



The Journal of *News Science*

Vol. 14, No. 4, Ser.56, Winter 2025, P. 42- 47

Journal homepage: <https://www.mjourcom.ir/>

DOI : <http://doi.org/10.22034/lrsi.2025.523835.1366>

Open Access

ORIGINAL ARTICLE

Developing and Validating an Adversarial Cognitive Warfare Model Against the Islamic Revolution: A Structural Equation Modeling Approach

Ehsan Mostafapour¹  | Aziz Ghazanfari²  

1. Corresponding Author, Assistant Professor, Department of Culture and Media, Shahhid Mahallati University of Islamic Sciences, Qom, Iran. E-mail: ema14251425@gmail.com
2. Assistant Professor of Politics, Imam Hussein University, Tehran, Iran. E-mail: ghazanfari.a@chmail.ir

Received: May 15, 2025

Accepted: September 22, 2025

EXTENDED ABSTRACT

Interdiction:

This study aims to develop and validate a strategic model of cognitive warfare as employed by adversaries against the Islamic Revolution of Iran. Employing a hybrid methodological approach, the research integrates structural equation modeling (SEM) with strategic scenario analysis to identify the constituent components, variables, and strategic responses associated with cognitive warfare.

Cognitive warfare represents an emerging yet increasingly prominent domain of conflict that targets human cognition through technological and psychological means. Given its ideological, spiritual, and anti-hegemonic foundations, the Islamic Revolution of Iran poses a substantial challenge to liberal secularism and Western-centric political orders. Consequently, it has become

a primary target of hostile psychological and cognitive operations designed to manipulate perception, erode public trust, and distort historical narratives. A critical research gap persists in the absence of a comprehensive, multidimensional, and predictive model of cognitive warfare. Previous efforts have either focused narrowly on propaganda or failed to integrate insights from decision science, strategic communication, and national security.

This study seeks to address this gap by answering two fundamental research questions, thereby identifying (1) the components and variables of the cognitive warfare model directed against the Islamic Revolution, and (2) the most effective strategic responses available to the Revolution in confronting such warfare.

The theoretical foundation of the study draws upon cognitive learning theories, behavioral psychology, cyber-psychology, and human factors engineering. Central to the proposed cognitive warfare model is the exploitation of inherent vulnerabilities in human cognition, including:

Limited attentional resources: Excessive sensory and informational inputs are utilized to desensitize audiences and obscure vital messages, resulting in "attention fatigue" that diminishes the public's capacity to differentiate authentic from manipulated information.

Cognitive dissonance and illusion: The introduction of conflicting narratives, moral relativism, and ambiguous language induces judgment paralysis, emotional fatigue, and mental disengagement.

Attribution errors and generalized bias: By reinforcing existing prejudices and promoting reductionist explanations, cognitive warfare disables rational public discourse and undermines social cohesion.

Furthermore, the study highlights that these tactics are executed through the coordinated use of media platforms, AI algorithms, and digital manipulation technologies—including deepfakes, echo chambers, and automated content targeting.

Method:

This applied developmental study adopts a triangulated method comprising qualitative and quantitative approaches. The research process included: a systematic literature review of over 120 scholarly sources; semi-structured interviews with 15 experts in strategic communication, media, military psychology, and Islamic thought; and content analysis of 50 domestic and international policy documents. Extracted data were categorized and coded into conceptual themes. Exploratory and confirmatory factor analyses (EFA and CFA) validated the relationships among identified variables. Reliability and validity measures were robust (Cronbach's alpha = 0.79; KMO = 0.701; RMSEA = 0.03), indicating statistical soundness. The final model was subsequently subjected to structural modeling using cross-impact balance analysis and scenario building via Scenario Wizard.

Findings:

The final cognitive warfare model comprises four primary components and 21 validated variables:

Damaging Revolutionary Functions: Encompasses strategic deception, fabrication of facts, inducing public pessimism, weakening the system's performance image, and manufacturing distrust in governance and leadership.

Cognitive Coexistence and Mental Reprogramming: Refers to sustained exposure to ideological distortions, memory reconstruction, instilling inferiority complexes, cultural alienation, and psychological warfare against national identity.

Legitimizing Media Techniques: Includes algorithmic manipulation, use of influencers, cognitive hacking through emotional narratives, viral disinformation, and amplification of disruptive discourses via technological tools.

Synchronization of Pressure Tools: Comprises the simultaneous application of political, legal, economic, and media levers to generate cumulative cognitive fatigue and systemic destabilization. These elements form a coherent structure through which cognitive warfare is waged to weaken the ideological base and strategic coherence of the Islamic Revolution.

Strategic Scenario Outcomes:

Through scenario analysis, the study identifies three synergistic and adaptive strategies for effective cognitive defense:

- **Institutionalizing strategic management:** Enhancing the Islamic system's capacity to monitor, predict, and respond to cognitive threats through structured crisis management and scenario-based policy design.
- **Self-legitimation through strategic communication:** Focusing on credible, transparent, and values-based narrative construction to neutralize disinformation and promote revolutionary achievements. This aligns with the Islamic concept of "Jihad of Explanation."
- **Ideological revitalization:** Promoting cognitive resilience via public education, grassroots mobilization, and reaffirmation of revolutionary values. This strategy emphasizes training actors capable of discursive confrontation and collective awareness-raising.

In the developed model, targeting the vital functions of the Islamic Revolution is identified as a prominent and prioritized strategy within the adversary's cognitive warfare. These core functions encompass fundamental activities distributed across political, military, social, and informational infrastructures, the disruption of which may lead to the collapse of essential service systems. While such functions possess inherent vulnerabilities, their exploitation is contingent upon the adversary's access to specific tools and operational capabilities. Moreover, some vulnerabilities—such as those exploited in cyberattacks—remain undetectable until the moment of execution, referred to as "zero-day" scenarios (Bloom, 2004). Consequently, continuous risk assessment is essential to detect and mitigate potential weaknesses and ensure systemic resilience. In addition, many of the Revolution's functions are not strictly structural but extend to ideological and cognitive domains, rendering their monitoring and management highly complex yet crucial. These findings align with Petit (2012), who emphasized the intrinsic unpredictability of hybrid cognitive

warfare, which hinders accurate forecasting and strategic response. In the media dimension, the study supports existing theories of strategic communication, underscoring the importance of leadership, credibility, mutual understanding, adaptability, and continuity. These principles are operationalized through hybrid warfare tactics—such as cognitive hacking, ideological distortion, and social manipulation—to influence public perception and behavior within target populations.

Conclusions:

This research provides a multidimensional, empirically validated model for understanding the structure and dynamics of cognitive warfare against the Islamic Revolution. By integrating structural equation modeling with strategic scenario analysis, the study bridges theoretical and practical perspectives. Its findings equip policymakers and scholars with actionable insights for safeguarding national identity, enhancing cognitive resilience, and securing the future of the Islamic Revolution against evolving psychological and technological threats.

Data Availability Statement

Data available on request from the authors.

Acknowledgements

The authors would like to thank anonymous reviewers.

Ethical considerations

Not applicable.

Funding

Not applicable.

Conflict of interest

The authors declare no conflict of interest.

References

- Araqi, A., Bidgoli, M., & Rajabi Deh Borzoei, A. (2023). Analyzing the enemy's cognitive war goals and coping strategies with emphasis on the teachings of the Qur'an. *Holy Defense Studies*, 8(4), 143-162. (in Persian)
- Bernal, A., Carter, C., Singh, I., Cao, K., & Madreperla, O. (2020). *Cognitive warfare - An attack on thought and truth*. Baltimore, MD: Johns Hopkins University. Retrieved from: <https://www.innovationhub-act.org/sites/default/files/2021-03/Cognitive%20Warfare.pdf>
- Biddle, T. D. (2020). Coercion theory: A basic introduction for practitioners. *Texas National Security Review*, 3(2), 1-25.
- Bock, P. (1993). *The emergence of artificial cognition: An introduction to collective learning*. Singapore: World Scientific.
- Brafman, O., & Brafman, R. (2008). *Sway: The irresistible pull of irrational behavior*. New York, NY: Broadway Books.
- Chiarelli, P. W., & Smith, S. (2007). Learning from our modern wars: The imperatives of preparing for a dangerous future. *Military Review*, 4(1), 2-15.
- Claverie, B., & du Cluzel, F. (2022). The cognitive warfare concept. *NATO ACT Innovation Hub*, 11. Retrieved from https://www.innovationhub-act.org/sites/default/files/2022-02/CW%20article%20Claverie%20du%20Cluzel%20final_0.pdf (accessed February 12, 2024).
- Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data*, 7. <https://doi.org/10.3389/fdata.2024.1452129>
- Dörnyei, Z., & Taguchi, T. (2010). *Questionnaires in second language research: Construction, administration and processing*. New York, NY: Routledge.

- Eslick, A. N., Fazio, L. K., & Marsh, E. J. (2011). Ironic effects of drawing attention to story errors. *Memory*, 19(2), 184-191.
- Farokhipur, S. (2024). Cognitive warfare: Emphasizing hybrid warfare. Qom: Zamzam-e Hedayat. (in Persian)
- Fazio, L. K., & Marsh, E. J. (2010). Correcting false memories. *Psychological Science*, 21(6), 801-803.
- Guadagno, R. E., & Gutteri, K. (2019). Fake news and information warfare: An examination of the political and psychological processes from the digital sphere to the real world. In I. E. Chiluiwa & S. A. Samoilenko (Eds.), *Research on deception, fake news, and misinformation online* (pp. 167-191). IGI Global.
- Hassanpoor, H., & Hosseini, S. M. (2024). Designing a dual-process model of cognitive value warfare with an emotional approach in society. *Military Psychology*, 15(2), 91-117. (in Persian)
- Hellström, J., Kallioniemi, P., Kytöneva, S., & Puranen, M. (2024). StratCom: NATO Strategic Communications Centre of Excellence. Riga, Latvia: NATO Strategic Communications Centre of Excellence. Retrieved from <https://stratcomcoe.org/publications/are-russian-narratives-amplified-by-prc-media-a-case-study-on-narratives-related-to-swedens-and-finlands-nato-applications/298> (accessed April 2, 2024).
- Hung, T. C., & Hung, T. W. (2022). How China's cognitive warfare works: A frontline perspective of Taiwan's anti-disinformation wars. *Journal of Global Security Studies*, 7(16), 13-21. <https://doi.org/10.1093/jogss/ogac016>
- Keshavarz, M. (2024). The strategy of the enemy in the cognitive war in the field of governance. *National Studies Journal*, 25(98), 159-180. <https://doi.org/10.22034/rjnsq.2024.433463.1557> (in Persian)
- Keshavarz, M., Siahpoosh, A., Arjini, H., & Naeni, A. M. (2024). The spectrum of people in cognitive warfare and the role of actors in intelligent warfare as human capital. *Islamic Social Studies*, 29(127), 101-126. <https://doi.org/10.30513/iss.2024.5565.1312> (in Persian)
- Le Guyader, H. (2022). Cognitive domain: A sixth domain of operations. In B. Claverie, B. Prebot, N. Buchler, & F. du Cluzel (Eds.), *Cognitive warfare: The future of cognitive dominance* (pp. 1-5). NATO Collaboration Support Office. Retrieved from <https://hal.science/hal-03635898v>
- Mateski, M. E., Mazzuchi, T. A., & Sarkani, S. (2010). The hypergame perception model: A diagrammatic approach to modeling perception, misperception, and deception. *Military Operations Research*, 15(2), 21-37.
- Mattingsdal, J., Espevik, R., Johnsen, B. H., & Hystad, S. W. (2023). Exploring why police and military commanders do what they do: An empirical analysis of decision-making in hybrid warfare. *Armed Forces & Society*, 1-23. <https://doi.org/10.1177/0095327x231160711>
- McWilliams, A., & Legnér, M. (2024). Threat assessments and heritage in the age of hybrid warfare. *International Journal of Heritage Studies*, 1-14. <https://doi.org/10.1080/13527258.2024.2393610>
- Michaels, D. (2020). *The triumph of doubt: Dark money and the science of deception*. Oxford, UK: Oxford University Press.
- Miller, S. (2023). Cognitive warfare: An ethical analysis. *Ethics of Information Technology*, 25(46). <https://doi.org/10.1007/s10676-023-09717-7>
- NATO. (2022). NATO 2022 strategic concept. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (accessed August 16, 2023).
- Pallant, J. (2013). *SPSS survival manual: A step-by-step guide to data analysis using IBM SPSS*. Berkshire, UK: Open University Press.
- Pentland, A. (2008). *Honest signals: How they shape our world*. Boston, MA : MIT Press.
- Petit, B. (2012). *Social media and UW*. U.S. Army John F. Kennedy Special Warfare Center and School.
- Putter, D. (2024). Navigating the interplay of cognitive warfare and counterintelligence in African security strategies: Insights and case studies. *Journal of Policing, Intelligence and Counter Terrorism*, 1-20. <https://doi.org/10.1080/18335330.2024.2440873>
- Saadatmand, H., Taheri, M., Piri Zamaneh, M., & Ghadami, K. (2024). Explaining future solutions to deal with the cognitive war of the West against the Islamic Republic of Iran. *Basij Strategic Studies*, 27(102), 97-136. (in Persian)
- Sharot, T. (2017). *The influential mind: What the brain reveals about our power to change others*. New York, NY: Henry Holt.
- Slovan, S., & Fernbach, P. (2017). *The knowledge illusion*. New York, NY: Riverhead Books.

Tasiu, A. (2018). Hostile gatekeeping: The strategy of engaging with journalists in extremism reporting. *Defence Strategic Communications - Official Journal of the NATO Strategic Communications Centre of Excellence*, 5, 51-85.

Cite this article : Mostafapour E, & Ghazanfari, A., (2025). Developing and Validating an Adversarial Cognitive Warfare Model Against the Islamic Revolution: A Structural Equation Modeling Approach, *News Science*, 14 (4), 42-47.

DOI: <http://doi.org/10.22034/lrsi.2025.523835.1366>



© The Author(s).

DOI: <http://doi.org/10.22034/lrsi.2025.523835.1366>
