BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Resilience – effects multiplier in preparing counter-deception

LTC George-Ion TOROI, Ph.D.*
*"Carol I" National Defence University
e-mail: george_toroi@yahoo.com

Abstract

This article examines the critical role of resilience as an effect multiplier in the preparation and training of military personnel. By developing the ability to operate under uncertainty and take calculated risks, armed forces can reduce their vulnerability to manipulation and disinformation. The analysis focuses on ways to build resilience, emphasizing the importance of mental flexibility, adaptability, critical thinking, and thorough preparation for dynamic challenges. The study also highlights the need to integrate these skills into military training programs to produce leaders capable of making informed decisions even in the absence of all necessary information. The findings suggest that a resilience-based approach can significantly improve the ability to counter deception and thus contribute to the operational success of the armed forces.

Keywords:
resilience; deception; counter-deception preparation; critical thinking; adaptation.

Article info
Received: 30 July 2024; Revised: 27 August 2024; Accepted: 24 September 2024; Available online: 15 October 2024

Citation: Toroi, G.I. 2024. "Resilience – effects multiplier in preparing counter-deception".
Bulletin of "Carol I" National Defence University, 13(3): 178-192. https://doi.org/10.53477/2284-9378-24-38

In today's world of increasing complexity and rapid change, deception has become a fundamental strategic weapon used by adversaries for malicious purposes to destabilize and manipulate different audiences. The technological characteristics of today's environment provide more and more opportunities for deception, while at the same time enhancing the destructive impact of such actions. Against this backdrop, armed forces are increasingly challenged to identify and counter-tactics specific to manipulation and disinformation operations. In this context, the article argues for the importance of effective preparedness in countering adversary deception, with the development of military organizational resilience becoming an essential component in maintaining operational effectiveness and ensuring force and mission protection.

Resilience, defined as the ability to adapt and recover quickly in the face of challenges and change, serves as an effect multiplier in the readiness of military structures. It enables personnel to operate effectively under conditions of uncertainty and to make quick and calculated decisions, even in the absence of complete information. Rather than waiting for the perfect moment to act, resilient leaders are prepared to navigate the complexities of unpredictable situations and take well-calculated risks to achieve their objectives.

Problem statement

Although deception is a historically proven and highly effective method in armed conflicts, and, as I will show later in this paper, the current operational environment increases the possibilities of success of such actions, as well as the negative effects on the deceived, Western armed forces, including Romanian ones, do not take sufficient steps to protect themselves against such actions. Specific doctrines in this area are either non-existent or very limited. Even literature notes that "there is hardly an adequate theory of deception, much less a theory of counter-deception." (Harris 2013, 551) Moreover, NATO's potential adversaries, Russia and China, are extremely experienced in using such methods, as deception is deeply rooted in the specific modus operandi of their militaries. Thus, I believe that this landscape highlights some systemic vulnerabilities of Western military structures, exposing them to increased risks of being deceived. Thus, **the research problem** that prompted this paper is the lack of an agreed doctrinal framework for countering adversary deception.

Research aim

Within this framework, the present study aims to analyze the relationship between two concepts highly relevant to the current operational context: resilience and counter-deception, in the context of preparing force structures for the information challenges specific to the current operational environment. **The main objective of this work** was to determine whether and how resilience can support counter-deception preparation, thereby contributing to reducing vulnerability to manipulation and increasing the chances of protecting military forces and their missions in contemporary armed conflicts.

Research Methodology

The research was **qualitative** in nature, seeking to understand the nuances of the operational need for protection against adversary deception and the ways in which this should be achieved. It also sought to explore the specific ways in which resilience can ensure the amplification of effects realized in preparation for countering deception. In line with this kind of methodological approach, I used **inductive reasoning**, starting from the data collected and systematically analyzed towards a general conclusion (Creswell and Creswell 2023, 276).

The main research question of this study was: *How can resilience support the counter-deception preparation?* In this context, the following **research objectives** were pursued:

- To understand the operational relevance of countering deception in the current operational context.
- To explore how to counter adversary deception.
- To analyze and describe the role of preparedness in countering deception.
- To examine how resilience can support the process of counter-deception preparation.

Structure of the paper

In order to meet the research objectives, I have structured the paper in three parts. First, I carried out an analysis of the current operating environment in order to identify those aspects that determine the operational relevance of counter-deception. Then, based on the previous findings, I have set out the concrete countermeasures and the aspects related to the preparation of this process. Finally, I have examined the importance of resilience in the process of preparing to counter deception, highlighting the ways in which it can be a multiplier of the effects achieved in the process of protecting against the deceptive actions of the adversary.

The operational relevance of counter-deception

In an increasingly uncertain and complex operating environment, creating effects in the adversary's psychological dimension by shaping his perception of the operational reality tends to take on new valences in the strategies of international actors (MCDC 2020, 1-2; TC 7-102 2014, 1-2; JCN 1/17 2017, 1).

The high transparency of the operational space represents one of the major challenges in contemporary conflicts. It has become increasingly difficult to conceal military forces and actions nowadays. Moreover, in a conflict of attrition such as the one in Ukraine, where the ability to maintain a superior ratio of forces and assets for as long as possible may be the key to operational success, the need to find solutions to protect military forces and actions has become extremely urgent for armed forces. In this context, simulation and dissimulation, essential methods of deception,

have taken on new operational dimensions, ensuring gaining and maintaining the initiative on the battlefield, an essential principle of military operations.

While the sensor overload of today's battlespace might lead one to conclude that deception is no longer viable, the reality in Ukraine has demonstrated just the opposite (NATO Headquarters 2023, 27). Deceptive actions have become more relevant and essential than ever, ensuring that the conditions are in place to maintain operational capability at the highest possible level, while determining the adversary's resources to be wasted on false targets.

Yet, deception has been a constant of warfare, regardless of historical era (Freedman 2014, 3; Friedman 2017, 73). This could be considered one of the perennial features specific to the nature of armed conflict. The well-known aphorism that "all warfare is based on deception" has proven its validity countless times over the years. Achieving operational advantages over the adversary by manipulating his perception and influencing his behavior and actions is a practice as old as warfare (Pijpers and Ducheine 2023, 1; Friedman 2021, 113), deception being a critical tool in this regard (Ryan 2022, 102). The increased chances of misleading actions, as demonstrated by the longitudinal study of the well-known researcher in this field, Barton Whaley, increases the appeal of using such techniques in military operations (Whaley 2007, 76).

In addition, some features of the enduring nature of armed conflict, such as uncertainty and the human element of armed conflict, create an optimal framework for the use of deception. Uncertainty is a critical element in the success of deception operations, with the literature recognizing two broad types of deception in relation to it, Type A - ambiguity-producing deception and Type M - misleading deception. (Daniel, *et al.* 1980, 8; FM 3-13.4 2019, 1-6; JP 3-13.4 2017, I-9; MCTP 3-32F 2024, 2-9).

An equally important aspect of successful deception is related to exploiting the adversary's vulnerabilities, this type of operation being considered a cognitive process (Whaley and Busby 2002, 187). This emphasizes the importance of the human nature of conflict in deception. Furthermore, although rapid advances in technology have drastically changed our way of life, I believe that, at least for the foreseeable future, the human rather than the technological factor will remain the central element of armed conflict. For this reason, the viability of deceptive actions to exploit adversaries' perceptions and influence their decisions will remain a constant in warfare.

In addition, the characteristics of the current operating environment increase both the likelihood of success of misleading actions and their impact. We now live in a digital and information age, where society in all its aspects is becoming increasingly dependent on technology and information.

The military, as part of society, does not ignore these influences and trends. The rapid advances in information technology and the increasing need for data from multiple sources for decision-making create the conditions for organizational vulnerabilities that can be exploited by potential adversaries through deception (Hays 2020, 56). While emerging technologies such as artificial intelligence, big data, or machine learning can support improved decision-making, they also open the door to disinformation campaigns, cyber-attacks, or hostile information manipulation. It is recognized that "with the scientific and technological revolution we are witnessing today, artificial intelligence and other emerging technologies can increase the effectiveness of disinformation" (Beauchamp-Mustafaga 2023, 35).

The characteristics of today's information environment add to the potential for deception. The sheer volume of data that can be shared simultaneously, the multitude of channels through which information can be transmitted, and the speed with which this can be done, all create the conditions for successful disinformation campaigns (Boswinkel, *et al.* 2022, 5). Nowadays, the ability to influence public perception has become much greater. One easy way to do this is through social media networks. The explosive growth of these applications has revolutionized the way we interact with each other. However, due to the magnitude of the resulting effects, social media has become one of the most widely used channels for influencing attitudes and misleading people on a large scale.

The importance of this channel of communication is also demonstrated by the conflict in Ukraine, where social media platforms are flooded with posts on a daily basis. The ability to maneuver information and win the battle of narratives against the opponent is a constant in all modern conflicts. Supporting one's own population at home and allies abroad, as well as keeping troop morale high, are just some of the benefits that have been demonstrated by the information warfare being waged in Ukraine. Therefore, gaining and maintaining information superiority on the modern battlefield is a critical aspect of operational success (Black, *et al.* 2022, 24; AJP3.10.2 2020, 1). Deception as a means of exploiting information is one of the most widely used and necessary methods in this regard (Watling, Danylyuk and Reynolds 2024, 31), helping to manipulate the adversary's mind, shaping his perceptions, and degrading his understanding of the operational situation.

Complementary to this, a US study on the operating environment of future conflicts identifies a number of methods and technologies that can give a decisive advantage to those who are superior to the opponent. The study refers to these as "potential game changers through 2035", and one of these capabilities with great potential to influence the battlespace is that of deception (TRADOC Pamphlet 525-92 2019, 13).

Moreover, NATO's potential adversaries, and by extension Romania's, Russia and China, have extensive experience in the use of deception in conflict, and the concept is deeply embedded in the operational art of these actors (AFM 2018, 3A-4; Kofman,

et al. 2021, 31; Paul, *et al.* 2021, 22; Cliff 2023, 45).

One can therefore see the timeliness and importance of deception in the current operational context. Accordingly, countering such actions is a prerequisite for any military force in conflicts specific to the contemporary operating environment. The application of specific countermeasures can provide the necessary protection in the face of such a scourge, thus ensuring a decisive advantage over the adversary.

The counter-deception process and the role of deceptive preparatory activities

Counter-deception involves "identifying and countering the adversary's deceptive actions designed to undermine the will, understanding, and proper use of one's own forces' capabilities". (AJP3.10.2 2020, 9)

As noted in the introduction, there is no generally accepted theory for counter-deception. However, it can be seen that it involves more than simple detection and is recognized by some actors as a process involving at least three phases (FM 3-13.4 2019, A-1), which follow a logical progression, each dependent on the previous results:

- detecting the adversary's deceptive actions;
- confirming the adversary's deceptive actions;
- exploiting the adversary's deceptive actions.

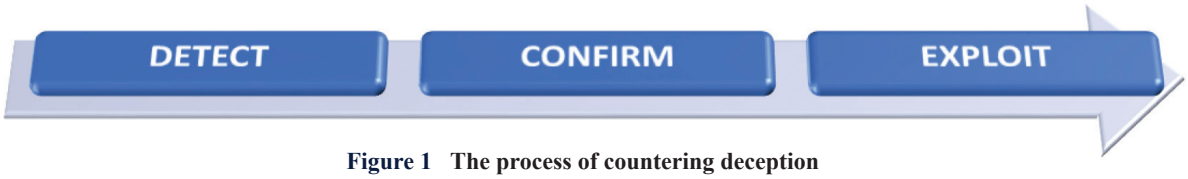

Figure 1 **The process of countering deception**
Source: author's conception

Detecting an adversary's deceptive actions involves identifying operational inconsistencies in the adversary's modus operandi, including suspicious gaps, contradictions with some previously adopted operational patterns, and confirmations that may seem dubious. However, given that "no imitation can be perfect unless it is the real thing" (Jones 1989), there should be clues to the detection of the adversary's deceptive indicators. In this respect, the reference system against which operational inconsistencies can be identified plays a crucial role. It is the degree of fidelity in understanding aspects of the adversary's modus operandi, the context of the operation, and the vulnerability of one's own forces to misleading elements that provide the reference system against which the adversary's deceptive actions can be identified.

Confirmation is the second phase of the counter-deception process and it aims to understand the adversary's overall deception plan, including the purpose, objectives, and scenario of the deception events. It is also necessary to identify the effects already produced by the adversary's actions up to the moment of detection. All this

information helps to make the best possible decision on the courses of action to be developed, thus ensuring a lower risk for the accomplishment of one's own mission. However, it is also necessary to take into account the time available to carry out the activities involved in this phase. There will certainly not be perfect conditions for decision-making. For this reason, it is necessary to analyze the level of information available and the possibility of losing the opportunity to exploit the detection of the adversary's deceptive intent.

The **exploitation** phase is designed to ensure that the opportunity created is capitalized on. In this phase, possible options are analyzed in terms of the benefits they could bring to the accomplishment of the force's original mission. For this reason, double-crossing the adversary, causing him to continue wasting resources on an ineffective deception plan, or publicly exposing the adversary's actions may be possible options to exploit. In all cases, however, the level of implicit risk should be analyzed and, if necessary, measures taken to mitigate it within the commander's risk tolerance. Developing as detailed a matrix as possible to support the decision and the alternatives to the plan can help streamline the implementation of the chosen option.

However, in order to increase the chances of success of the whole process, extensive preparation is required to counter deception. "A holistic analytical approach to fully effective counter-deception requires a trained mind and a trained organization. Achievable? Yes, but not easily." (Bennett and Waltz 2007, Introduction) For this reason, the present section aims to identify those indicators that can contribute to an organization's readiness to effectively counter deception, and then, building on the partial results obtained, I will show in the next section how resilience can contribute to making them a reality.

As mentioned above, **preparation** plays a critical role in successful countermeasures. It is recommended that it be initiated in peacetime to provide a greater chance of protection against the adversary's deceptive actions. It is extremely important because it provides the basis of knowledge and understanding against which operational inconsistencies in the adversary's modus operandi can be identified. Comparing what happens (reality) with what should have happened (expectations) can lead to the discovery of the adversary's deceptive intentions.
In addition, to maximize the effectiveness of counter-deception, preparation must also take into account elements specific to one's own forces that could be exploited by the adversary's actions, such as cultural aspects, prejudices and preconceptions, or different leadership styles.

In order to fulfill its purpose, therefore, preparedness must include activities aimed at both studying information about potential adversaries and one's own forces and creating the optimal conditions for applying the results of these analyses, as can be seen in the figure below. All this information will be materialized in the assessment of the adversary's potential deception. The degree of accuracy is of

paramount importance, as effective preparation creates the conditions for successful countermeasures.

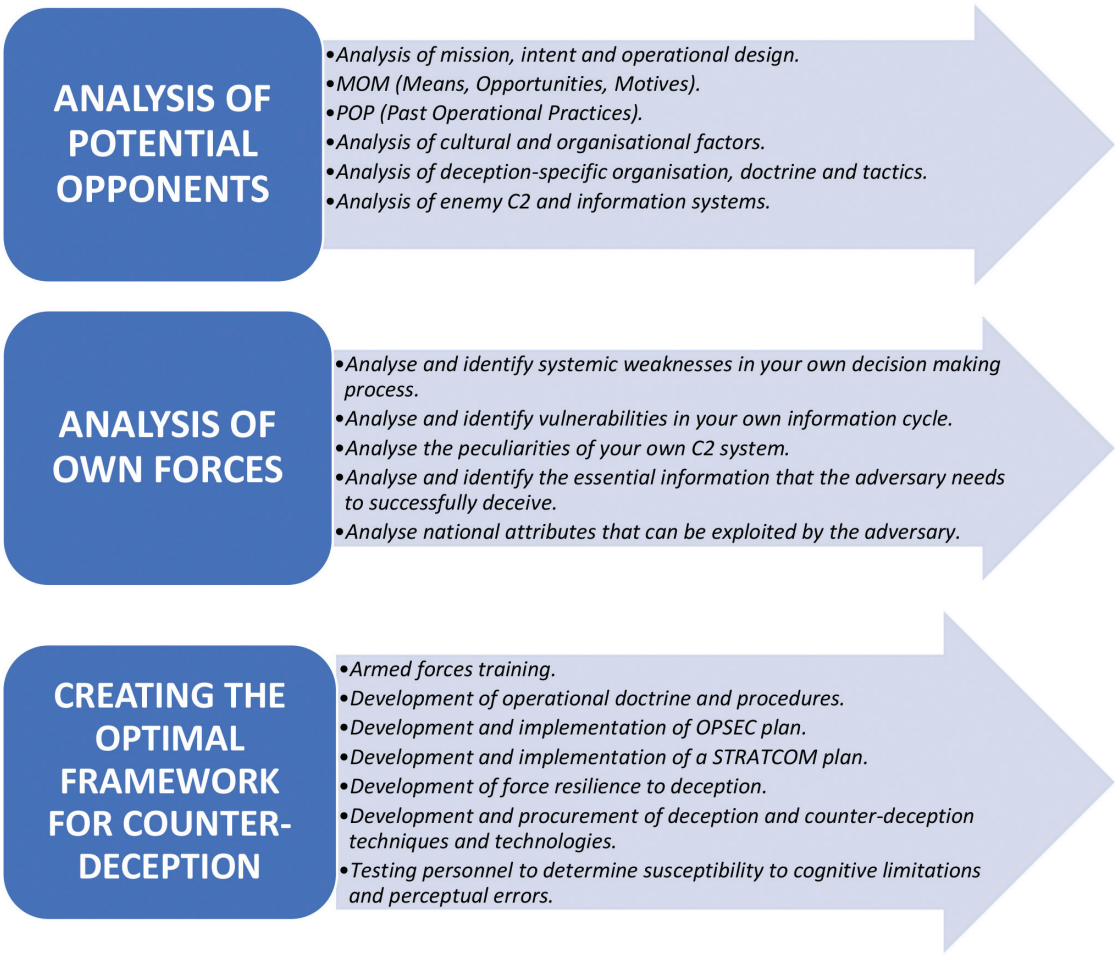

Figure 2 Preparing counter-deception
Source: author's conception

The power of resilience to support preparedness and counter misconceptions

The complexity of today's environment, the rapid pace of situational change, and increasing uncertainty make **the concept of resilience critical for any actor**. Resilience is the ability of a system to adapt and quickly return to a state of good functioning after significant difficulties or changes (Cambridge Dictionary 2024).

Romania's National Defence Strategy presents resilience as the appropriate response to threats specific to the current operating environment (Administrația Prezidențială 2020, 5). It also plays a very important role in the military domain, Romania's Military Strategy including it among the essential concepts on which its armed forces must focus (Strategia Militară a României 2021, 30).
At the Madrid Summit in 2022, NATO recognized the need to develop the resilience

of nations in the face of threats in the current security environment (NATO 2022). Military resilience underpins the Alliance's deterrence and defense by developing its ability to anticipate, prepare for, and adapt to threats, and to withstand, respond to, and recover rapidly from strategic shocks (E-ARC 2024). This concept is not new, however, and is deeply rooted in the nature of the Alliance. It was one of the pillars of its defense against the Soviet Union during the Cold War (Dowd and Cook 2022).

The US also understands the importance of this concept, which is considered essential to the accomplishment of the military mission (FM 6-22 2022, 4-16). In this regard, the US has created a directorate specifically for developing personal and organizational resilience (United States Army 2024). Resilience is also recognized as one of the qualities of effective military leaders (FM 6-22 2022, 4-16), understood as the ability to persevere and adapt in the face of adversity in today's highly dynamic and uncertain operating environment.

One of the disruptive factors in the conduct of military operations is deception. History has shown on countless occasions, as mentioned earlier, that deceived military structures have found it difficult to recover, and in most cases have had to give up the fight.

The primary purpose of deception, to induce the adversary to take certain actions that cause operational disadvantages without even realizing it, is perhaps the best argument for its inclusion among the elements that have the potential to cause operational difficulties.
For this reason, this section focuses on how resilience development can support the ability of military structures to both anticipate and detect deceptive adversary intentions and to ensure a resilient system capable of absorbing such shocks and recovering as quickly as possible without seriously compromising the accomplishment of its core mission.

Preparing the structure to respond effectively to an adversary's deceptive actions involves more than simply identifying indicators that can increase the likelihood of detection. It requires developing the military organization's ability to absorb shocks and move on. Thus, **the ability to be resilient to an adversary's deceptive actions is perhaps as important as countering them**, providing the opportunity for rapid regeneration of structure and adjustment of plans to overcome the adverse moment (Joint Doctrine Publication 02 2021, 3). In this way, the window of opportunity for the adversary to speculate on the possible operational advantage he has created is minimized, or even conditions can be created in which it may not materialize at all.
In addition, the Romanian Military Strategy identifies reduced resilience to disinformation as one of the challenges facing Romanian society (Strategia Militară a României 2021, 8), which further emphasizes the importance and relevance of introducing this activity in the training phase of military structures in order to counter the adversary's misleading actions. For these reasons, I believe that a

high level of resilience can mitigate the effects of the adversary's stratagems, thus contributing to the optimization of the overall strategy to counter the adversary's deceptive actions.

Complementary to this, developing the resilience of the military system can benefit the other activities specific to counter-intervention preparedness shown in Figure 2. First, an essential element of a resilient organization is **its flexibility and adaptability**. The high degree of adaptability of military systems can significantly reduce the impact of potential adversary missteps, thereby contributing to the effectiveness of the counter-deception process. Building a flexible force, both physically and especially mentally, must be a priority in the adaptive approach. The resulting mental flexibility directly supports the ability of those involved in the counter-deception process.

Flexibility and adaptability can create the conditions for identifying and reducing one's own vulnerability to potential deceptive actions. Critical analysis and awareness of one's own elements susceptible to deception directly contribute to increasing the level of resilience of the military structure in the face of potential deception attempts by the adversary. Given that the target of deception is the commander of the opposing forces, adaptation must sometimes include the ability to accept criticism, regardless of the position held. This is a matter of understanding one's own shortcomings and the desire to improve.

A critical element in building resilience is **education**. Nelson Mandela saw it as the most powerful weapon in changing the world. Education plays an essential role in both building resilience and increasing the chances of countering deception. First and foremost, education ensures an optimal level of awareness of potential threats. Adequate awareness of how deception works and its impact, but also the dangers to which superficial military structures are exposed, contributes directly to increasing both individual and organizational resilience, and also the preparation of counter-deception.

Education also contributes significantly to the development of critical and creative thinking among military personnel. The ability to correctly identify the real problems facing the organization, to analyze and determine their real and root causes, and to develop ingenious methods of solving them in a way that does not compromise the mission at hand, are characteristics of a critical and creative mind. These attributes are therefore *"sine qua non"* conditions for overcoming difficult moments on the battlefield. Critical and creative thinking can therefore be seen as a critical factor in shaping the resilience of any organization.

In this way, the conditions for preparing counter-deception are also ensured. In this way, staff with a developed critical sense, who are involved in this endeavor can ensure the premises for adequate results in terms of analyzing the adversary

and understanding the true nuances in terms of his intentions, motives, or modus operandi in similar situations. The ability to see things from other perspectives, to ask vital questions, to criticize one's own previous conclusions, to think openly, and to analyze existing assumptions in a relevant way, are characteristics of a person who has developed critical thinking skills in a refined and profound way, ensures the conditions for good preparation of counter-deception.

Ongoing **training**, by exercising its own structures under the most difficult conditions replicating contemporary battlefield situations, supports the development of the resilience of the military organization. Providing a training framework that incorporates potentially deceptive adversary situations of the highest possible complexity also enables the development of the structure's ability to counter and respond to such operational problems as effectively as possible. There is an unwritten trend within Western military structures towards military exercises. Most of them end with the success of the trained structure, which manages to resolve most of the situations created. Although I am aware of the moral benefits of such an approach, I believe that the armed forces should also encourage failure as a form of training. This, combined with a thorough analysis of its causes, may offer the chance to significantly increase the resilience of the armed forces. This is also in order to prevent misunderstandings. In addition, counterpart training (force against force) ensures a more realistic level of readiness for the armed structure. The possibility of fighting an adversary who is also thinking and planning to win increases operational uncertainty and requires a much greater intellectual effort from the personnel involved. Operating under such conditions leads the military to take calculated risks, rather than expecting optimal conditions for decision making. This creates the premises for more effective preparation of the military structure.

Another extremely important element in the development of military resilience is **leadership**, as mentioned above. It also plays a crucial role in countering deception. Commanders are the ones who set the training framework, select personnel, and identify the most appropriate positions for them, as well as set the internal pace and working environment, thereby influencing the moral component of their structure's combat power. A critical element for any leader is the desire for self-improvement, and in this sense the ability to recognize one's own limitations, the mistakes made in the act of leadership, as well as to accept one's personal prejudices and preconceptions, favor the development of resilience in the face of the opponent's deceptive actions. I can therefore conclude that leadership style has a direct impact on the performance of military personnel in countering deceptive behavior.
In Figure no. 3 I have illustrated how the specific elements of resilience provide the counter-deception preparation in order to highlight the factual way in which these two concepts are related.

Figure 3 Resilience support in counter-deception preparation
Source: author's conception

Conclusions

Resilience is the ability of an organization to adapt and recover quickly from significant challenges or changes. It is recognized by most actors as one of the solutions to the challenges of today's complex and highly volatile security environment. Its importance is also critical in the military domain, as it provides the conditions for an adequate response to the various threats and challenges of today's battlespace, thus creating the optimal framework for operational success.

Moreover, the characteristics of today's information environment make the ability to maneuver information and shape the desired perceptions of a target audience an extremely easy weapon for most modern armed forces. For this reason, preparing appropriate responses to the potential deceptive actions of adversaries must be a priority of any military structure in order to ensure a viable framework for accomplishing the assigned mission.

In this respect, resilience can be a critical factor in preparing forces to counter misdirected actions. In this endeavor, by developing and implementing effective resilience strategies, armed forces can secure multiple benefits. First, the increased level of critical and creative thinking that results from enhanced military resilience can facilitate deeper analysis of adversary information relevant to countering deception. Similarly, the development of organizational resilience can contribute to military-relevant outcomes by ensuring a more robust and adaptable structure against modern information challenges. In addition, increasing the level of training of the armed forces, another critical aspect of resilience will ensure that they are best prepared to counter deception.

In conclusion, I believe that by developing robust resilience, the Armed Forces will be better able to deal with the specific information challenges of the modern battlefield, thus preparing the organization to better counter potential adversary deceptive actions.

References

Administrația Prezidențială. 2020. Strategia Națională de Apărare a Țării pentru perioada 2020-2024. București. https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

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. https://assets.publishing.service.gov.uk/media/6422d0ba60a35e00120caf09/20230327-AJP_3_10_2_Ops_and_Deception-O.pdf.

Beauchamp-Mustafaga, Nathan. 2023. Chinese Next-Generation Psychological Warfare. Santa Monica, California, 2023: RAND Corporation.

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

Black, James, Alice Lynch, Kristian Gustafson, David Blagden, Pauline Paille, and Fiona Quimbre. 2022. Multi-Domain Integration in Defence Conceptual Approaches and Lessons from Russia, China, Iran and North Korea. Santa Monica, California: RAND Corporation.

Boswinkel, Lotje, Neill Bo Finlayson, John Michaelis, and Michel Rademaker. 2022. Weapons of mass influence Shaping attitudes, perceptions, and behaviours in today's information warfare. Hague: The Hague Centre for Strategic Studies, Haga.

Cambridge Dictionary. 2024. resilience. https://dictionary.cambridge.org/dictionary/english/resilience.

Cliff, Roger. 2023. China's Future Military Capabilities. US Army War College Press.

Creswell, John W., and J. David Creswell. 2023. Research design. Qualitative, Quantitative, and Mixed Methods Approaches. 6th Edition. Los Angeles: Sage Publications.

Daniel, Donald C., Katherine L. Herbig, William Reese, Richards J. Heuer, Theodore R. Sarbin, Paul H. Moose, and Ronald G. Sherwin. 1980. Multidisciplinary Perspectives on Military Deception. Monterey, California: US Department of the Navy, United States Naval Postgraduate School. https://apps.dtic.mil/sti/tr/pdf/ADA086194.pdf.

Dowd, Anna, and Cynthia Cook. 2022. Bolstering Collective Resilience in Europe. https://www.csis.org/analysis/bolstering-collective-resilience-europe.

E-ARC. 2024. NATO's Resilience Concerns. 29 February. https://e-arc.ro/2024/02/29/natos-resilience-concerns/.

FM 3-13.4. 2019. Army Support to Military Deception. Washington DC: US Department of the Army.

FM 6-22. 2022. Developing leaders. Washington: US Department of the Army. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36735-FM_6-22-000-WEB-1.pdf.

Freedman, Lawrence. 2014. Strategy: A History. Oxford: Oxford University Press.

Friedman, B.A. 2017. On Tactics. A theory of victory in battle. Annapolis: Naval Institute Press.

—. 2021. On operations. Operational art and military disciplines. Annapolis: Naval Institute Press.

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

JCN 1/17. 2017. Joint Concept Note (JCN) 1/17 Future Force Concept. UK Ministry of Defence. https://assets.publishing.service.gov.uk/media/657c3bb80467eb001355f8e2/ARCHIVE_FFC_JCN1_17-O.pdf.

Joint Doctrine Publication 02. 2021. UK Operations: the Defence Contribution to Resilience. 4th Edition. London: UK Ministry of Defence. https://assets.publishing.service.gov.uk/media/6384a153e90e0778a511ab69/20221128-JDP_02_Web.pdf.

Jones, Reginald Victor. 1989. Reflections on Intelligence. London: Mandarin Paperbacks.

JP 3-13.4. 2017. Military Deception. US Joint Chiefs of Staff. https://irp.fas.org/doddir/dod/jp3_13_4.pdf.

Kofman, Michael, Anya Fink, Dmitry Gorenburg, Mary Chesnut, Jeffrey Edmonds, and Julian Waller. 2021. Russian Military Strategy: Core Tenets and Operational Concepts. Virginia: US Center for Naval Analysis.

Lieutenant Colonel Michael G. Hays. 2020. „Convergence of Military Deception in Support of Multi-Domain Operations." În Theater Army in Multi-Domain Operations Integrated Research Project, de Gregory L. Cantwell, 55-86. US Army War College.

MCDC. 2020. Future Leadership. Multinational Capability Development Campaign. https://assets.publishing.service.gov.uk/media/5fdccd0de90e07452ec36ee8/20201210-MCDC_Future_Leadership-web.pdf.

MCTP 3-32F. 2024. Deception. US Marine Corps. https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/3815472/mctp-3-32f/.

NATO Headquarters. 2023. Russian War Against Ukraine. Lessons Learned Curriculum Guide. Bruxelles. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/12/pdf/231208-RusWar-Ukraine-Lessons-Curriculum.pdf.

NATO. 2022. Madrid Summit Declaration. 29 June. https://www.nato.int/cps/en/natohq/official_texts_196951.htm.

Paul, Chistopher, James Dobbins, Scott W. Harold, Howard J. Shatz, Rand Waltzman, and Lauren Skrabala. 2021. A Guide to Extreme Competition with China. Santa Monica, California: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1378-1.html.

Pijpers, Peter B.M.J., and Paul A.L. Ducheine. 2023. Deception as the Way of Warfare. Armed Forces, Influence Operations and the Cyberspace paradox,. Hague: The Hague Centre for Strategic Studies. https://hcss.nl/wp-content/uploads/2023/05/01-Ducheine_Pijpers_Deception-as-the-way-of-warfare.pdf.

Ryan, Mick. 2022. War Transformed. The Future of Twenty-First-Century Great Power Competition and Conflict. Annapolis, Maryland: US Naval Institute Press.

Strategia Militară a României. 2021. Capacitate defensivă credibilă, pentru o Românie sigură, într-o lume marcată de noi provocări. București: Ministerul Apărării Naționale.

TC 7-102. 2014. Training Circular No. 7-102 Operational Environment and Army learning. Washington DC: Headquarters Department of the Army. https://odin.tradoc.army.mil/TC/042214e84da40544fdc66cd82d41f941.

TRADOC Pamphlet 525-92. 2019. The Operational Environment and the Changing Character of Warfare. Washington DC: U.S. Army Training and Doctrine Command. https://adminpubs.tradoc.army.mil/pamphlets/TP525-92.pdf.

United States Army. 2024. Directorate of Prevention, Resilience and Readiness. https://www.armyresilience.army.mil/index.html.

Watling, Jack, Oleksandr V Danylyuk, and Nick Reynolds. 2024. Preliminary Lessons from Ukraine's Offensive Operations, 2022–23. London: Royal United Services Institute.

Whaley, Barton. 2007. Stratagem: Deception and Surprise in War. London: Artech House.

Whaley, Barton, and Jeffrey Busby. 2002. "Detecting deception: Practice, Practitioners, and Theory." In Strategic Denial and Deception: The Twenty-First Century Challenge, by James J. Wirtz, (ed), Roy Godson. Transaction Publishers.