Security Horazions

Validation of the strategic deception model with Offensive Approach to Intelligence

Ehsan Kiani[1]| Hadi Tajik[2]| Mehdi Firouzkouhi[3]

1. Corresponding Author: Phd of Middle East Studies. University of Imam Hussein, Tehran, Iran.
Email: e1386k@gmail.com
1. Associate Professor, University of Imam Hussein, Tehran, Iran
1. Associate Professor, University of Imam Hussein, Tehran, Iran

Volume info

Vol. 18
Series: 68
Autumn 2025

Article Type

Research Paper

Article History

Received:
2024-01-31
Revised:
2025-03-29
Accepted:
2025-08-20
Published:
2025-11-29

ISSN – E-ISSN

ISSN: 2538-1857
E-ISSN: 2645-5250

Abstract

Introduction

Surprise is one of the most important threats to the information society and political structures. One of the negative paths to reduce this threat is defensive policies through the expansion of intelligence surveillance and control over the country's security environment. However, a more positive and sustainable path could be to pursue an offensive policy to attack the opponent's or enemy's computing devices. Adopting an offensive approach to intelligence is one of the issues that has not received much attention in the foreign policy of the Islamic Republic of Iran. This should be taken seriously, especially regarding the Hybrid war against Iran at hard and soft power, as well as in various security, economic, military and diplomatic fields. Due to the necessity of this issue, in this research, an offensive approach to intelligence has been tried from the perspective of strategic deception. In this regard, a definition of offensive approach has been tried first. Then, according to the literature on deception, a strategic deception model with an offensive Intelligence approach has be formulated.

Methodology

In this research, first the library study method and then the elite opinion survey method were used. In the library studies method, an attempt was made to extract the components and axes of these two concepts using the existing literature on strategic deception and intelligence invasion. Then, the model resulting from these studies was evaluated by elites. In fact, to increase the validity of the final Pattern, this model is submitted to the opinion of elites to measure its validity and reliability. These elites included people who had scientific or practical experience of working in the country's foreign policy in various agencies. In the end, the components that had a stronger evaluation formed the final model.

Cite this Article: Kiani, E., Tajik, H., & Firouzkouhi, M. (2025). Validation of the strategic deception model with Offensive Approach to Intelligence. Security Horizons, 18(68), 11-38.
DOR: 20.1001.1.25381857.1404.18.68.1.5

OPEN ACCESS

Publisher: Imam Hossein University.

Result and discussion

The strategic deception model with an intelligence offensive approach has two dimensions. The first dimension is information superiority, according to which the deceiver dominates the path of intelligence exchange and the type of data by controlling intelligence channels. The second dimension is obtaining intelligence through observing the actions and behaviors of the intelligence subject. This model can be implemented at two levels: the first level is information networks and the higher level of subject perception. This model is a type of preemptive operation that penetrates the intelligence cycle of the opponent's elites with the aim of changing their behavior. The success of implementing this model is measured through these indicators. First, it should provide the basis for penetrating the opponent's intelligence network. Second, it should lead to the accumulation of experience by the deceiver and help him design future operations more accurately. Third, it should gain a good understanding of how the opponent perceives. Fourth, it should have long-term results.

Conclusion

The results of this elite survey show that this model has been approved and has the potential to become a Pattern. The stages of this Pattern include goal setting, subject identification, implementation, and ultimately monitoring and controlling the implementation. The first stage is to determine strategic goals and ultimately design a deception scenario with reasonable methods and available tools. The second stage is to identify the subject and the route of the deception operation through analyzing the enemy's behavior, the available routes for transmission, and design information propositions to formulate the deception story. The third stage is to disseminate incorrect, incomplete, and selective information and perform fake shows to deceive the enemy. The final stage is to monitor the enemy's reaction, evaluate the effectiveness of the deception, and modify processes for subsequent operations. This Pattern, while strengthening the indigenous literature on the concept of intelligence invasion, provides clearer paths and solutions for strengthening and enhancing national security through the development of a strategic deception model with an intelligence invasion approach. At the same time, efforts to strengthen the literature on intelligence invasion in other subjects can produce applied knowledge on this subject and also favor positive and proactive approaches in the operational field.

Keywords: Strategic deception, information invasion, foreign policy.

References

Almalki. Sami (2016), Integrating Quantitative and Qualitative Data in Mixed Methods Research—Challenges and Benefits, Journal of Education and Learning; Volume 5, Number 3.

Australian defense force, (2001), ***Information Operations Planning Manual***

Caddell. Joseph (2004), deception 101: primer on deception, Army War College, Strategic Studies Institute

Cohen. Fred (2006), The Use of Deception Techniques: Honeypots and Decoys, **Handbook of Information Security**, Volume 3

Denning, Doherty (2004), Information Warfare and Security, Translators' Group, Tehran: Intelligent Signal Processing Research Institute. (In Persian).

Ebrahimi, Mansour (2007), **Psychological Operations and Strategic Deception**, Tehran: Abrar Moaser. (In Persian).

Erdie. Philip (2004), Network-Centric Strategic-Level Deception, Monterey, California. Naval Postgraduate School

Gerwehr. Scott, (2000), The Art of Darkness: Deception and Urban Operations

Godson. Roy (2000), *Strategic Denial and Deception***, International Journal of Intelligence and Counter Intelligence**, Volume 13, Number 4, 2000

Hutchinson. William (2006), Information Warfare and Deception, **Informing Science**, Volume 9

Latimer. Jon, (2001), Deception in war, John Murray, London

Libicki. Martin, (1999), ***The Changing Role of Information in Warfare***, "Strategic Appraisal: The Changing Role of Information in Warfare", Publisher: Rand Corporation.

Machiavelli, Niccolo (2013), **The Prince**, translated by Ahmad Zarkesh, Tehran: Pajhwok Publishing. (In Persian).

Monoro. James (2012), ***Deception***: ***Theory and Practice,*** Naval Postgraduate School

Namazi, Mohammad (2003), "The Role of Qualitative Research in the Humanities", Journal of Geography and Development, No. 1. (In Persian).

Podhorec. Milan (2011), ***Information Operations in the Command and Control Process at the Time of Their Planning***, Economics and Management of Faculty of Military Leadership in University of Defence.

Prunckun. Henry (2014), *Extending the Theoretical Structure of Intelligence to Counterintelligence***, Salus Journal**, Issue 2, Number 2.

Reid. Iain, 2020, Toward a holistic model of deception: Subject matter expert validation, Proceedings of the 53rd Hawaii International Conference on System Sciences

Stein. Georg (1996), Information Attack, Information Warfare in 2025, Air War College

Shulusky. Abram (2000), Elements of strategic denial and deception, **Trends in Organized Crime**, Volume 6, Number 1

Sharp, Walter (2006), Military Deception, Joint Chiefs of Staff.

Vandome. Roger (2010), From Intelligence to Influence: The Role of Information Operations, Centre for National Security Studies

Waltz. Edward, June (2000), Data Fusion in Offensive and Defensive Information Operations, National symposium of sensor and data fusion

Welch. Donald (1999), Strike Back: Offensive Actions in Information Warfare, United States Military Academy

Whaley. Barton (2008), Toward a general theory of deception, **Journal of Strategic Studies**, Volume 5, Issue 1

Woodcock. Alexander (1999), Information Operations in Support of Civil-Military Interactions, Conference Analysis of Civil-Military Interactions

Zand, Ebrahim (2017), **Generalities of Information Investigation**, Tehran: National Intelligence and Security Faculty Publications. (In Persian).

Zavidniak. Paul (1999), Achieving Information Resiliency, Information Technology Security Report, Volume 4, Number 3

Zolfaghari, Mehdi (2013), **Psychological Operations, Information Warfare and Strategic Deception**, Tehran: Imam Sadeq University Publications. (In Persian).