sciendo

Scientific Bulletin
Vol. XXIX, No. 1(57), 2024

ENHANCING OPERATIONAL PROTECTION: A STEP-BY-STEP COUNTER-DECEPTION GUIDE

George-Ion TOROI
george_toroi@yahoo.com
"CAROL I" NATIONAL DEFENSE UNIVERSITY, BUCHAREST, ROMANIA

ABSTRACT:

It has long been recognized that military deception is an effective strategy for confusing and disorientating adversaries, thereby creating favorable operational conditions for the deceiver. Moreover, the current characteristics of the operational environment provide the perfect landscape for such operations, enhancing the desired effects. In this context, dealing with such malicious actions can create serious dilemmas for the targeted forces. Under such circumstances, the development of a counter-deception tool to protect mission accomplishment becomes a must for any military organization. However, this requires a great deal of expertise and self-awareness. Today, more than ever, the ability to use timely and accurate information is the key to gaining decisive advantage on the battlefield. In this regard, countering the enemy's deception operations is an important contribution to this objective. Moreover, from a NATO and Romanian perspective, the Russian Federation's high level of expertise in this type of operations requires solutions to counter it. Nevertheless, there is a lack of research in this area in Western countries, which contributes to the creation of major vulnerabilities that potential adversaries could exploit. In this landscape, the article aims to provide solutions that enhance operational protection against such a scourge through a structured counter-deception process. Beginning with an analysis of deception doctrines to identify solutions to counter common identified themes, I have then reconstructed them into a specific process that is linked to the operational process.

KEYWORDS:

Analysis, counter-deception, deception, information, intelligence

1. Introduction

Access to reliable information seems to be more important than ever in the current information age, where our way of life has been drastically altered by extraordinary advances in technology. Thanks to social media, smartphones and the internet, it is now possible to manipulate opinions at a speed and to an extent that was unthinkable just a few decades ago. (Strategy for Operations in the Information Environment, 2023, 3; Davis, 2021, 16). In this context, information has become an essential resource for any actor (AJP-3.2, 2022, 47; Annual Threat Assessment of the US Intelligence Community, 2023, 26; ADP 3-13 Information, 2023, 1-1).

From a military point of view, achieving the desired objective depends on the ability of the armed forces to create operational conditions that allow them to control the flow of events, set the pace and stay one step ahead of the enemy. Achieving information and decision superiority on today's battlefield is more important than ever in meeting these requirements. But they can only be achieved in the context of an accurate situational awareness.

DOI: 10.2478/bsaft-2024-0019

© 2024 George-Ion Toroi. This work is licensed under the Creativ Commons Attribution-Non Commercial-No Derivatives 3.0 License.

Therefore, manipulating the enemy's understanding of the operating environment can provide the basis for gaining and maintaining the initiative over the enemy. Deception is one of the primary strategies that can be employed in this context. It involves influencing the adversary by disseminating misleading information that helps to create confusion and misperception, upon which the adversary makes detrimental decisions without realizing the seriousness of those actions. As such, it implies maneuvering the enemy's mind (Jasper, Puttonen, De Jong, Van der Zee & Rademaker, 2023, 1).

Nevertheless, deception is not new to modern conflicts. Throughout history, the use of stratagems, various subterfuges or tricks, cunning and deceptive techniques, has been an important and common aspect of armed conflict. History abounds in such examples (Latimer, 2015). For military leaders and strategists, they are an incredibly useful and accessible tool because of the many benefits they can bring. On the other hand, being deceived can have extremely negative effects on operations, placing the victim at a great disadvantage and possibly even costing the war.

It should be noted that the characteristics of today's operating environment intensify the effects that can be achieved by using certain deception methods, making them an integral part of contemporary military conflicts. The current crisis in Ukraine serves as an example of both the practical applicability and the benefits of using these strategies. Intelligence suggests that both the Russians and the Ukrainians have made extensive use of deception to defeat the enemy (Russian War Against Ukraine. Lessons Learned Curriculum Guide, 2023, 26-27).

Additionally, the Russian Federation, NATO's main adversary, as well as the Romanian armed forces, have a great deal of expertise in employing maskirovka, or deception, which they regard as a necessary prerequisite for effective military operations (AFM, 2018, 3A-4; Kofman, Fink, Gorenburg, Chesnut, Edmonds & Waller, 2021, 31).

As such, all of the above underline the need to develop and employ adequate tools to counter deception operations in an increasingly complex contemporary operating environment (TC 7-102, 2014, 1-2; Future Leadership, 2020, 1-2; JCN1/17, 2017, 1).

Though most international actors are aware of the high potential to encounter enemy deceptive tactics, their strategies to combat this problem are still relatively rudimentary (FM3-13.4, 2019, A-1; AJP3.10.2, 2020, 9). *"There is hardly an adequate theory of deception, much less a theory of counter-deception"* (Harris, 2013, 551). In this landscape, the research problem we have identified is that although deception has been around for as long as war and can be extremely harmful to the target, there is no known strategy to counter it. This issue is relevant because it exposes the armed forces to significant vulnerabilities that compromise their ability to provide the best possible operational protection and security framework.

2. Research methodology

In this context, the article strives to bridge this procedural gap by uncovering solutions that support countering adversary deception tactics specific to the current operational situation.

Therefore, the aim of my research was to develop an operational process that effectively counters adversary deception operations. In doing so, I intend to provide a methodical approach to this problem that will assist military planners and commanders in conducting combat operations. Therefore, I strongly believe that this study will help military formations to be better prepared for the demands of the modern operational environment and provide a higher level of operational security against potential adversary deception.

In this regard, the primary research question was the following: "How can adversary's deception operations be

countered?" In order to fulfill the overall aim of the study and provide suitable answers to the primary question, I have also developed 3 secondary questions:

SQ 1 – "Which are the relevant factors for a successful deception operation, and how can they be countered?"

SQ 2 – "How do officers of the Romanian Armed Forces perceive and understand the concept of countering deception?"

SQ 3 – "How do end-users assess the effectiveness of the proposed solution for countering deception, and what suggestions do they have for its refinement?"

To present the methodological choices carried out in this study, I have employed the well-known structural framework developed by Adrian Thornhill, Philip Lewis, & Mark N.K. Saunders, the research onion (Saunders, 2019, 130). The below figure depicts all of the methodological approaches employed within this study.



Figure no. 1: *Research methodological choices*
(Source: Author's compilation)

As one can notice, I have conducted cross-sectional qualitative research, using the interpretivism philosophy and an inductive approach. Moreover, the overall methodological strategy employed was the constructivist grounded theory, proposed by Charmaz (2014).

Considering this strategy, I have employed an iterative process of sampling, data collection and data analysis, constantly comparing the results obtained with previous data in order to develop the counter-deception process. I have obtained the level of theoretical saturation after three research phases:

RESEARCH PHASE 1 - Operational level counter-deception process development.

RESEARCH PHASE 2 - Operational level counter-deception process enhancement.

RESEARCH PHASE 3 - Operational level counter-deception process refinement.

I began the research process by examining the deception doctrines of four actors relevant to this study: Romania, NATO, the United States and the United Kingdom. The aim of this introspection was to find recurring themes in the methods used to study this phenomenon. Later, using the reverse brainstorming technique, I identified the factors that need to be taken into account in order to counter them. A first draft of the counter-deception process was then developed. All of these consisted the research phase 1. This approach is recognized as one of the proper ones when trying to develop suitable responses to enemy deceitful acts (Bennett, 2007, 2). The methodological approach for this phase can be depicted in Figure no. 2.

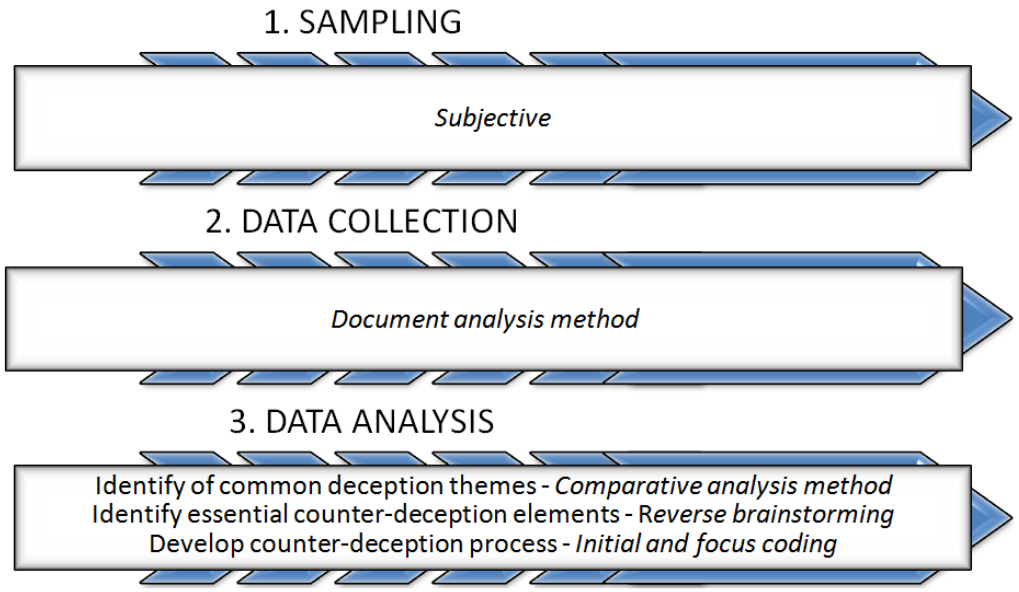

Figure no. 2: *RESEARCH PHASE 1 – Operational level counter-deception process development*
(Source: Author's compilation)

Next, in the second research phase, I improved the final product by using a questionnaire that illustrated the Romanian Army officers' understanding of the phenomenon of counter-deception. I followed the same procedure for data analysis as in the previous phase, coding the responses received and continuously comparing the data with the results of previous research. In this way, I was able to improve the counter-deception process. The methodological approach for this phase can be depicted in Figure no. 3.

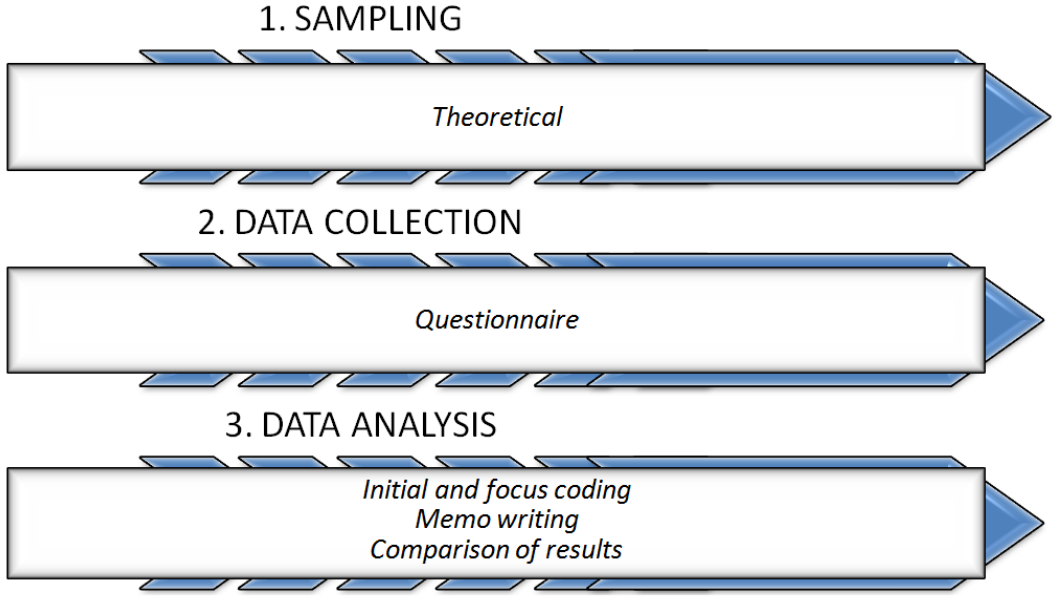

Figure no. 3: *RESEARCH PHASE 2 – Operational level counter-deception process enhancement*
(Source: Author's compilation)

The third and final phase of the study was conducted to find new components that could have improved the product and to evaluate the established procedure in a tactical scenario. To do this, I decided to use the Concept Development Assessment Game (also known as CDAG), a game that is one of NATO's techniques for improving new concepts. It involved six rounds of play correlated to the primary categories of the deception process previously developed. Upon completion of this step, I concluded that theoretical saturation had been reached, as I was unable to identify any critical components that would have improved the final product. The methodological approach for this phase can be depicted in Figure no. 4.

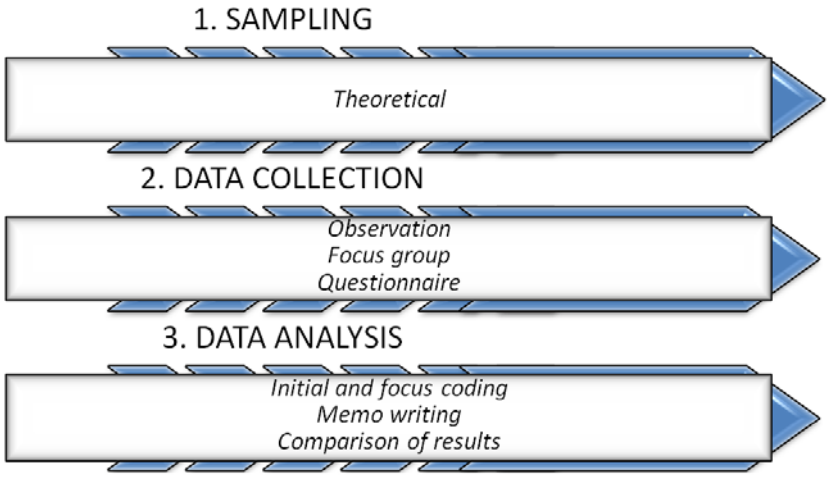

Figure no. 4: *RESEARCH PHASE 3 - Operational level counter-deception process refinement*
(Source: Author's compilation)

3. Counter-deception process

The final product of my study was a consolidated counter-deception process that could be applied within the overall operations process. It is a five distinct phases process, as shown in the figure below, each of them consisting of subsequent specific steps and activities. They all follow a logical progression and are dependent on the results of the previous phases. The process is built in accordance with previous research findings in the counter-deception field.

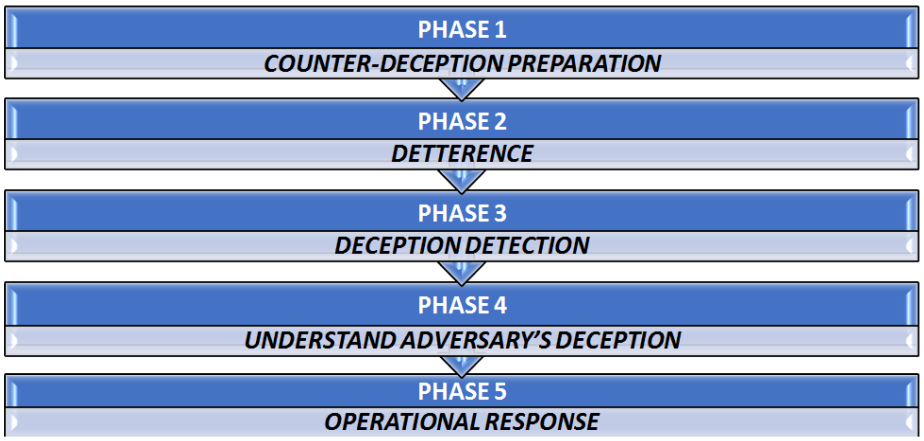

Figure no. 5: *Research findings – The counter-deception process*
(Source: Author's compilation)

The first phase of any effort to successfully counter an adversary's deception is the preparation of the counter-deception. It begins in advance, with the creation of targeted databases on possible adversaries and the identification and management of some of the weaknesses in one's own organization that could be used against one in a hypothetical conflict. Ongoing specialized training is another crucial component of the countermeasures included in this phase. At the same time, besides preparation, this phase is crucial for the fact that it develops an appropriate level of understanding that allows the comparison of operational situations at different points in the conflict in order to identify anomalies that could indicate enemy deception. It is recon that in the military domain *"understanding underpins everything that we do"* (Joint Doctrine Publication 04 – Understanding and Decision-making, 2016, 3). This phase is continuous, beginning in peacetime and ending with the cessation of hostilities and the end of fighting. The main steps of this phase can be detected in Figure no. 6.

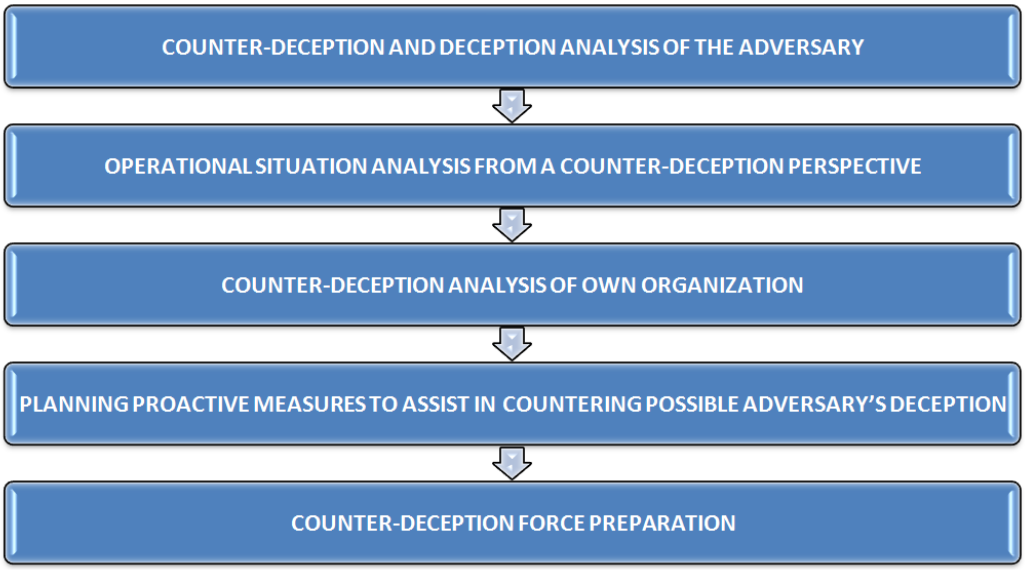

Figure no. 6: *PHASE 1 – COUNTER-DECEPTION PREPARATION*
(Source: Author's compilation)

The second phase represents an important pillar of this process, ensuring a proactive approach to reducing the likelihood that the adversary will resort to such deceptive methods in his operational design. The potential effects of such a phase may be at least twofold: it may cause the adversary to abandon the use of deception, or, if he does, it may significantly increase the level of risk to which he is exposed. Moreover, it is worth noting that the successful deterrence of the adversary will mean that the following phases of this process will no longer be necessary. One can therefore see the increased importance of this phase in achieving the overall goal of this process. By extrapolation, Sun Tzu's assessment that *"the supreme art of war is to subdue the enemy without fighting"* further highlights the importance of this phase in countering the opponent's deception operations. However, the end-state of this phase cannot be accomplished if proper understanding of the enemy and the situation do not occur within the previous one. The bellow figure highlights the main steps of this process phase.

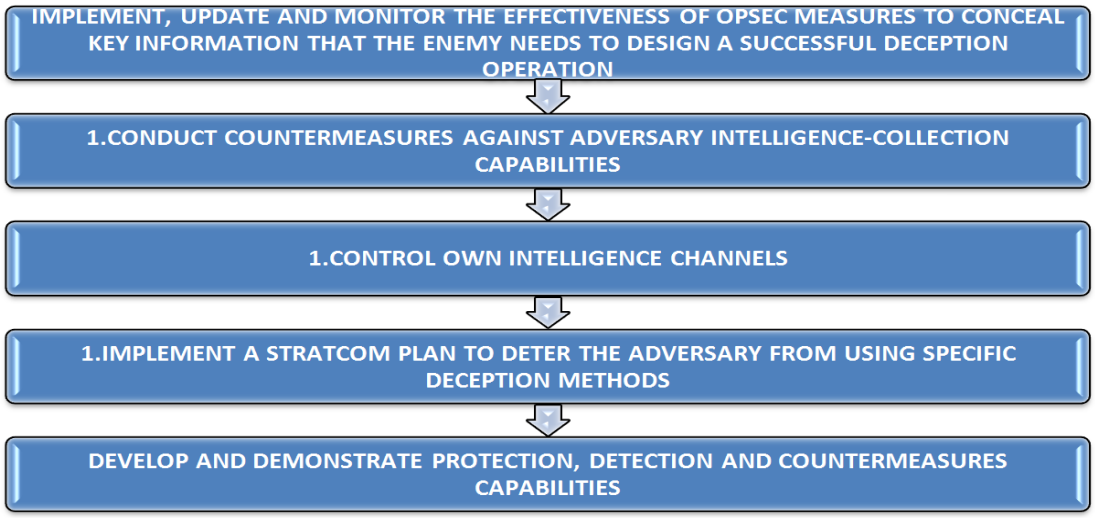

Figure no. 7: *PHASE 2 – DETTERENCE*
(Source: Author's compilation)

In the third phase, deception detection, intelligence structures play the most important role. To this end, their critical role is to find operational discrepancies. These result from a process of contrasting one's own expectations with the enemy's actions and overall understanding of the situation. One can see the importance of the counter-deception process previous phases for successful deception detection, as they develop the correct understanding of the enemy and the operational situation, and thus the expectations. The next step is to examine the discovered discrepancies to see if the deceptive actions of the enemy are the cause or if there are other factors at play. This is done by formulating and testing several hypotheses about these inconsistencies. If the testing confirms deception on the part of the opponent, then the following two phases come into play. However, the testing of hypotheses should be done in a way that does not alert the opponent to our findings. Figure no. 8 illustrates the specific stages of the deception detection phase of the counter-deception process.

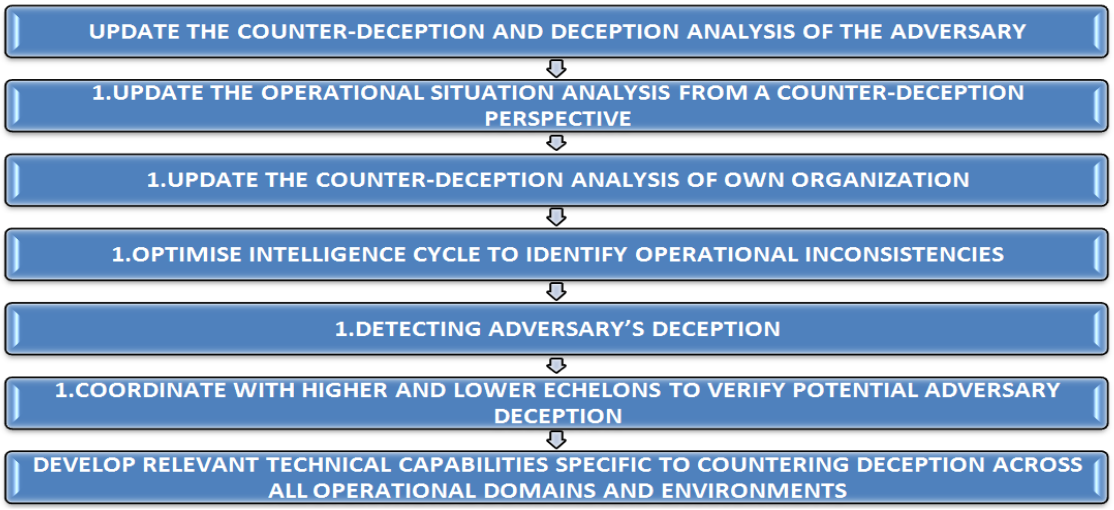

Figure no. 8: *PHASE 3 – DECEPTION DETECTION*
(Source: Author's compilation)

Once you have identified your opponent's deceiving aim, you need to understand its entire deception plan in order to take advantage of the situation. This is done throughout the fourth phase. This is crucial in setting the stage for the operational response. The better the understanding gained during the stages of this phase, the better the decisions made in the following phase. This fourth phase has two main functions. First, to identify the objectives of the adversary's deception operation, the perceptions he wants to convey, the scenario of his deceptive acts, the means, techniques and channels through which he disseminates false information. Second, activities specific to this phase should develop a proper understanding of the damage the enemy's deception operation has already done to one's own organization, forces, and mission. Fulfilment of these two tasks will serve as the basis for a correct understanding of the operational circumstances, enabling the selection of the most advantageous course of action. However, there are two important aspects to be considered in fulfilling these roles. Firstly, it is of paramount importance to continue to present observables that maintain the enemy's false perception of his successful deception. Secondly, the information required to take countermeasures should be carefully considered in relation to the time available. In this context, a time versus information analysis should be carried out. The more time spent gathering more information, the smaller the window of opportunity to successfully double-cross the opponent. This is a critical decision the commander should make during this phase. Figure no. 9 depicts the stages of this fourth phase of the counter-deception process.

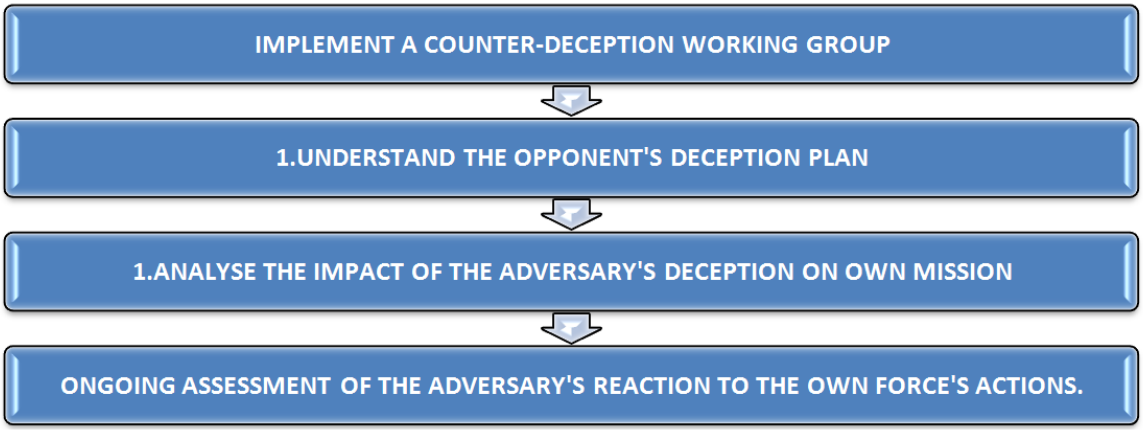

Figure no. 9: *PHASE 4 – UNDERSTAND ADVERSARY'S DECEPTION*
(Source: Author's compilation)

The fifth phase is dedicated to the operational response which builds on the findings of the preceding phase. *"The response to the detection of deception against friendly forces is a command-led J3/5 responsibility"* (AJP3.10.2, 2020, 5). During it, the Counter-Deception Working Group develops, analyses and compares potential response options and then recommends the best alternative to the commander based on predetermined criteria. The chosen course of action is then implemented and the results are continually assessed to determine whether the operation is moving towards the desired outcome. As in the previous phase, maintaining the enemy's misperception can contribute significantly to the effectiveness of the operational response. The specific stages of this phase are illustrated in the below figure.

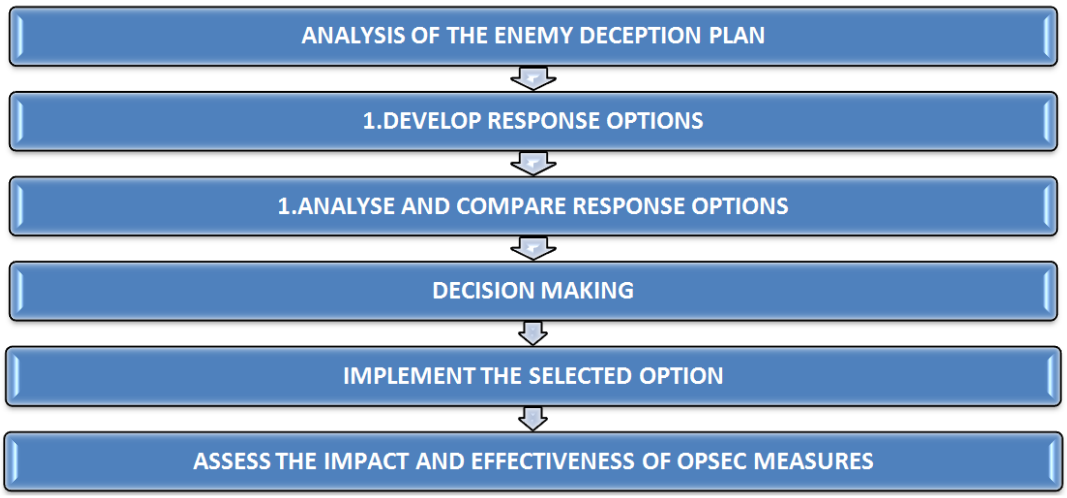

Figure no. 10: *PHASE 5 – OPERATIONAL RESPONSE*
(Source: Author's compilation)

This was the last phase of the counter-deception process. It is obvious that the process offers a holistic approach to countering misleading operations, contributing to the overall operational security of the military forces. In this regard, the process covers three critical functions for the contemporary operations success: protection, detection and action, as depicted in the bellow table. It is also worth mentioning that the process builds on previous researches and acknowledges the common themes within the counter-deception field.

Table no. 1

The relationship between the phases and functions of the counter-deception process

PHASE	FUNCTION
PHASE 1 – "COUNTER-DECEPTION PREPARATION"	Protection
PHASE 2 – "DETTERENCE"	
PHASE 3 – "DECEPTION DETECTION"	Detection
PHASE 4 – "UNDERSTAND ADVERSARY'S DECEPTION"	
PHASE 5 – "OPERATIONAL RESPONSE"	Action

(Source: Author's compilation)

4. Conclusion

In conclusion, against the backdrop of an increasingly complex confrontational environment, the ability to understand the situation correctly can offer considerable advantages for mission success. However, the challenges are numerous. The features of the information environment, such as its almost unrestricted accessibility, speed, and volume of transmission, have made it easier for anyone, anywhere in the world, to access information in real-time. However, the rapid technological advances we are currently experiencing have made it easier for hostile actors to exploit these features of the information environment for malicious purposes and to influence target audiences much more easily and on an unprecedented scale to achieve their goals. Deception is now one of the most commonly used methods. Therefore, anticipating, detecting and countering these tactics is critical to operational success. In this respect, I believe that the counter-deception process derived as a result of this study provides an appropriate tool in today's complex and uncertain operational environment.

REFERENCES

ADP 3-13 Information. (2023). Washington DC: US Department of the Army.

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

AJP3.10.2. (2020). *Allied Joint Doctrine for operations security and deception, edition A, version 2*. NATO Standardization Office.

AJP-3.2. (2022). *Allied Joint Doctrine for Land Operations, Edition B, Version 1*. NATO Standardization Office.

Annual Threat Assessment of the US Intelligence Community. (2023). Office of the Director of National Intelligence.

Bennett, M., & Waltz, E. (2007). *Counterdeception Principles and Applications for National Security*. London: Artech House.

Charmaz, K. (2014). *Constructing Grounded Theory, 2nd edition*. London: Sage Publications.

Davis, M.N. (2021). *Operations in the Information Environment: Achieving Decision Dominance.* School of Advanced Military Studies, US Army Command and General Staff College.

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

Future Leadership. (2020). Multinational Capability Development Campaign.

Harris, W.R. (2013). *Counter-deception Planning*. In *The Art and Science of Military Deception*, by Whaley, B. (ed.) Hy Rothstein. London: Artech House.

Jasper, L., Puttonen, S., De Jong, M., Van der Zee, S., & Rademaker, M. (2023). *Start with the End: Effect Measurement of Behavioural Influencing in Military Operations*. Hague: The Hague Centre for Strategic Studies.

JCN1/17. (2017). *Joint Concept Note (JCN) 1/17 Future Force Concept*. UK Ministry of Defence.

Joint Doctrine Publication 04 – Understanding and Decision-making. (2016). UK Ministry of Defence.

Kofman, M., Fink, A., Gorenburg, D., Chesnut, M., Edmonds, J., & Waller, J. (2021). *Russian Military Strategy: Core Tenets and Operational Concepts*. Virginia: US Center for Naval Analysis.

Latimer, J. (2015). *Deception in War*. London: Thistle Publishing.

Russian War Against Ukraine. *Lessons Learned Curriculum Guide.* (2023). Bruxelles: NATO Headquarters.

Saunders, M.N.K., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students, 8th edition*. Pearson Education.

Strategy for Operations in the Information Environment. (2023). Washington DC: US Department of Defence.

TC 7-102. (2014). *Training Circular No. 7-102 Operational Environment and Army learning*. Washington DC: Headquarters Department of the Army.