this context, the role of combat information dissemination (اطلاعرسانی رزمی) in strengthening national security and building cognitive deterrence has become a decisive factor for states such as the Islamic Republic of Iran.

The conceptual roots of information warfare and propaganda are deeply embedded in historical and contemporary scholarship. As Taylor (Taylor, 2003) demonstrates in his historical analysis of propaganda, the manipulation of narratives has been a tool of governance and warfare since antiquity. Chomsky (Chomsky, 2002) further argues that propaganda in modern democratic societies is not merely a tool of authoritarian regimes but also a mechanism through which elites manufacture consent and maintain political control. These insights align with Seaton's (Seaton, 2005) study of Gulf War propaganda and Carruthers' (Carruthers, 2011) comprehensive analysis of media and war in the twentieth century, both of which underscore how states weaponize media ecosystems during conflict.

From a strategic communication perspective, Hallahan and colleagues (Hallahan et al., 2007) define strategic communication as the purposeful use of communication by organizations to fulfill their missions. Applied to national security, this framework suggests that combat information dissemination can be systematically designed to align military, political, and societal objectives. Williams (Williams, 2018) expands on this logic, noting that strategic communication in national security contexts must integrate psychological operations, public diplomacy, and crisis messaging to generate trust, resilience, and legitimacy. In this regard, Seib (Seib, 2008) emphasizes the transformative power of global media, such as Al Jazeera, in reshaping world politics by diffusing narratives that transcend national borders.

The theoretical foundations of soft power and perception management further illuminate the importance of information in security strategies. Nye's concept of soft power highlights how attraction, legitimacy, and narrative control often provide more sustainable influence than coercion (J. Nye, 2004; J. S. Nye, 2004). His later work on leadership underscores how the ability to mobilize networks, shape agendas, and inspire trust represents a critical dimension of power in the twenty-first century (Nye, 2008). Combat information dissemination, therefore, can be conceptualized as an operational manifestation of soft power, transforming narratives into instruments of deterrence and national cohesion.

Emerging theories of cognitive warfare deepen this understanding by focusing on the battle for perceptions and beliefs. Geers (Geers, 2015) describes cognitive warfare as a "never-ending battle for minds," where the control of information ecosystems becomes as important as the control of territory. Thomas (Thomas, 2004) complements this with his analysis of Russia's reflexive control theory, which highlights how adversaries manipulate the decision-making processes of opponents by shaping their perception of reality. Such insights resonate with Tatham and Thies (Tatham & Thies, 2013), who stress that understanding human behavior, motivations, and cultural narratives will prove decisive in future conflicts.

Against this global theoretical backdrop, Iran's national security challenges reveal specific vulnerabilities and imperatives. Regional crises, hybrid threats, and the intensification of disinformation campaigns against Iran's domestic and international image necessitate a systematic model of combat information dissemination. Scholars have noted how regional security arrangements affect Iran's strategic environment (Mohammadi, 2024), while others analyze the implications of geopolitical developments such as the Abraham Accords (Shah Rezai, 2024) or the Al-Aqsa Storm (Moghavemi, 2024). These developments illustrate how adversarial narratives and perception management are integral to contemporary regional conflicts.

At the same time, global transformations such as digitalization create new risks and opportunities. Belyaevskaya-Plotnik (Belyaevskaya-Plotnik, 2025) highlights how the digital transformation of economies and public administration introduces novel threats to national security, while Cucoreanu (Cucoreanu, 2024) demonstrates how algorithms, bots, and social platforms can manipulate electoral processes and destabilize democratic governance. Maesschalck (Maesschalck, 2024) further explains that cyberspace operations fundamentally alter the logic of international security, making states more vulnerable to covert influence and psychological manipulation.

These global dynamics intersect with Iran's internal governance and security structures. Elahiyari and colleagues (Elahiyari et al., 2024) underscore that sustainable national security is dependent on good governance, institutional legitimacy, and transparent political communication. Izadi and Nezafati (Izadi & Nezafati, 2024) extend this argument by examining the military and political threats of artificial intelligence, which simultaneously create opportunities for enhancing defense capabilities and risks of exacerbating vulnerabilities. Similarly, Neikova (Neikova, 2024) highlights how illegal migration operates as a risk factor undermining national security, while Nechyporuk and Romanyuk (Nechyporuk & Романюк, 2024) emphasize the importance of metacognitive control and self-regulation in preparing future security professionals to cope with cognitive warfare challenges.

These perspectives reinforce the notion that modern national security is increasingly defined by the ability to manage perceptions, narratives, and public trust. Shahheidari (Shahheidari, 2024) underscores the importance of public order and security in international commercial arbitration, showing how legal and security frameworks are intertwined in safeguarding national interests. Weiss (Weiss, 2010) also demonstrates the normative dilemmas of humanitarian intervention, where narrative legitimacy often determines whether military action is viewed as lawful or coercive. These insights stress that without credible communication strategies, even legitimate defense operations risk being delegitimized in international discourse.

The challenge of countering disinformation has gained increasing prominence in recent years. Rid (Rid, 2020) documents the history of disinformation and active measures, revealing how foreign actors systematically exploit cognitive vulnerabilities. Paul and Matthews (Paul & Matthews, 2016) develop the “firehose of falsehood” model, illustrating how overwhelming information ecosystems with rapid, repetitive, and contradictory messages can effectively destabilize public trust. Pomerantsev (Pomerantsev, 2019) adds that the war against reality is no longer confined to authoritarian regimes but has become a global struggle where facts themselves are contested. These dynamics highlight the urgency for states to design robust models of combat information dissemination that can provide real-time accuracy, strategic narrative construction, and proactive psychological defense.

For Iran, the lack of an institutionalized and indigenous model of combat information dissemination poses strategic risks. Unlike traditional state-centric propaganda, combat information dissemination requires an integrated model that connects military institutions, media organizations, and cultural frameworks to produce coherent narratives. As Libicki (Libicki, 2007) observes, conquest in cyberspace is achieved not through physical force but through controlling the informational domain. The ability to prevent adversaries from shaping domestic and international perceptions is therefore a matter of survival.

Scholarly debates about media, propaganda, and security further stress that the success of any communication strategy depends on credibility and legitimacy. Seib (Seib, 2008) warns that new media ecosystems make censorship and information control less effective, while Seaton (Seaton, 2005) shows how poorly designed propaganda campaigns can backfire and reduce trust. Chomsky (Chomsky, 2002) similarly notes that when communication strategies are perceived as manipulative, they can erode legitimacy rather than enhance it. Thus, designing a model of combat information dissemination requires balancing operational secrecy with transparency, and narrative persuasion with authenticity.

Within this evolving framework, the concept of cognitive deterrence emerges as a vital strategic objective. By shaping public perception, reinforcing psychological resilience, and legitimizing defensive actions, combat information dissemination can prevent adversaries from exploiting informational vulnerabilities. As Nye (Nye, 2008) notes, leadership in the modern era is not only about command but also about persuasion and trust-building. Similarly, Geers (Geers, 2015) emphasizes that the future of conflict will depend on states’ ability to fight in the cognitive domain. For Iran, this means that national security strategies must evolve from reactive crisis communication to proactive, institutionalized, and coordinated combat information dissemination.

In conclusion, the literature demonstrates that information is both a vulnerability and a source of resilience in modern security environments. Historical analyses of propaganda (Carruthers, 2011; Chomsky, 2002; Taylor, 2003), theoretical contributions on soft power and strategic communication (Hallahan et al., 2007; J. S. Nye, 2004; Williams, 2018), and contemporary studies of cognitive warfare and digital risks (Cucoreanu, 2024; Geers, 2015; Maesschalck, 2024; Rid, 2020) all converge on a central insight: managing perceptions is as critical to national security as managing borders or weapons. For the Islamic Republic of Iran, the absence of a structured and indigenous model of combat information dissemination represents a strategic gap. Addressing this gap through the design of a conceptual model that integrates narrative construction, real-time information management, and institutional coordination will be essential to strengthening cognitive deterrence, safeguarding public trust, and enhancing national security in an era defined by hybrid and cognitive warfare.

2. Methods and Materials

The present research employed a qualitative approach based on grounded theory, following the Strauss and Corbin model. Data were collected through semi-structured interviews with 34 experts in the fields of media, security, soft warfare, and military command. Sampling was conducted purposefully and theoretically, continuing until theoretical saturation was achieved. For data analysis, three stages of open, axial, and selective coding were applied, and the analyses were carried out using MAXQDA software. During the analytical process, key concepts, causal, contextual, and intervening conditions, strategies, and consequences were extracted, and within the framework of a final paradigmatic model, a combat information dissemination model for enhancing national security was designed.

3. Findings and Results

In this study, using the grounded theory method and conducting 34 semi-structured interviews with specialists in the fields of media, security, soft warfare, and military command, the data were analyzed in three stages: open coding, axial coding, and selective coding. As a result, a conceptual model of combat information dissemination was identified and explained as a mechanism for cognitive deterrence and strengthening national security.

In the first stage, more than 120 initial concepts were extracted from the analysis of interview texts, which were classified into 18 subcategories. The most important of these concepts included:

1. Information security and disclosure control
2. Narrative construction and management of the security discourse
3. Institutional coordination in crisis communication
4. Public opinion as a battlefield of perception
5. Media literacy education and cognitive resilience

Table 1. Open Coding (Expert Interviews)

Primary Category (Open Code)	Initial Concept (Conceptual Code)	Key Statement (Quote or Theme Expressed by Interviewee)	No.
Effective and purposeful narrative construction	Legitimizing narrative construction	We need narratives of military actions that can gain public trust	1
Real-time information management	Information management in crisis	In today's psychological warfare, managing information is the most vital deterrent tool	2
Field information dissemination	On-the-ground presence of journalists	Deploying military journalists to the frontlines boosts troop morale	3
Institutional media–military coordination	Media–military structure	Coordination between military command and the media must be institutionalized	4
Countering enemy cognitive warfare	Cognitive threats from the enemy	The enemy targets our public opinion with propaganda and fake news	5
Legitimization of military actions	Strategic messaging	Intelligent communication can consolidate our defensive legitimacy in global public opinion	6
Countering misinformation	Speed in information transfer	Quick access to accurate information prevents rumor dissemination	7
Training military journalists	Integrated journalist training	A combat journalist must simultaneously receive military and media training	8
Institutionalizing combat information dissemination	Structural linkage to national security	Combat information dissemination must be part of the country's defense mechanism, not merely a media function	9
War of narratives	Importance of perception-making versus field reality	In today's wars, controlling the war narrative is more important than the war itself	10

In this stage, the subcategories were organized into six axial categories that formed the core structure of the combat information dissemination theory:

1. Narrative engineering and perceptual persuasion: Emphasis on producing strategic narratives for legitimizing defensive actions and managing public opinion.
2. Information management in crisis situations: Necessity of speed, accuracy, and coordination in disseminating military news while adhering to operational security requirements.

3. Media–security synergy: Establishment of communication structures between armed forces, national media, and cultural institutions for effective messaging.
4. Cognitive defense and media literacy: Strengthening public perception against rumors, psychological warfare, and enemy narratives.
5. Trust-building and psychological cohesion: The role of combat information dissemination in generating mental security and countering the weakening of social capital in defense institutions.
6. Public diplomacy and soft deterrence: Utilizing media tools to influence international audiences and explain the official narrative of the Islamic Republic.

Table 2. Axial Coding (Most Frequent Concepts)

Sample Related Concepts (Open Codes)	Subcategories (Conceptual Subunits)	Core Category	No.
Rapid dissemination of information, blocking false sources, narrative control, maintaining information readiness	Crisis information control / Preventing rumor generation / Rapid response	Real-time information management	1
Indigenous narrative design, explaining the reason for military presence, countering enemy narratives, controlling public opinion	Legitimizing military actions / Public perception-making / Reinforcing the national narrative	Purposeful and coordinated narrative construction	2
Training war correspondents, deploying journalists to the frontlines, media display of the battlefield	Reporting from operations / Showcasing bravery / Realistic reporting	On-the-ground presence of military journalists	3
Targeted media attack, psychological content production, confronting enemy soft warfare	Perceptual confrontation / Weakening enemy morale / Strengthening troop morale	Pre-emptive psychological operations	4
Using indigenous platforms, launching psychological campaigns, controlling social media	Social media utilization / Audience perception penetration / Media construction of resistance identity	Strategic use of digital media	5
Linking media systems to command, establishing media headquarters, command discipline in messaging	Institutionalizing communication / Formation of integrated media–military structure / Designing media command	Institutional coordination between media and military	6
Rapid response, transparency in crises, maintaining national cohesion	Increasing psychological resilience / Public persuasion / Strengthening trust in crises	Public trust and social stability	7
Sending diplomatic messages, positive global narrative construction, utilizing media diplomacy	International image-building / Neutralizing enemy accusations / Global legitimization	International credibility management	8

In the final stage of analysis, a paradigmatic model based on grounded theory was presented. This model identifies combat information dissemination as the central phenomenon in cognitive deterrence and specifies its causal, contextual, intervening, strategic, and consequential relationships:

1. **Causal Conditions:** Intensification of hybrid warfare, weakness in national narrative construction, and the rise of perceptual threats.
2. **Contextual Conditions:** Expansion of digital media, media polyphony, and the weakening of public trust.
3. **Strategies:** Training soft warfare journalists, developing indigenous platforms, and designing resistance narratives.
4. **Consequences:** Increased cognitive deterrence, reinforcement of the social capital of the system, psychological cohesion of society, and enhancement of national security.

Table 3. Selective Coding (Final Key Concepts)

Selective Category	Frequency in Interviews	Description of the Selective Concept within the Theoretical Framework	No.
Public trust and management of social morale	80 times	Combat information dissemination must strengthen social trust, preserve psychological cohesion, and withstand enemy psychological operations.	1
Information warfare and cyber security	45 times	Confronting digital infiltration, rumor generation, psychological disruption, and disinformation through combat information strategies and cyber defense.	2
Legitimization of military actions	44 times	Creating accurate public understanding of defensive and military operations through narrative construction and framing aligned with national and legal values.	3
International credibility management	60 times	Designing messages for global public opinion to reduce international pressure and enhance the image of the Islamic Republic of Iran in the international media environment.	4
Political stability and military–civilian relations	60 times	Combat information dissemination as a link between military structures and civilian perception to increase mutual understanding and reduce domestic perceptual tension.	5
Strategic messaging and psychological warfare	33 times	Designing a combat information dissemination structure to pre-empt cognitive warfare with the aim of influencing audience perceptions and weakening the enemy's cognitive apparatus.	6
Operational security and controlled disclosure of information	19 times	Intelligent integration of disclosure and concealment during military operations so that while informing, field security is preserved.	7

The findings indicate that combat information dissemination, if designed and implemented in a coordinated manner, can play an effective role in:

1. Preventing enemy cognitive warfare
2. Increasing the psychological resilience of the population during crises
3. Reducing the gap between military institutions and public opinion
4. Consolidating the official narratives of the Islamic Republic of Iran
5. Enhancing the effectiveness of defense and security media

This model encompasses realistic and applicable strategies for military commanders, media managers, and national security policymakers.

Table 4. Positive and Negative Consequences of Implementing the Model

Analytical Explanation	Description of Consequence	Type of Consequence	No.
With effective guidance and management of messaging, the enemy's ability to influence public opinion is reduced.	Increased cognitive deterrence against enemy psychological warfare	Positive	1
Targeted messages increase trust in defense institutions and reduce social anxiety.	Strengthening national cohesion and boosting the morale of the armed forces	Positive	2
Formal and structural cooperation between media and military command enhances the effectiveness of psychological operations.	Institutionalization of media–military linkage within the official structure of the country	Positive	3
Effective narrative construction can legitimize military actions in global public opinion.	Increased legitimacy of defensive actions domestically and internationally	Positive	4
Establishing mechanisms for rapid counteraction against rumors and cognitive warfare neutralizes enemy media penetration.	Increased national cyber and informational resilience	Positive	5
Enhancing international image through diplomatic messaging and intelligent offensive psychological operations.	Strengthening the soft power of the Islamic Republic of Iran at the international level	Positive	6
In the absence of transparency and honesty, public trust may be lost.	Risk of combat information dissemination being perceived as misunderstood government propaganda	Negative	7
May lead to unnecessary censorship or restrictions on freedom of expression, causing negative public reaction.	Risk of excessive information control and reduction of media transparency	Negative	8
Media independence may be undermined, reducing the professional credibility of the media.	Excessive dependency of media on military institutions	Negative	9
Weak or contradictory narratives can cause audience distrust and lead to failure in psychological operations.	Creation of strategic error in narrative construction in the absence of specialized training for media personnel	Negative	10

The implementation of the combat information dissemination model, if accompanied by specialized training, transparency, institutional coordination, and adherence to the principles of media ethics, can become one of the main pillars of cognitive deterrence and the enhancement of national security under conditions of hybrid and cognitive warfare. However, challenges such as excessive message control, weakened media independence, and public misperception must also be managed intelligently.

4. Discussion and Conclusion

The findings of this study provide evidence that combat information dissemination can be conceptualized as an effective mechanism for strengthening national security through the development of cognitive deterrence. By analyzing qualitative data from experts in media, security, and military command, the study identified six key components—real-time information management, strategic narrative construction, on-the-ground presence of military journalists, pre-emptive psychological operations, strategic use of digital media, and institutional coordination between media and military structures—that together form the backbone of an indigenous model of combat information dissemination. These findings align with existing research emphasizing the centrality of narrative, perception management, and communication in modern conflict environments (Geers, 2015; Pomerantsev, 2019; Rid, 2020).

The emphasis on narrative construction as a central mechanism of cognitive deterrence resonates strongly with Taylor's historical overview of propaganda, which situates narrative as a strategic weapon in both ancient and modern contexts (Taylor, 2003). Similarly, Carruthers highlights how the media has consistently been mobilized to shape public opinion during wartime (Carruthers, 2011). This study's findings on the importance of legitimizing military actions through narrative echo Chomsky's argument that propaganda in democratic and authoritarian contexts alike functions to generate consent and control perception (Chomsky, 2002). Moreover, the identification of narrative construction as a process of managing public trust and global legitimacy reflects Seaton's analysis of Gulf War media strategies (Seaton, 2005), as well as Seib's account of how new global media ecosystems transform political communication (Seib, 2008).

The role of real-time information management emerged as another critical determinant of effective combat information dissemination. The ability to rapidly and accurately communicate during crises is consistent with Paul and Matthews' analysis of the Russian "firehose of falsehood" propaganda model, where speed and volume often outweigh truth in shaping perception (Paul & Matthews, 2016). The findings demonstrate that Iran's national security requires not only defensive measures against disinformation but also proactive strategies for ensuring that accurate narratives are disseminated before rumors dominate the information environment. This insight mirrors Rid's historical examination of disinformation campaigns (Rid, 2020), which shows how delay or inconsistency in communication creates vulnerabilities that adversaries can exploit.

The study further highlights the importance of military journalists' field presence in reinforcing troop morale and creating authentic narratives. This finding supports the argument advanced by Williams, who underscores the role of strategic communication in national security as a means of building legitimacy and resilience (Williams, 2018). By enabling journalists to provide direct accounts from the battlefield, states can generate credibility that pre-packaged propaganda cannot achieve. Such credibility is crucial for both domestic cohesion and international image-building, in line with Weiss's emphasis on legitimacy in humanitarian intervention (Weiss, 2010).

The component of pre-emptive psychological operations identified in the findings reflects broader scholarly insights into cognitive warfare and reflexive control. Geers emphasizes that modern conflict is fundamentally about controlling minds, not territory (Geers, 2015), while Thomas explains how reflexive control can manipulate adversaries' decision-making by shaping their perception of reality (Thomas, 2004). The finding that Iran must design proactive psychological strategies rather than simply reacting to adversarial propaganda is therefore consistent with global theories of information warfare. Tatham also stresses the necessity of understanding human motivation and cultural context in order to design effective communication campaigns (Tatham & Thies, 2013), which directly aligns with the strategies identified by experts in this study.

The strategic use of digital media was repeatedly highlighted as a necessary pillar of combat information dissemination. This aligns with Libicki's argument that conquest in cyberspace occurs not through physical means but by controlling information systems (Libicki, 2007). As Maesschalck notes, cyberspace operations profoundly impact international security by enabling covert influence and manipulation (Maesschalck, 2024). Cucoreanu further shows how digital platforms can be weaponized to manipulate electoral outcomes (Cucoreanu, 2024), reinforcing the finding that effective national security strategies must integrate digital communication as both an opportunity and a threat. This is particularly relevant for Iran, where adversarial actors increasingly deploy bots, algorithms, and social media campaigns to undermine public trust and sow division.

Another significant finding concerns the necessity of institutional coordination between military and media structures. Experts emphasized that fragmented communication undermines credibility and effectiveness, while institutionalized cooperation enhances strategic outcomes. This reflects Hallahan's definition of strategic communication as the coordinated use of communication processes to fulfill organizational missions (Hallahan et al., 2007). It also aligns with Elahiyari and colleagues' research on the role of governance quality in national security, which stresses that sustainable security requires legitimacy and coordination between institutions (Elahiyari et al., 2024). The call for integration between defense structures and media echoes Nye's soft power framework, which underscores that credibility and legitimacy are the foundations of influence (J. S. Nye, 2004; Nye, 2008).

The consequences of implementing the model—including increased cognitive deterrence, enhanced social cohesion, improved legitimacy of military actions, and greater cyber resilience—were found to be broadly consistent with prior scholarship on the role of communication in security. For instance, Seib's work on the Al Jazeera effect illustrates how global communication platforms can reshape narratives and political legitimacy (Seib, 2008). Pomerantsev similarly argues that the war against reality has become global, where legitimacy and trust are contested in information ecosystems (Pomerantsev, 2019). The study's identification of risks, such as excessive censorship or over-dependence of media on military institutions, reflects concerns raised by Chomsky (Chomsky, 2002) and Seaton (Seaton, 2005), who both warn that manipulative or heavy-handed propaganda can erode rather than strengthen legitimacy.

In addition, the research findings resonate with more recent analyses of Iran's regional security environment. Mohammadi highlights the impact of West Asian security arrangements on Iran's strategic position (Mohammadi, 2024), while Shah Rezai points to the implications of the Abraham Accords (Shah Rezai, 2024). Both studies reinforce the importance of Iran having a coherent information strategy to mitigate external pressures and delegitimizing narratives. Moghavemi's analysis of the Al-Aqsa Storm (Moghavemi, 2024) also underscores how information campaigns have become a central theater of regional conflict, validating this study's emphasis on institutionalizing combat information dissemination.

Finally, the broader implications of this research connect to the challenges of globalization, migration, and governance. Neikova identifies illegal migration as a security risk that undermines state stability (Neikova, 2024), while Nechyporuk stresses the role of metacognitive and self-regulatory skills in preparing future security professionals (Nechyporuk & Романюк, 2024). Both insights suggest that the battle for perceptions extends beyond immediate military threats, encompassing long-term societal resilience and adaptive capacity. Belyaevskaya-Plotnik also warns that digital transformation introduces new vulnerabilities in governance and public administration (Belyaevskaya-Plotnik, 2025), reinforcing the urgency for Iran to institutionalize robust combat information dissemination strategies as part of its national security doctrine.

Overall, the results confirm that combat information dissemination is not merely a tactical tool but a strategic necessity in hybrid and cognitive warfare. The findings build on, and extend, the existing body of literature by offering an indigenous conceptual model tailored to Iran's security environment. This model addresses global lessons from propaganda studies, soft power theory, strategic communication, and cognitive warfare, while also responding to the unique regional and institutional challenges faced by Iran.

This study is not without its limitations. First, the reliance on qualitative interviews, while offering deep insights, limits the generalizability of the findings. The perspectives reflect the views of selected experts and may not capture the full diversity of opinions across Iran's broader defense and media ecosystems. Second, the study focused on national-level security challenges and did not examine local variations in media practices or public responses across different regions of the country. Third, although efforts were made to triangulate the findings through coding and validation, the inherently interpretive nature of grounded theory research introduces the possibility of researcher bias. Finally, the study did not incorporate quantitative measures of the effectiveness of combat information dissemination, which may be necessary to empirically validate the proposed model.

Future research should consider expanding the scope of analysis by incorporating quantitative methods to measure the impact of combat information dissemination strategies on public trust, resilience, and national security indicators. Comparative studies across countries facing similar hybrid threats could provide valuable cross-national insights into the effectiveness of different approaches. Longitudinal studies that track the evolution of media–military coordination over time would also contribute to understanding the sustainability of such models. Additionally, future research should examine the ethical dimensions of combat information dissemination, including the balance between transparency and operational secrecy, as well as the potential risks of undermining media independence.

For policymakers and practitioners, the findings underscore the need to institutionalize combat information dissemination as an integrated component of national security strategy. This requires formalized coordination mechanisms between military, media, and cultural institutions; investment in training specialized military journalists; and the development of rapid-response communication protocols for crisis situations. Ethical guidelines must also be established to ensure that communication strategies maintain credibility and do not devolve into manipulative propaganda. Finally, leveraging digital platforms intelligently, while simultaneously safeguarding against disinformation and cyber threats, should be a core priority for enhancing cognitive deterrence and protecting national security.

Ethical Considerations

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

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

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

References

Belyaevskaya-Plotnik, L. (2025). Threats to National Security in the Context of Digital Transformation of the Economy and Public Administration. *National Interests Priorities and Security*, *21*(2), 65-76. https://doi.org/10.24891/ni.21.2.65

Carruthers, S. L. (2011). *The Media at War: Communication and Conflict in the Twentieth Century*. Palgrave Macmillan. https://search.proquest.com/openview/58afb5c00f45914ecac721428ec2d8c0/1?pq-origsite=gscholar&cbl=6565

Chomsky, N. (2002). *Media Control: The Spectacular Achievements of Propaganda*. Seven Stories Press. https://books.google.com/books?hl=fa&lr=&id=IQR3X9KwR44C&oi=fnd&pg=PA3&dq=Media+Control:+The+Spectacular+Achievements+of+Propaganda&ots=pwNclL2AyX&sig=fkOVPkMG1lYJQFRgwGT1V0h53cs

Cucoreanu, C. (2024). Cyber Risks to National Security: Manipulation of the Electoral Process Through the Use of Bots and Algorithms on Social Platforms. *European Journal of Law and Public Administration*, *11*(2), 226-236. https://doi.org/10.18662/eljpa/11.2/244

Elahiyari, M., Sazmand, B., & Roshad, M. (2024). Examining the Impact of Good Governance Components on Sustainable National Security: Emphasizing Iran's Governance Experience (1989-2021). *Contemporary Political Studies*, *15*(4).

Geers, K. (2015). Cognitive Warfare and the Future of Conflict. https://hcss.nl/wp-content/uploads/2023/06/04-Cognitive_Warfare_as_Part_of_Society__Never_Ending_Battle_for_Minds.pdf

Hallahan, K., Holtzhausen, D., van Ruler, B., Vercic, D., & Sriramesh, K. (2007). Defining strategic communication. *International Journal of Strategic Communication*, *1*(1), 3-35. https://doi.org/10.1080/15531180701285244

Izadi, J., & Nezafati, T. (2024). An Examination of the Military and Political Threats and Opportunities of Artificial Intelligence on Iran's National Security. *International Relations Studies*(67), 217-237.

Libicki, M. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press. https://doi.org/10.7249/CB407

Maesschalck, S. (2024). Gentlemen, You Can't Fight in Here. Or Can You?: How Cyberspace Operations Impact International Security. *World Affairs*, *187*(1), 24-36. https://doi.org/10.1002/waf2.12004

Moghavemi, A. R. (2024). Analyzing the Impacts of Al-Aqsa Storm on Israel's National Security. *Strategic Environment Journal of the Islamic Republic of Iran*, *8*(1), 9-48.

Mohammadi, S. (2024). The Impact of Security Arrangements in West Asian Countries on the National Security of the Islamic Republic of Iran: A Copenhagen School Perspective. *Jspsich*, *3*(3), 200-219. https://doi.org/10.61838/kman.jspsich.3.3.12

Nechyporuk, M., & Романюк, В. Н. (2024). Methodological Aspects of Researching National Security Students' Metacognitive Control in the Context of Self-Regulated Learning. *Scientific Notes of Ostroh Academy National University Psychology Series*, *1*(17), 46-55. https://doi.org/10.25264/2415-7384-2024-17-46-55

Neikova, M. (2024). Illegal Migration as a Risk Factor and Potential Threat to Bulgarian National Security. *Strategies for Policy in Science and Education-Strategii Na Obrazovatelnata I Nauchnata Politika*, *32*(4s), 83-88. https://doi.org/10.53656/str2024-4s-8-ill

Nye, J. (2004). *Soft Power: The Means to Success in World Politics*. PublicAffairs. https://go.gale.com/ps/i.do?id=GALE%7CA126682714&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00323195&p=AONE&sw=w

Nye, J. S. (2004). *Soft Power: The Means to Success in World Politics*. PublicAffairs. https://go.gale.com/ps/i.do?id=GALE%7CA126682714&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00323195&p=AONE&sw=w

Nye, J. S. (2008). *The Powers to Lead*. Oxford University Press. https://books.google.com/books?hl=fa&lr=&id=HNXQCwAAQBAJ&oi=fnd&pg=PR7&dq=The+Powers+to+Lead&ots=u9thVXGE4Z&sig=9DLOb-HAW-Vh8extZOgv4K0Jvwc

Paul, C., & Matthews, M. (2016). The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. https://doi.org/10.7249/PE198

Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality*. Faber & Faber. http://eipt.khpi.edu.ua/index.php/2313-4895/article/download/219687/219412

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux. https://academic.oup.com/ia/article-abstract/97/1/244/6041478

Seaton, J. (2005). War and the Media: Propaganda and Persuasion in the Gulf War. In *Media Studies Reader*. https://books.google.com/books?hl=fa&lr=&id=V9tRAQAAIAAJ&oi=fnd&pg=PR7&dq=War+and+the+Media:+Propaganda+and+Persuasion+in+the+Gulf+War&ots=AI5DTiVLTQ&sig=WVveW0frJoHEuId61VrjODyQhfQ

Seib, P. (2008). *The Al Jazeera Effect: How the New Global Media Are Reshaping World Politics*. Potomac Books. https://books.google.com/books?hl=fa&lr=&id=TuqWvYVo1rsC&oi=fnd&pg=PP2&dq=The+Al+Jazeera+Effect:+How+the+New+Global+Media+Are+Reshaping+World+Politics&ots=MsmRlbxLwP&sig=38DOTqYEqgCrNFzbp8em99R4n9E

Shah Rezai, M. H. (2024). *The Impact of the Abraham Accords on the National Security of the Islamic Republic of Iran* Islamic Azad University, Khorasgan Branch.

Shahheidari, F. (2024). The Role of Public Order and National Security in International Commercial Arbitration. *Iranian Research Journal on International Relations*, *1*(3).

Tatham, S., & Thies, G. (2013). *Behavioural Conflict: Why Understanding People and Their Motivations Will Prove Decisive in Future Conflict*. Military Studies Press. https://www.behaviouralconflict.com/s/Bolt-review.pdf

Taylor, P. (2003). *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day*. Manchester University Press. https://www.manchesterhive.com/abstract/9781847790927/9781847790927.xml

Thomas, T. (2004). Russia's Reflexive Control Theory and the Military. *Journal of Slavic Military Studies*, *17*(2), 237-256. https://doi.org/10.1080/13518040490450529

Weiss, T. G. (2010). *Humanitarian Intervention*. Polity Press. https://www.tandfonline.com/doi/pdf/10.1080/714003751

Williams, K. (2018). Strategic Communication for National Security. *Naval War College Review*. https://apps.dtic.mil/sti/html/tr/ADA575204/