No.2/2023, APRIL-JUNE
https://doi.org/10.53477/2284-9378-23-26

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Intelligence support for the operational level counter-deception

Maj. George-Ion TOROI, Ph.D. Candidate*
Col. Cristian-Octavian STANCIU, Ph.D.**

*"Carol I" National Defence University, Bucharest, Romania
e-mail: george_toroi@yahoo.com
**"Carol I" National Defence University, Bucharest, Romania
e-mail: cristianstanciu73@yahoo.com

Abstract

Given modern warfare's complex and dynamic nature, military deception has become a vital tool in the contemporary operating environment for gaining strategic advantage and achieving operational success. For this reason, countering enemy deception operations has become an operational requirement to support mission accomplishment. Furthermore, with the increased use of modern technologies and information warfare tactics by adversaries, intelligence has become a critical asset in countering enemy deception operations and protecting the safety and security of military personnel and operations. The Russian-Ukrainian ongoing war has proven once again that deception remains a viable tool in the contemporary operating environment and can still have a huge impact on the battlefield. Considering its value, this article explores approaches to diminish and counter the impact of deception at the operational level of war. Moreover, our research explores how the joint function of intelligence can support the efforts of counter-deception throughout its entire process.

Keywords:

deception; counter-deception; information; detect; Russia; war.

Introduction

„*All warfare is based on deception*" is one of the oldest and well-known aphorisms in the military domain. History has proven countless times that, indeed, deception has been a critical aspect of warfare regardless of the period. By creating confusion and uncertainty in the enemy's mind, protecting friendly forces and assets, exploiting the enemy's vulnerabilities and weaknesses, and reducing friendly casualties, deceit has played a crucial role in ensuring operations success.

It has been proven by centuries of historical examples that military deception can provide numerous benefits to armed forces, including achieving surprise, disrupting the adversary's decision-making process, protecting critical information, enhancing operational security, and improving the effectiveness of military operations. For this reason, nowadays, regardless of the technological development of intelligence sensors, deception remains a powerful weapon in order to gain operational advantages on the battlefield. Nowadays, the majority of the western military doctrines still recognize its relevance: „*No major operations should be undertaken without planning and executing appropriate deceptive measures*". (AFM 2018, 3A-1)

The impression that possessing evolved collection assets can bring about full clarity on the operational situation is a false one. Not only is it erroneous, but it furthers amplifies the possibility for successful enemy deception by creating preconceived ideas, thus vulnerabilities for the enemy deceit to exploit.

The main reason why deception remains effective regardless of the sensors' evolution is simple: capitalizing on the vulnerable aspects of the psychological dimension of human nature is the main characteristic of misleading actions. Therefore, the enemy's mind is the target of these operations, and as long as the human brain is susceptible to error, the chances of a successful deception remain constant.

NATO recognizes deception as one of the military drivers in today's operating environment. „*Our adversaries will seek to present the Alliance with multiple dilemmas through deception and by sowing confusion across the continuum of competition*" (AJP-01 2022, 37). Furthermore, NATO members are extremely aware of their adversary's experience with respect to employing deception: „*Russia views deception (Maskirovka) to be a vital precursor to success*" (AFM 2018, 3A-4). However, in our humble opinion, NATO doctrine does not adequately address the subject in accordance with its importance. There is no dedicated NATO document to explore the counter-deception process, regardless of the level of war. Moreover, Allied Joint Doctrine for Operations Security and Deception, although relatively recently approved, in March 2020, dedicates only half of page to counter-deception. This being said, there is much room for improvement in the Alliance when it comes to addressing such a sensitive and important aspect of any military operation. This represents a crucial aspect at any

level of war, but more importantly at the operational level, where Joint HQs need to integrate effects and counter enemy actions in multiple operational domains.

Furthermore, although one of the functions of intelligence is to counter enemy deception operations and surprise (AJP-2 2020, 1-3), none of the NATO intelligence functional doctrine addresses this issue separately. There are indeed sporadic references to this in the NATO "Information" documents, but no coherent and logical approach to countering adversary deception can be found in any of these works.

In light of this, our research's primary question is the following:
- *How can intelligence joint function support the counter-deception process?*
For this reason, our article explores how intelligence can better support the counter-deception process and tries to raise awareness amongst NATO commanders and intelligence specialists with respect to the lack of doctrinal foundation on this subject. In addition, the present paper also offers a procedural framework as a solution to the identified problem, which should constitute the subject of future quantitative research to validate and develop it in order to apply it at the operational level of armed conflicts.

Based on the primary question stated before we developed several subsequent questions to help us solve the problem identified:
- *Is counter-deception a critical operational requirement considering the features of the contemporary operating environment?*
- *How should counter-deception work? What is the process of countering deception?*
- *What is the intelligence role in this process? How can intelligence joint function support the counter-deception process?*
In this respect, we divided the topic into several logical steps that should provide answers to the research questions.

First, we analyzed whether deception is still a valid operational concept in today's conflicts in order to see if efforts to develop a counter-deception doctrine are required. Furthermore, using a multidisciplinary analysis we provided some essential benefits of countering deception in support of military operations. Next, using the qualitative research methods of content and comparative analysis we performed a thorough introspection within NATO and some other Western nations' doctrines to see how counter-deception is addressed. Moreover, we made an analysis of their respective deception doctrine in order to develop countering methods to the essential deception concepts identified. Using an inductive method, we then reconstructed the conclusions obtained from the deception analysis into a counter-deception process.
In the end, based on the already recognized intelligence functions, using deduction, we depicted those specific intelligence-related activities that need to be performed within every phase of the counter-deception process.

1. Counter-deception – an essential operational requirement

The well-known aphorism presented at the opening of the introduction, „*all warfare is based on deception*", is attributed to Sun Tzu as part of his work, The Art of War. It represents a saying more than two millennia old and serves as a constant reminder that deception is a key component of war. By remaining unpredictable, it is often possible for one side to outsmart their opponents, even when chances are not favorable.

In order to gain an advantage over the enemy, military commanders have employed various forms of deception throughout history, such as misdirection, feints, or false information. As such, deception has been a part of warfare since ancient times and continues to play a significant role in modern conflicts. The multitude of successful examples is the main reason why Sun Tzu's aphorism has remained operationally viable for so long. Considering all of this, deception should be recognized as an integral part of the nature of war, and those engaged in military planning must be aware of its potential within the overall concept of operations.
Furthermore, nowadays, the operating environment, characterized by an abundance of information, rapid communication, global reach, technology dependency, or hybrid tactics, presents significant opportunities for deception operations to be carried out effectively.

At the same time, based on the technological development of intelligence sensors, as part of the contemporary environment, one might conclude that deceiving has become almost impossible. While, indeed, recent technological advancements in Intelligence, Surveillance, and Reconnaissance (ISR) capabilities have greatly enhanced military intelligence-gathering capabilities, it would be a mistake to assume that deception is no longer viable in modern warfare. Deception remains an effective tactic in military operations, especially when it is executed creatively and adaptively to exploit the cognitive weaknesses of the enemy.

In addition, it is important to underline that, while technological advancements have enabled military forces to collect and process vast amounts of data, this data is not always complete, accurate, or timely. Consequently, the resulting level of situational understanding is often truncated, which provides opportunities to mislead the opponent. Moreover, the increasing complexity of modern conflicts and the rapid pace of technological change mean that there will always be opportunities for deception to be used effectively.

Therefore, it is important for military commanders and intelligence analysts to recognize the ongoing threat posed by deception and to develop and implement effective counter-deception strategies. This requires a multi-disciplinary approach that integrates technological solutions, analytical expertise, and operational experience. Ultimately, by maintaining a clear-eyed understanding of the continuing

threat posed by deception, military forces can better prepare themselves to defend against and counter enemy deception operations.

Furthermore, the ongoing conflict between Russia and Ukraine has proven deception to be a key enabler for success on either side. At the operational level, the most conspicuous example might be considered the Kherson ruse employed by the Ukrainians in September 2022, as part of their counteroffensive. The rapid advancement and the vast territorial gains of the Ukrainians have proven deception to be a very effective shaping operation, regardless of the Russian ISR technological development.

Moreover, deception viability in the contemporary operating environment is demonstrated by the interest of Western actors in deception operations. Many of the important allies and NATO itself have recently developed doctrines that address this key enabler of modern operations. The table below highlights some of the doctrines and their release year in order to support our previous statement.

TABLE no. 1 Deception doctrines

Actor	Releasing year	Document
NATO	**2020**	***, AJP 3.10.2, *Allied Joint Doctrine for operations security and deception*, edition A, version 2, NATO Standardization Office
US	**2017**	***, JP 3-13.4, Military deception, US Joint Chiefs of Staff
US	**2019**	***, FM 3-13.4, *Army Support to Military Deception*, US Department of the Army
UK	**2018**	***, Army Field Manual - Warfighting Tactics Part 1: The Fundamentals, UK Ministry of Defence - *Annex A addresses the subject of deception*
ROU	**2021**	***, S.M.Ap. – 55, *Romanian deception doctrine*, Defense Staff, Bucharest

Additionally, deception represents a successful method that can bring a lot of benefits for the deceiver. It is a valuable tool for any military operation as it can create confusion, disrupt enemy plans, conceal intentions and capabilities, and ultimately increase the probability of success in achieving operational objectives.

Deception can be used to surprise the enemy by concealing intentions and operations, allowing military forces to gain the upper hand on the battlefield before the enemy can respond. It can also enhance security by misleading the enemy about the location and strength of military forces, protecting them from attack and preserving their combat power. Furthermore, deception can support creating opportunities for military forces to maneuver and operate freely in some operational areas by distracting the enemy's attention and effort. In addition, deceit might also be employed to conserve resources and minimize risk by fooling the enemy about the size and scope of military operations, allowing forces to achieve objectives with fewer resources and reducing the likelihood of casualties. All of these make deception a very valuable and sometimes cheaper tool for operational planners.

Furthermore, Russia, NATO's most significant threat, sees deception as a huge enabler of its operations. „The Russian Federation is the most significant and direct threat to Allies' security and to peace and stability in the Euro-Atlantic area" (NATO 2022, 4; JP3-13.4 2017). Russia is well-known for employing maskirovka within its military operations

Maskirovka is a Russian military doctrine that involves the use of deceit, camouflage, and concealment to support military objectives. It has been a central component of Russian military operations for many years and it is often used to confuse and mislead the enemy, protect Russian forces, and achieve operational objectives. Maskirovka can involve a range of tactics and techniques, including the use of decoys, false targets, disinformation, and psychological operations, among others. The goal of Maskirovka is to create uncertainty and confusion among the enemy, allowing Russian forces to gain the advantage and attain their objectives with minimal risk and cost.

Consequently, taking into account the above arguments, it becomes mandatory for all military forces to develop effective procedures to counter the deceptive actions carried out by their adversaries, so that the achievement of their own mission is not jeopardized. Furthermore, counter-deception can provide several benefits to military organizations:

- Maintaining operational security: Military counter-deception can maintain operational security (OPSEC) by detecting and neutralizing adversary deception operations. By identifying and countering adversary deceit, military organizations can prevent the adversary from exploiting vulnerabilities within its own concept of operations and protect the safety and security of military personnel and assets.
- Enhancing situational awareness: By identifying and exploiting the adversary deception, military organizations can gain insight into adversary capabilities, intentions, and activities, which can inform decision-making and enable operational advantages.
- Improving decision-making: Military counter-deception can improve decision-making by providing accurate and timely information about adversary capabilities, intentions, and activities. Based on the information obtained as a consequence of countering enemy deception, military organizations can reduce uncertainty and make informed decisions based on reliable information.
- Enhancing operational effectiveness: Military counter-deception can enhance operational effectiveness by neutralizing adversary deception operations and enabling military organizations to accomplish their mission with greater efficiency and effectiveness. It ensures maintaining the initiative and gaining the ability to dictate the course of events in accordance with its own concept of operations. Moreover, efficient counter-deception can create operational opportunities to double-cross the enemy, thus providing a more viable approach to solving the problem and fulfilling the mission.

It is obvious that military counter-deception can provide many benefits to the operational commander. Recognizing this, military organizations can enhance their ability to achieve operational success and protect the safety and security of military personnel and resources.

Considering the arguments provided in this section, it becomes evident that military counter-deception should be considered an essential operational requirement, as the use of deception by adversaries can pose significant threats to military operations and mission success. Effective counter-deception measures are necessary to detect, disrupt, and neutralize enemy deception efforts, thereby enabling military forces to maintain situational awareness, protect critical assets, and accomplish their objectives with greater efficiency and effectiveness. In this respect, developing a proper counter-deception framework becomes an operational necessity for any force.

2. Counter-deception process

As demonstrated before, counter-deception is a critical operational requirement in modern conflicts, given the significant role that deception plays in an operating environment characterized by features such as instant communication, information overload, and technology dependency. Effective counter-deception requires a multi-disciplinary approach, incorporating intelligence gathering, analysis, and dissemination, as well as specialized operations personnel and skills to exploit the opportunities that might arise from detecting the enemy's deceptive intentions. By developing and implementing a robust counter-deception process, military forces can better protect themselves against the negative impacts of enemy deception, and gain an operational advantage over the enemy.

First of all, in order to substantiate such a process, we consider it mandatory to understand the definition of counteracting the misleading actions of the adversary. To this end, „*counter-deception is an effort to detect, confirm, and subsequently negate, neutralize, or diminish the effects of, or gain advantage from, a foreign deception operation*" (JP3-13.4 2017, VII-1).

We would also like to point out that our analysis of this concept's definition has brought to light the conclusion that there is a great deal of synchronization in the Western way of thinking in relation to the definition of countering misrepresentation. Also, an in-depth examination of these approaches highlights the existence of three main phases of a potential counter-deception process: detection, confirmation, and exploitation, as outlined in the US military's deception doctrine (FM3-13.4 2019, A-1 – A-2). However, we consider it opportune, at this moment, to mention the fact that NATO does not address, in any of its doctrines, the process of countering deception, so the previously presented stages, specific to the American vision, are not implemented in the Alliance's documents.

Understanding the fundamentals of military deception is essential to developing effective countermeasures. It is impossible to neutralize the effects of any phenomenon if you do not develop a comprehensive understanding with respect to how it works. „*As the role of deception is expanding, the importance of implementing methods of countering deception is increasing. This requires a more thorough understanding of deception processes to implement counter-deception methods*" (Bennett and Waltz 2007, 2). Military deception is a complex and multifaceted concept that involves the use of a range of tactics and techniques to deceive the enemy. To effectively counter deception, military forces must first have a thorough understanding of the principles and fundamentals of deception, including the various types of deception, the methods, means and specific techniques. With this knowledge, military forces can develop effective counter-deception strategies that allow them to portray the benefits previously presented.

This was actually the procedure we used to develop our proposed process of counter-deception which enhances the one US uses and was previously presented. We do recognize the three phases the US process incorporates, but, in our opinion, to enhance the probability to counter enemy deception, military organizations should follow a five-phase process. We have added two more before the three US employs: counter-deception preparation and deception deterrence. The reason for including preparation is that it covers a set of activities that will enhance the probability of deception detection. Deterrence, on the other hand, helps forces to counter enemy deception by not portraying suitable conditions for them to make use of such methods. The process follows a logical flow, each phase playing a critical role in countering enemy deception.

The first phase, counter-deception preparation, involves developing and implementing measures to reduce the effectiveness of enemy deception. This phase includes an analysis of the enemy, the situation, and its own forces from the deception point of view. Identifying potential deception scenarios, the enemy's deceptive experience, but also its own vulnerabilities constitute some of the activities within this phase.

The second phase, deception deterrence, involves creating a credible deterrent to enemy deception. This phase includes planning special activities designed to make it difficult for the enemy to successfully execute their deception plans, thus determining them to give up own deceptive intentions. For example, NATO recognizes some suitable situations when there is a high probability to employ deception (AJP3.10.2 2020, 25). From a counter-deception perspective, not portraying to the enemy these operational situations on the battlefield can lead to the enemy not employing deception in their concept of operation, due to the increased risk it might imply.

The third phase, detection, involves identifying indicators that the enemy is attempting to deceive our friendly forces. This phase involves a substantial focus

on intelligence structures. In this sense, all subsequent processes of the information cycle contribute substantially to increasing the chances of identifying the adversary's deceptive actions. To this end, knowing one's own ISR capabilities, but also their limitations, as well as employing appropriate methods of analysis and processing of collected data is a "*sine qua non*" condition for the success of countering the adversary's deceptive actions at this stage of the process.

The fourth phase, deception confirmation, involves confirming all the details of the enemy's deception plan. Activities within this phase are of critical importance for exploiting the detection of enemy deceit. Without proper details regarding its plan, one cannot exploit the opportunity created by the detection phase.

The final phase, exploitation, involves using the information gathered during the previous phases to develop a double-cross plan. This phase includes exploiting the weaknesses in the enemy's deception plan and developing strategies to create operational battlefield advantages.

As a partial conclusion, we consider this counter-deception process an essential part of military operations. It provides a structured approach to countering enemy deception and ensuring the success of military missions. By following the five phases of the process, military organizations can effectively prepare, deter, detect, and exploit enemy deception to gain a decisive advantage on the battlefield. Further on, based on this process, we will identify how the joint intelligence function can support countering enemy deception operations.

3. A framework for intelligence support to counter-deception process

„*Deception is one of the biggest challenges in intelligence collection and processing. A well-organized attempt of deception by an adversary or any other actor may be difficult to reveal*" (AJP-2 2020, 2-13).

Therefore, deception poses significant challenges to the intelligence structures and processes. In intelligence operations, the collection of relevant data and its correct analysis and interpretation are essential in order to inform decision-makers and support the achievement of mission objectives. However, deceptive tactics employed by adversaries can undermine the accuracy and reliability of intelligence, making it difficult to distinguish between truth and falsehood. Deceptive practices can take many forms, including disinformation campaigns, false flag operations, and covert operations designed to mislead intelligence collectors. Such efforts can lead to the misinterpretation of data, false conclusions, and the allocation of resources based on incorrect assumptions. As such, intelligence professionals must remain vigilant to the potential for deception, and employ specialized tools and techniques to identify and neutralize deceptive tactics. This section represents general guidance

for intelligence structures in order to support each phase of the counter-deception process presented before to enhance the probability of its success.

3.1. Intelligence support to counter-deception preparation

As previously presented, preparation plays a huge role in the counter-deception process. The main role of the joint intelligence function in this phase is to provide updated information on the enemy and the situation in order to support the next steps of this process. The intelligence generated within this step is critical for the overall success of the counter-deception process. Much of this information should be obtained by the intelligence structure as part of the JIPOE (Joint Intelligence Preparation of the Operating Environment). The following are types of intelligence that should be generated within this phase:

- enemy mission, intent and distinct features of its operational art;
- enemy cultural and organizational factors;
- profiles of significant adversary decision-makers, including examinations of their professional backgrounds and experiences;
- enemy experience in deception operations;
- enemy doctrine and tactics specific for deception;
- limitations and capabilities with respect to deception;
- possible suitable situation for the enemy to employ deception;
- analyzing and identifying specific vulnerabilities with respect to our own information support process, including the elements specific to the preconceptions and prejudices of the personnel involved in this process and which can be exploited by the adversary.

3.2. Intelligence support for deception deterrence

Deterrence requires hiding elements essential for the enemy in order to develop successful deceptive plans. Establishing and implementing effective OPSEC measures are essential for the success of this phase. Although intelligence structures are not in the lead for this phase, they play an important part as they should provide information on the enemy's current knowledge of friendly disposition and intentions. Furthermore, during execution, the intelligence function should provide information on the operational situation and identify suitable situations in which the enemy may employ deception.

Moreover, intelligence support can be crucial in deterring deception, as it can provide early warning of potential deception attempts, enabling organizations to take proactive measures to deter or mitigate the effects of such efforts.

3.3. Intelligence support for deception detection

Deception detection requires, first of all, an understanding of the operational situation in order to separate true from false information out of the multitude of indicators that the enemy portrays on the battlefield. The level of understanding resulting from the collection and analysis of the information presented in the first stage of this process is a crucial factor in the effort to detect the deceptive actions of

the adversary. The motivation is extremely simple. The multitude of data collected during the operation is analyzed and interpreted in relation to the previous level of situational awareness. Cases that differ from the natural development of a regular adversary operational approach should constitute question marks for one's own intelligence structures regarding possible deceptive actions by the adversary. The identification of these incongruities is therefore the foundation by which the adversary's deceptive intent can be detected.

For these reasons, „*the detection of deception against friendly forces is a J2 responsibility*" (AJP3.10.2 2020, 5). Intelligence structures are the ones responsible for identifying specific indicators of enemy deception. An adequate intelligence cycle should be able to complete this task. However, there are several important recommendations that intelligence staff should apply:

- when it comes to identifying deceit, collection is not enough. It is important to have sensors that provide data, but, without proper processing, it is almost impossible to detect sophisticated deception operations;
- all collection capabilities have limitations and vulnerabilities that can be exploited by the enemy. If time permits, cross-checking data provided by multiple intelligence collection capabilities should be performed. „*While the level of detail in a single-source report could sometimes be sufficient to meet more immediate and narrowly defined requirements, all-source reporting is essential to gain in-depth understanding and avoid deception and misinformation*" (AJP-2 2020, 2-11);
- source reliability should always be analyzed;
- applying suitable structured analytical techniques has proven to be very useful in sorting out whether or not the deception is occurring (Moore 2015, 6);
- intelligence staff should always adopt a skeptical approach to all the collected data. There should be no shortages when it comes to analyzing these data;
- intelligence staff should always be aware of some barriers, either technical or human, such as cognitive limitations or personal biases and preconceptions;
- a very important aspect of detection is that intelligence resulted from processing data should always be compared to the one developed during the preparation phase in order to identify incongruities, which constitute the basis of deception detection.

3.4. Intelligence support to deception confirmation

Confirmation of the enemy's entire deception plan is essential to developing strategies to counter it. However, in order to choose the optimal option to capitalize on the opportunity created by detecting the adversary's deceptive indicators, it is necessary to develop a thorough understanding of his entire plan. Data must be collected on the scenario employed, methods and techniques, but also the level of progression and effectiveness of his plan so far. Equally, it is necessary to carry out an analysis of the effects created by misleading the adversary so far on our forces, but also of the effects that, according to the plan, it expects to achieve further on.

In order to be able to turn the situation into a vulnerability for the adversary, it is necessary to encourage his beliefs that his plan is working within the anticipated limits, and therefore correct knowledge of his future actions is a must.

The intelligence function should provide the necessary level of understanding in this regard. Identifying and prioritizing information requirements is of great importance to obtain essential data about the enemy's deception plan. In addition, it is important that this entire information cycle be extremely discreet so as not to give clues to the enemy that his plan has been debunked.

3.5. Intelligence support to exploitation

„*The response to the detection of deception against friendly forces is a command-led J3/5 responsibility*" (AJP3.10.2 2020, 5). Based on the situational understanding provided by the information processed in the earlier stages of this process, a series of options can be developed that the staff must analyze in relation to the established mission objectives and propose to the commander. „*Based on risks, commanders can ignore, expose, exploit, or defeat enemy deception efforts*" (FM3-13.4 2019, A-2). Regardless of the decision, intelligence can support any of the approaches.

Perhaps the most challenging option for information structures is the exploitation of the opportunity created. This essentially involves playing a double-deception on the adversary by developing plans that encourage his false belief with regards to the effectiveness of his actions, plans that, at the appropriate time, support achieving the operational surprise.

We consider it appropriate to emphasize again that the present process works in a logical and cascading progression, in such a way that the information developed in the early stages is essential for the success of the later ones. Therefore, in the case of this last stage of the counter-deception process, all previous data, especially those identified in the first and fourth stages, are extremely important in developing viable options for capitalizing on the operational situation created.

Conclusions

As a conclusion, it goes without saying that intelligence support to operational level counter-deception is a critical component of military operations. By identifying and countering enemy deception efforts, intelligence analysts can help ensure that military operations are successful and that personnel are kept safe. To this end, applying a structured framework to prepare, deter, detect, confirm, and exploit enemy deceit is mandatory.

One of the most prominent experts in the field of military deceit, Barton Whaley, came to the following conclusion in one of his studies: „*Indeed, this is a general*

finding of my study–that is, the deceiver is almost always successful regardless of the sophistication of his victim in the same art" (Whaley 1969, 76). For this reason, the need to come up with an effective counter-deception process is paramount. Furthermore, the scientific literature dedicated to deception acknowledges that *„the operational level commander is vulnerable to adversary deception and should formalize an internal systemic deception recognition process*" (McPherson 2010, 1). In this respect, the intelligence framework that we provided represents an effective approach to countering enemy deception operations.

Moreover, considering the evidence related to the employment of deceit in contemporary operating environment, this article intended to raise awareness within NATO with respect to the enemy employment of deception operation and the need to develop proper strategies to defend against these types of operations. Only with appropriate tools can the operational advantage so needed in modern conflicts be obtained, and the proposed process can represent one of these tools in terms of effectively countering the misleading actions of the adversary.

References

AFM. 2018. *Army Field Manual - Warfighting Tactics Part 1: The Fundamentals.* UK Ministry of Defence.

AJP-01. 2022. *Allied Joint Doctrine, Edition F, Version 1.* NATO Standardization Office.

AJP-2. 2020. *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security, edition B, version 1.* NATO Standardization Office.

AJP3.10.2. 2020. *Allied Joint Doctrine for operations security and deception,ediția A, versiunea a 2-a.* NATO Standardization Office.

Bennett, Michael, and Edward Waltz. 2007. *Counterdeception Principles and Applications for National Security.* London: Artech House.

FM3-13.4. 2019. *Army Support to Military Deception.* US Department of the Army.

JP3-13.4. 2017. *Military Deception.* US Joint Chiefs of Staff.

McPherson, Denver E. 2010. "Deception Recognition: Rethinking the Operational Commander's Approach." https://apps.dtic.mil/sti/pdfs/ADA535598.pdf.

Moore, David T. 2015. "A Short Primer on Deception and What to Do About It." *American Intelligence Journal, vol. 32, no. 2:* 3-12.

NATO. 2022. "NATO Strategic Concept." https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

Whaley, B. 1969. *Stratagem: Deception and Surprise in War.* Center for International Studies, Massachusetts Institute of Technology.