sciendo
Scientific Bulletin
Vol. XXIX, No. 2(58), 2024

DISSECTING DECEPTION OPERATIONS. A LONGITUDINAL ANALYSIS

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

ABSTRACT

As the ongoing conflict in Ukraine demonstrates, deception tactics remain a critical component of military plans, especially on the modern battlefield, which is rich in sensors and information from multiple sources. As it is harder to conceal forces and prevent detection, armed forces must concentrate on hiding their intentions in order to gain surprise and preserve weaknesses. In this endeavour, deception continues to be essential. But in a time of ubiquitous information and rapid technological advancement, successful deception has become more challenging, but also more critical than ever. Through a qualitative analysis, the study seeks to offer a deeper comprehension of its underlying mechanisms in this particular context. This longitudinal research examines a variety of written sources after the 2nd World War until today to identify common topics in planning and executing successful deception operations in order to overcome the challenges of today's transparent battlefield.

KEYWORDS:

Deception, information, perception, operational advantage, critical thinking

1. Introduction

As we remember the 80th anniversary of D-Day's triumph on Normandy's beaches, we think about the key tricks that helped the Allies win and finish World War II in Europe. This great moment in history reminds us of the importance of outsmarting the enemy in war. In an extremely complex and confusing world, as the one we live in, armies are rediscovering deception as a useful tool to gain the upper hand over their opponents in contemporary conflicts.

Deception has always been an integral part of warfare and one of the most powerful tools employed in it (Friedman, 2017, p. 73). From the ancient ruse of the Trojan Horse to the recent 2022 Ukrainian counteroffensive in Kharkiv, military leaders have always relied on trickery to outsmart their opponents. Deceptive tactics can help demoralizing the enemy and creating potential opportunities often tipping the odds in the deceiver's favour. Deception, regardless of its form, whether of false withdrawals or disinformation campaigns, is a sign of the ingenuity that characterise successful military operations. Deception is used in almost every military action, demonstrating its enduring importance within the art of warfare. One might even inquire that the multitude and ever presence of deception throughout history make it an attribute of the constant nature of war.

Although there are some currents that suggest the impossibility of deception in 21st century military operations, given the high transparency of the battlefield and the multitude of sensors for surveillance and intelligence collection, the Russian-Ukrainian war proved the opposite (NATO, 2023, p. 27). The most notable case occurred in the autumn of 2022, when, as part of the counter-offensive to retake territory in the Kharkiv region, the Ukrainians were able to convince the Russians to move most of their forces to the southern front in the Kherson region, based on false indicators of a Ukrainian attack in this region. This action made it possible for the Ukrainians to recapture around 3000 km2 in the Kharkov region (Santelises, 2022).

DOI: 10.2478/bsaft-2024-0032

It is recognized that in today's increasingly transparent operating environment, which has arisen as a result of accelerated technological developments in intelligence collection sensors, deception can provide the solution to stay one step ahead of the adversary and create operational advantages that will cause the adversary to become reactive, thus ensuring the preconditions for military success (Anderson, 2022, p. 38). It takes more than just being able to observe the battlefield to fully understand the operating environment (Ryan, 2024).

2. Research methodology

2.1. Problem statement

Although history is replete with successful examples of deception, interest in this field has decreased since the beginning of the third millennium. Many of the current writings refer to deception as a lost art, demonstrating that the level of research interest in this area has indeed declined, even though the benefits that such actions can provide in achieving the proposed objectives have always been substantial.

The establishment of a unipolar power system with the collapse of the Soviet Union and the transformation of the typology of military conflicts towards stability operations, against the backdrop of the challenges of the operating environment at the time, contributed to this. On the one hand, the ability of the United States and Western countries in general to shape the course of international relations and, on the other, their technological superiority in the conflicts in which they were involved meant that deception was no longer a significant element in supporting operations. Against this background, the expertise of many Western states in the effective planning and execution of such actions has declined significantly (IISS, 2022, p. 40).

However, "*the return of great power competition against peer adversaries with advanced A2AD capabilities requires a refocus on the employment of military deception*" (Hays, 2020, p. 56). Due to the evolution of today's world towards a multipolar one, as well as the features of today's information environment, the use of deception operations has once again become of crucial interest to the military. It is recognised that deception can be an essential force multiplier for military commanders to gain and maintain operational advantage in today's multi-domain environment. The increased complexity and volatility of the current operating environment (MCDC Future Leadership, 2020, p. 1-2), with the emergence of new operational domains, cyber and space, creates a favourable environment to use deception amidst increasing uncertainty.

Many of the Western actors have recognised this and have taken serious steps to relearn the lost art of deception, their recent publication of doctrines acknowledging this growing interest in understanding deception and how it can enhance operational effectiveness in today's conflicts.

2.2. Research aim and question

In this context, my study's research goal was to identify the mechanisms of deception operations by uncovering recurring patterns in the body of literature that has been written since the Second World War. By examining a wide range of sources, the study sought to understand the fundamental theories that underpin successful deception operations. The study concentrated on important components such the preparation and execution of deception, the significance of noise management, the impact of timing and risk, and the utilisation of diverse channels and ways to send misleading signals. The aim of the research was to give military commanders and planners a useful tool for both present and future operations by delivering a deeper understanding of the mechanisms of military deception.

Against this background, the main research question that guided this study was: *Which are the common themes within*

the existing literature that underpin successful military deception?

I would like to highlight that this analysis strictly focuses only on legal forms of deception within the context of military operations. *"Provided it is not perfidious or otherwise prohibited by law or policy, deception is a legitimate military activity and is a ruse of war"* (AJP3.10.2, 2020, p. 1). I was completely aware that while deception can be a legitimate tool in operations planning to mislead adversaries, perfidious acts, such as feigning surrender or civilian status to gain a tactical advantage, are illegal and condemned under the law of armed conflict. In this regard, the article deliberately excluded such tactics, addressing only legally accepted aspects of deception that are recognized within the military doctrines of important actors such as NATO or the US.

2.3. Research design

To this end, I employed **qualitative research** to understand the profound implications and mechanisms of deception within military operations. Complementing this, I used an **inductive reasoning** to generate general conclusions about employing deception, derived from the empirical analysis of the data (Given, 2008, p. 429; Creswell & Creswell, 2023, p. 276). Through the qualitative **longitudinal analysis**, insights were gained into how deception has been effectively implemented in different historical contexts, thereby contributing to a deeper understanding of its nuances.

In this regard, I employed **secondary data** to identify the recurrent themes within the existing deception literature, using the **document analysis method to collect this data**. Secondary data are recognized for their value within research studies, as it allows researchers to draw insights from previously collected and analysed information, providing a rich context for the current study (Walliman, 2022, p. 102). This approach enabled a comprehensive examination of relevant historical and contemporary sources, facilitating the identification of consistent themes in military deception operations.

Although deception has been an integral part of military operations throughout history, and most military theorists such as Sun Tzu, Niccolò Machiavelli, Carl von Clausewitz, Antoine-Henri Jomini, J.F.C. Fuller, B.H. Liddell Hart, and John Boyd have emphasized its importance for the outcome of armed conflicts, the in-depth analysis of the field and its implications for military operations truly began after World War II. The manner in which this global conflict unfolded underscored the need for deception as an essential element of military strategy, with many confrontations during the war involving significant elements of deceiving the adversary.

Thus, to accomplish the research aim, my analysis covered relevant research papers written from the post-World War II period to the present day. The table below highlights the studies used to derive the common deception themes. I organized this paper in a chronological manner to be more easily exploited. In addition to research papers, I also employed specialized military doctrines. Despite not being peer-reviewed, these doctrines are highly valuable as they represent the philosophy of warfare of the analysed actors. One of the values of this paper lies in the comprehensive list of pivotal post-World War II studies on deception operations that might be found in Table no. 1.

Table no. 1
Deception literature

No.	Year	Paper
1.	**1969**	**Barton Whaley** - *Stratagem: Deception and Surprise in War* (Whaley, Stratagem: Deception and Surprise in War, 1969)
2.	**1980**	**Donald C. Daniel, Katherine L. Herbig, William Reese, Richards J. Heuer, Theodore R. Sarbin, Paul Moose, Ronald G. Sherwin** – *Multidisciplinary Perspectives on Strategic Deception* (Daniel & Herbig, 1980)
3.	**1980**	*Deception Maxims: Fact and Folclor* (Governmentattic.org, 1980)
4.	**1982**	**J. Bowyer Bell, Barton Whaley** – *Cheating and deception* (Bowyer Bell & Whaley, 1982)
5.	**1987**	**Michael I. Handel (ed.) –** *Strategic and Operational Deception in the Second World War* (Handel, 1987)
6.	**1989**	**Michael Dewar** – *The Art of Deception in Warfare* (Dewar, 1989)
7.	**1997**	**Mark Lloyd** – *The Art of Military Deception* (Lloyd, 1997)
8.	**1999**	**Richards J. Heuer** – *Psychology of Intelligence Analysis* (Heuer, 1999)
9.	**2002**	**Godson, R., and J. Wirtz (ed) -** *Strategic Denial and Deception: The Twenty-First Century Challenge* (Godson, 2002)
10.	**2007**	**Michael Bennett, Edward Waltz -** *Counterdeception Principles and Applications for National Security* (Bennett & Waltz, 2007)
11.	**2012**	**James D. Monroe –** *Deception: Theory and Practice* (Monroe, 2012)
12.	**2013**	**Hy Rothstein, Barton Whaley (ed.) –** *The Art and Science of Military Deception* (Rothstein & Whaley, 2013)
13.	**2015**	*American Intelligence Journal – Vol. 32, Issue 2, Denial and Deception* (JSTOR, 2015)
14.	**2016**	**Barton Whaley –** *Practice to deceive* (Whaley, Practice to deceive, 2016)
15.	**2018**	**Christopher M. Rein (ed.) –** *Weaving the Tangled Web. Military Deception in Large-Scale Combat Operations* (Rein, 2018)
16.	**2019**	**Robert M. Clark, William L. Mitchell –** *Deception, Counterdeception and Counterintelligence* (Clark & Mitchell, 2019)
17.	**2019**	*FM 3-13.4 Army Support to Military Deception* (FM 3-13.4, 2019)
18.	**2020**	**Justin J. Green –** *The Fifth Masquerade: An Integration Experiment of Military Deception Theory and the Emergent Cyber Domain* (Green, 2020)
19.	**2020**	**Albert Johan Hendrik Bouwmeester -** *'Krym Nash': An Analysis of Modern Russian Deception Warfare* (Bouwmeester, 2020)
20.	**2020**	**Michael G. Hays -** *Convergence of Military Deception in Support of Multi-Domain Operations* (Lieutenant Colonel Michael G. Hays, 2020)
21.	**2020**	*AJP-3.10.2 Allied Joint Doctrine for operations security and deception* (AJP-3.10.2, 2020)
22.	**2024**	*MCTP 3-32F Deception* (MCTP 3-32F Deception, 2024)

After the selection and collection process of key studies, the second phase of my research was the **data analysis and interpretation**. To this end, I employed the **comparative analysis and thematic analysis** methods to identify the recurrent deception themes in the literature analysed, both of which recognized for their value

within qualitative researches (Howitt, 2019, p. 148; Given, 2008, p. 100). On one hand, the comparative analysis allowed me to examine the differences and similarities across these studies, while thematic analysis, on the other hand, enabled me to systematically identify, organize, and offer insights into patterns and themes within the collected data.

3. Results

The purpose of this chapter is to present the main findings of the research. As a consequence of analysing the collected data, I have discovered several themes that I grouped within two broader categories: the definition and the process of deception, this chapter being organized accordingly. These findings provide a deeper understanding into the crucial need for deception operations within today's transparent and fluid battlefield.

3.1. Defining deception

The first theme I have identified is related to the understanding of the term deception. In this regard, the table below highlights the common themes in the literature regarding the definition of deception.

Table no. 2

Defining deception – common themes

DEFINING DECEPTION (Common themes)	- the **aim** is to mislead the adversary by creating a false perception of the operational situation; - the **deception target** is the adversary's decision-maker; - deception must create **operational advantages** for the initiator - deception involves eliciting a **behavioural response** from the adversary

It is worth noting that military deception, while integral to any operation, is governed by clear legal boundaries as set by Protocol I of the Geneva Conventions, particularly in Article 37 (Additional Protocol no. 1 to Geneva Conventions, 1977, p. 13). This article differentiates between lawful "stratagems of war" and unlawful "perfidy", ensuring that deception does not violate the principles of international humanitarian law.

Unlawful deception activities violate the law of war by undermining protections and breaching trust with the enemy. Perfidy, or acts that invite an enemy's confidence in protection under the law of war only to betray it, is strictly prohibited, as are other deceptions that misuse protected symbols (like the Red Cross), involve wearing the enemy's uniform in combat, or feign non-hostile relations for tactical gain. These acts harm the protection the law of war affords to civilians, the wounded, and others, as well as erode trust between combatants, which is essential for peace restoration.

Legitimate ruses in warfare, on the other hand, include tactics such as surprising the enemy, ambushes, feigned attacks, retreats, or simulated withdrawals. Other methods encompass creating a facade of inactivity, using small units to appear as larger forces, and sending false or misleading radio or telephone messages, such as orders pretending to come from the enemy's command, or faking communication with imaginary reinforcements. Additional techniques include deceptive supply movements, deliberately spreading false information, employing spies and secret agents, setting up dummy weapons, vehicles, and mines, and erecting mock installations and airfields.

As such, legal considerations play a pivotal role in planning deception operations. Commanders and planners must ensure that any deception methods they employ strictly adhere to international legal standards to maintain the legitimacy of their actions and avoid violations that could lead to criminal accountability. Consulting with legal advisors

is essential, particularly in complex scenarios where the distinction between lawful ruses and unlawful acts of perfidy may appear blurred. Thus, deception operations are subject to both operational and ethical scrutiny, emphasizing a commitment to lawful conduct even within adversarial contexts.

3.2. Deception process

Further-on I will employ a graphical representation to highlight the process of deception as it is perceived in the specialized literature analysed. In general, considering that deception requires a form of communication with the enemy it follows a logical flow of sending a deceptive message through selected channels to the target in order to form a certain perception that will determine him to decide for his forces to act in a manner that portrays operational advantages for the deceiver, as seen in the simplistic figure below.

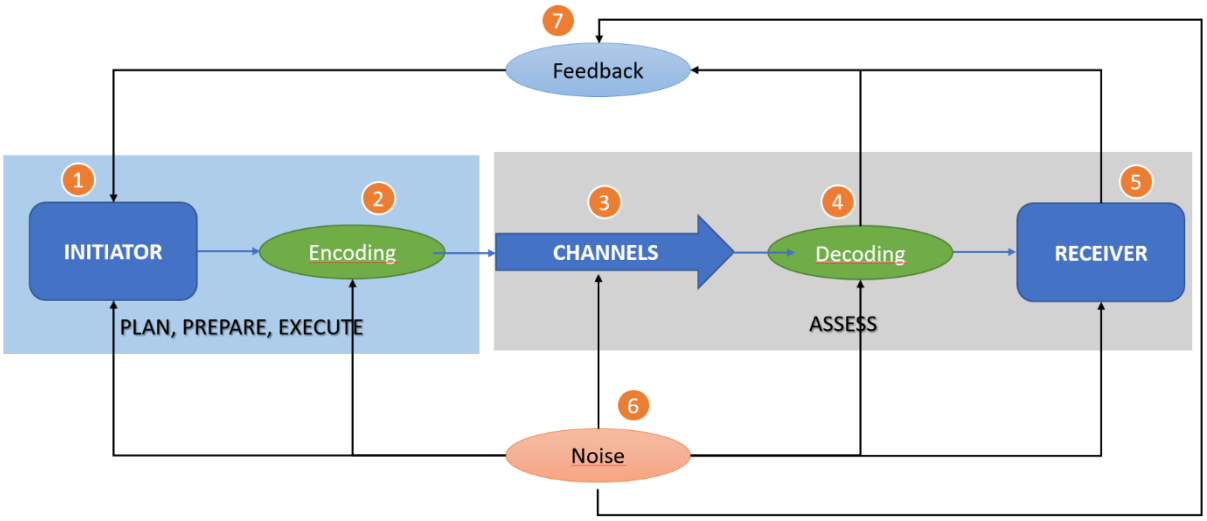

Figure no. 1: *Deception communication process*
(Source: Author)

3.2.1. Initiator

The friendly forces commander holds the decision to incorporate deception within the overall concept of operation, based on the staff assessment and proposal, during the mission analysis phase of the operations planning process. This decision is made after an extensive analysis of the situation. Examining their own mission and tasks, along with the enemy's susceptibility to deception, are just a few of the elements that need addressing when analysing the suitability of deception. Other factors include the operational environment, available resources, and potential risks. A thorough evaluation ensures that deception plans are tailored to exploit enemy vulnerabilities effectively while supporting the overall mission objectives.

In this respect, the process starts with the end in mind. There are 2 essential aspects that set the deception process into motion, both determining the desired end-state of the deceptive operation, as seen in Table no. 3:

– Establish the deception aim and objectives

– Establish the desired enemy perception

Both of them are of critical importance to the force as they are the standard against which the assessment process measures the effectiveness of the deception. Establishing a clear aim, but also suitable objectives and desired enemy perceptions ensures that all efforts are aligned and focused on achieving the intended outcome. Ensuring coherence in planning and execution is crucial to mission success, as it ultimately increases the likelihood of success.

Table no. 3
Deception end-state

DECEPTION AIM and OBJECTIVES	- **Deception Aim** - It should reflect the operational effects that deception provides within the overall concept of operations - The aim should be written from the initiator point of view. - Examples of operational effects: achieving surprise, freedom of movement, security and protection, economy of effort. - **Deception Objectives** - They reflect the external conditions that the deception should attain, with respect to how the adversary, the civil environment, the operating environment should look like as a consequence of the deception operation. - They should be written from the adversary point of view.
ADVERSARY'S DESIRED PERCEPTION	- Perception is how the adversary must understand a situation in order to make the decisions that will determine the expected behavioural response. - The desired perception will be the basis for accomplishing the intended deception objectives. - Account must be taken of the opponent's level of understanding of the situation up to that point, but also of the specific way in which it interprets certain elements. - The process of forming the perception is closely linked to the analysis of the deception target, as there are a multitude of factors that can cause the same situation to be perceived differently by different people, at different moments.

3.2.2. Encoding

Encoding refers to the way in which the message is sent to the receiver, meaning the specific actions taken so that the enemy's collection sensors receive the deceptive message. Regarding this step, the literature employs several concepts that help encoding the deceptive message: techniques, methods, types, tactics, and means. These concepts are concrete procedures that have proven their utility in armed conflicts throughout history. By effectively employing them, military planners can ensure the deceptive message is send in a way that maximizes the chances to create the desired enemy perception. Details with respect to these concepts can be found in the below table.

Table no. 4
The "how" of deception

TECHNIQUES	- **The obvious solution**: Appear to follow a predictable path while pursuing a different one. - **The false routine**: Condition the enemy to expect standard behaviour, masking the real plan. - **The substitution**: Swap real elements with false ones covertly. - **The lure**: Present an enticing opportunity to trap the enemy. - **The deliberate leak**: Intentionally leak false information to be perceived as genuine intelligence.

<table>
<tr><td>TECHNIQUES</td><td>- The mistake: Make the enemy believe they obtained crucial information by error.
- The piece of bad luck: Create the impression that vital information was acquired by the enemy accidentally.
- Amplifying signatures: Appear larger, more capable.
- Suppressing signatures: Appear smaller, less capable.
- Conditioning the adversary: Desensitize the enemy to the deceiver behaviour patterns, making their perceptions exploitable at a chosen time.</td></tr>
<tr><td>METHODS</td><td>- Deception is not equal to lying. In order for the target to believe the deceptive message, one should be presented with both real and fictious facts. For this reason, deception implies both showing and hiding information depending on the technique employed and the desired end-state. These two specific methods of deception are simulation and dissimulation.
<table>
<tr><th>Methods</th><th>Simulation</th><th>Dissimulation</th></tr>
<tr><td>Truth</td><td><u>Showing: NEFI</u>
- portrayal of true information to the adversary to support the insider’s actions
- portrayal of locations of military entities, events or processes that are true but irrelevant</td><td><u>Hiding: EEFI</u>
- operations security measures
- concealment of force dispositions and intentions
- multispectral camouflage measures</td></tr>
<tr><td>Fiction</td><td><u>Showing: EEDI</u>
- portrayal of false information to the adversary (false targets)
- portrayal of locations of military entities, events or processes that are false</td><td><u>Hiding: NDDI</u>
- withholding information that is false to heighten uncertainty.</td></tr>
</table>
- NEFI (Non-Essential Friendly Information) – True information that is deliberately shared with the target to help convincing him to build the desired perception.
- EEFI (Essential Elements of Friendly Information) – Critical true information that must be concealed from the adversary’s sensors in order to be able to trick him.
- EEDI (Essential Elements of Deception Information) – False information that is intentionally conveyed to the target to help create the desired perception.
- NDDI (Non-Disclosable Deception Information) – False information that must be hidden from the adversary’s sensors to ensure the enemy is misled effectively.</td></tr>
</table>

<table>
<tr><td>TYPES</td><td colspan="2">- Ambiguity producing deceptions – A-Type – create confusion by presenting information that can be interpreted in multiple ways. The goal is to make it difficult for the enemy to discern the true intentions of friendly forces, thereby causing hesitation in decision-making or misjudgement.
- Misleading deceptions – M-Type – providing false information to direct the enemy's perception and consequently its decision-making. By steering the adversary towards incorrect conclusions, misleading deceptions aim to exploit their miscalculations in order to gain a certain advantage.</td></tr>
<tr><td rowspan="5">TACTICS</td><td rowspan="3">Simulation
(Active measures)</td><td>Display: Show capabilities or intentions to mislead about actual strength or plans.</td></tr>
<tr><td>Feint: A diversionary tactic to mislead about the real focus of effort.</td></tr>
<tr><td>Demonstration: Visible action simulating a planned operation to influence enemy perception.</td></tr>
<tr><td rowspan="2">Dissimulation
(Passive measures)</td><td>Disinformation: Spread of false information to confuse or mislead the enemy.</td></tr>
<tr><td>Camouflage: Concealment to hide forces or activities from detection.</td></tr>
<tr><td>Denial: Preventing access to critical information to limit enemy situational awareness.</td></tr>
<tr><td>MEANS</td><td colspan="2">- Physical – Tangible elements like decoys and camouflage used to mislead about size or capability.
- Technical – Use of technology, such as electronic warfare and false signals, to create misleading impressions.
- Administrative – Organizational measures, including manipulated documents and controlled leaks, to support deception tactics.</td></tr>
</table>

Two extremely important themes in the existing literature on deception are timing and risk. Timing is essential as the success of a deception often depends on when these actions are introduced relative to the enemy's decision-making process in order to create the desired outcomes in due time. Precise timing can exploit moments of vulnerability or uncertainty, making the deception more impactful. Conversely, risk involves potential hazards such as exposure, unintended consequences, and adversary countermeasures. Effective deception requires a careful balance of these risks versus benefits, as the deceptive message is influenced by many factors such as noise and other filters in its way towards the target.

Table no. 5

Deception - risk and time analysis

RISK	- Deception should incorporate a risk analysis process to mitigate it and minimize unexpected negative outcomes. - The risk analysis must be carried out in relation to the potential benefits. - Constant assessment of the assumptions against which the analysis was made needs to be a must.
TIME	- Time determines the extent of deception operation. - One should ask during planning whether the desired perception can be achieved in the time available. - Time is also relevant to know when and on which channel to place the deceptive information

Specific actions designed to portray the deceptive message towards the enemy are seen by its collection assets as observables. They represent an important theme within the existing literature, as they represent the detectable elements that the enemy is able to monitor, which convey the intended false information, thus shaping the enemy's perception according to the deception objectives, as seen in Table no. 6.

Table no. 6

Deception observables

OBSERVABLES	- An observable is what the adversary's intelligence collection systems need to detect. - Attention must be paid to the competing observables to ensure that the deceptive message is received by the adversary's collection sensors in the form and time desired by the deceiver so that it can contribute to forming the intended false perception.

3.2.3. Channels

This is another recurrent theme in the deception literature. Deception channels are the pathways through which deceptive messages are transmitted to the enemy. Without being able to identify the information portrayed, deception will not succeed in shaping the perception of the adversary. It is very important that the adversary has access to those channels, but also means to decode the message sent through them. Ensuring that the enemy can detect and proper interpret the deceptive signals is crucial for the deception to be effective. Synchronizing deception actions across multiple channels into a coherent narrative is a prerequisite for successful deception. One should also consider the availability of the channel for the enemy in order to be able to place the desired message within that timeframe.

Table no. 7
Deception channels

DECEPTION CHANNELS	- Adversary intelligence collection disciplines: HUMINT, OSINT, MASINT, SIGINT, IMINT, GEOINT. - Traditional media sources: television, newspapers, radio, etc. - Internet: social media sites, e-mail, websites. - Military communication systems: radio, official e-mails, orders, radar, electronic signature. - Diplomatic sources.	**Considerations** regarding selecting the appropriate channels: - Exploiting vulnerabilities in the adversary ISR systems. - Ensuring that those systems can and will pick up the deceptive messages (channel uptime and technology that can receive the message). - Transmitting information through channels trusted by the adversary - Synchronized transmission of the deceptive message through as many channels as possible. - Identifying the optimal channels for transmitting information is essential to the success of the action.

3.2.4. Decoding and receiver

Decoding implies a process that the enemy is performing in order to interpret the information sent by the initiator. In this regard, decoding take place during the enemy intelligence cycle, which is "*the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available for users*" (AJP-2, 2020, p. 4-1). First, the information is collected and analysed by single-source intelligence disciplines during the JISR (Joint Intelligence Surveillance and Reconnaissance) process and then integrated into a multi-source analysis during the Processing phase. In the end, the intelligence resulted is delivered to those needing it. Following a Rapid decision-making process, based on the perception created by the intelligence received, the commander takes a decision for its forces. Ideally, it should set into motion the actions intended by the deceiver in order to create the desired end-state.

However, when planning how to deliver the deceptive information, it is of utmost importance that the initiator analyses all the details regarding how the message will be decoded by the enemy, in what timeframe, what external influences (noise) might degrade the intended message towards the target, but also particularities of the enemy decision-making process and specific traits of the enemy commander that might affect the intended outcome. In order to exploit the enemy's vulnerabilities, one needs to consider the information detailed in the table below.

Table no. 8
Adversary analysis

ADVERSARY INTELLIGENCE CYCLE	- Analysis of the adversary's intelligence collection capabilities. - Enemy intelligence collection plan analysis. - Enemy intelligence analysis methods. - Analysis of credibility of adversary's intelligence sources.
DECEPTION TARGET	- Level of situational awareness. - Risk tolerance. - Leadership style. - Experience, behaviour, character. - Biases / Prejudices (cultural, organizational, personal).
ENEMY DECISION-MAKING PROCESS	- Timelines. - Adversary mission and objectives. - Doctrinal approach. - Psychological profile of those involved in the process. - Patterns in the adversary's decision-making process.

3.2.5. Noise and feedback

Noise is an extremely important theme that directly affects the success of deception operations. It refers to any conflicting data or other influence, internal and external, that might degrade the efficiency of deception.

Noise can originate from a variety of sources, including unintentional leaks, inability to properly control the message, unanalysed elements regarding the enemy or the operational variables, but also internal noises specific to every conflict such as stress, fear, or the level of tiredness of the personnel involved. It can occur at any point throughout the deception process. These conflicting signals can either erode the credibility of the deceptive message, reduce its effectiveness, and increase the risk of the adversary uncovering the deception, or make it irrelevant for the enemy to take it into account.

It is recommended that a close manage of noise be made through anticipation, but also strict control over information dissemination, consistent actions, redundancy in communication channels, and enhanced operational security. Feedback is critical to ensure prompt adaptation of the deceptive plan to address any emerging noise. By maintaining a clear, consistent, and credible deceptive narrative, but also through a flexible deception plan, military planners can ensure that the adversary is effectively misled and the deception operation achieves its predefined objectives.

Starting with the decoding phase, the friendly forces' main mission is to monitor and assess the progress of the deceptive message towards the desired end-state. This involves closely observing how the adversary interprets the observables and reacts to the deceptive signals being sent. Continuous intelligence collection and analysis are essential to understand the deception progress. By tracking the adversary's responses, the deceiver can determine whether the deception is being believed, progresses towards the desired objectives and is steering the enemy towards the intended perception. Any indications that the deception is not working accordingly must be addressed swiftly through adaptation, either new actions or a reinforcement of the narrative. This phase is critical to ensure that the deception maintains its effectiveness, ultimately leading to the successful achievement of the objectives. To this end, one should consider applying the information provided in Table no. 9.

Table no. 9
Deception feedback phase

CONTINUOUS FEEDBACK	- Monitoring the effectiveness of operational security measures. - Monitoring the effectiveness of deceptive actions. - Evaluation of the effects created	- Matching expectations to the effects created by deception actions - Analysing the filters influence over the deceptive message - Analysing how the information reaches the target (both its form and time it takes to reach it).

4. Conclusions

In conclusion, as deception becomes more important in operations, this study fills a gap in research by giving military leaders a useful tool to plan and carry out successful deception operations. By identifying common themes that have lasted over time, this work offers key insights and advice for current and future military plans. This ensures that leaders can appropriately use deception to reach their goals in today's complex and transparent battlefield setting.

The relevance of the study also lies in its exhaustive compilation of some of the most important research on deception operations carried out since the Second World War. This compilation provides a thorough analysis of the development and use of deception in military strategy, as well as insights into the ways in which different ideas and concepts have been applied and understood over time. By analysing these significant works, the research highlights the crucial role of deception in contemporary military operations and its continuing importance in determining the outcome of armed conflict, as well as the timeless elements of effective deception that have stood the test of time.

REFERENCES

AJP-2. (2020). *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security* (Edition B, Version 1). NATO Standardization Office.

AJP-3.10.2. (2020). *Allied Joint Doctrine for Operations Security and Deception* (Edition A, Version 2). NATO Standardization Office.

Anderson, M. G. (2022). The Case for Deception in Operational Success. *Military Strategy Magazine, Vol. 8, Issue 2*, 38-42.

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

Bouwmeester, A.J. (2020). *'Krym Nash': An Analysis of Modern Russian Deception Warfare*. Utrecht: Utrecht University.

Bowyer Bell, J., & Whaley, B. (1982). *Cheating and deception* (1st Edition). St. Martin's Press.

Clark, R.M., & Mitchell, W.L. (2019). *Deception: Counterdeception and Counterintelligence*. Los Angeles: CQ Press.

Creswell, J.W., & Creswell, J.D. (2023). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (6th Edition). Los Angeles: Sage Publications.

Daniel, C.D., & Herbig, K.L. (1980). *Multidisciplinary Perspectives on Strategic Deception*. Monterey, California: US Naval Postgraduate School.

Dewar, M. (1989). *The Art of Deception in Warfare*. Devon, UK: David & Charles Publishers.

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

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

Given, L.M. (2008). *The SAGE Encyclopedia of Qualitative Research Methods*. *Vol. 1&2*. California: Sage Publications.

Godson, R.J. (2002). *Strategic Denial and Deception: The Twenty-First Century Challenge*. New Jersey: New Transaction Publishers.

Governmentattic.org. (1980). *Central Intelligence Agency (CIA) research paper: Deception Maxims: Fact and Folklore*. Washington DC: Deception Research Program.

Green, J.J. (2020). *The Fifth Masquerade: An Integration Experiment of Military Deception Theory and the Emergent Cyber Domain*. Annapolis: US Naval Postgraduate School.

Handel, M.I. (1987). *Strategic and Operational Deception in the Second World War*. London: Frank Cass.

Hays, M.G. (2020). *Convergence of Military Deception in Support of Multi-Domain Operations*. In Cantwell, G.L., *Theater Army in Multi-Domain Operations Integrated Research Project*, 55-86. US Army War College.

Heuer, R.J. (1999). *Psychology of Intelligence Analysis*. Washington DC: Center for the Study of Intelligence, Central Intelligence Agency.

Howitt, D. (2019). *Introduction to qualitative research methods in psychology: Putting theory into practice* (4th Edition). Pearson Education Limited.

IISS. (2022). *Strategic Survey 2022: The Annual Assessment of Geopolitics*. London: Routledge.

Lloyd, M. (1997). *The Art of Military Deception* (1st Edition). Leo Cooper.

JSTOR. (2015). Denial and Deception. *American Intelligence Journal, Vol. 32, Issue 2.* Available at: https://www.jstor.org/stable/26202127.

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

MCTP 3-32F. (2024). *Deception*. US Marine Corps.

Monroe, J. D. (2012). *Deception: Theory and Practice*. Monterey, California: US Naval Postgraduate School.

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

Rein, C.M. (2018). *Weaving the Tangled Web. Military Deception in Large-Scale Combat Operations.* Kansas: Army University Press.

Rothstein, H., & Whaley, B. (2013). *The Art and Science of Military Deception*. Artech House.

Ryan, M. (2024). *The Quest for a New Offensive Doctrine*. Available at: https://mickryan.substack.com/p/the-quest-for-a-new-offensive-doctrine, accessed on June 12, 2024.

Santelises, A. (2022). *The Ukrainian Kharkiv Counter-Offensive and Information Operations*. Available at: https://cove.army.gov.au/article/ukrainian-kharkiv-counter-offensive-and-information-operations.

Walliman, N. (2022). *Research methods – the basics* (3rd Edition). New York: Routledge.

Whaley, B. (1969). *Stratagem: Deception and Surprise in War* (1st Edition). London: Artech House.

Whaley, B. (2016). *Practice to deceive*. Annapolis: US Naval Institute Press.