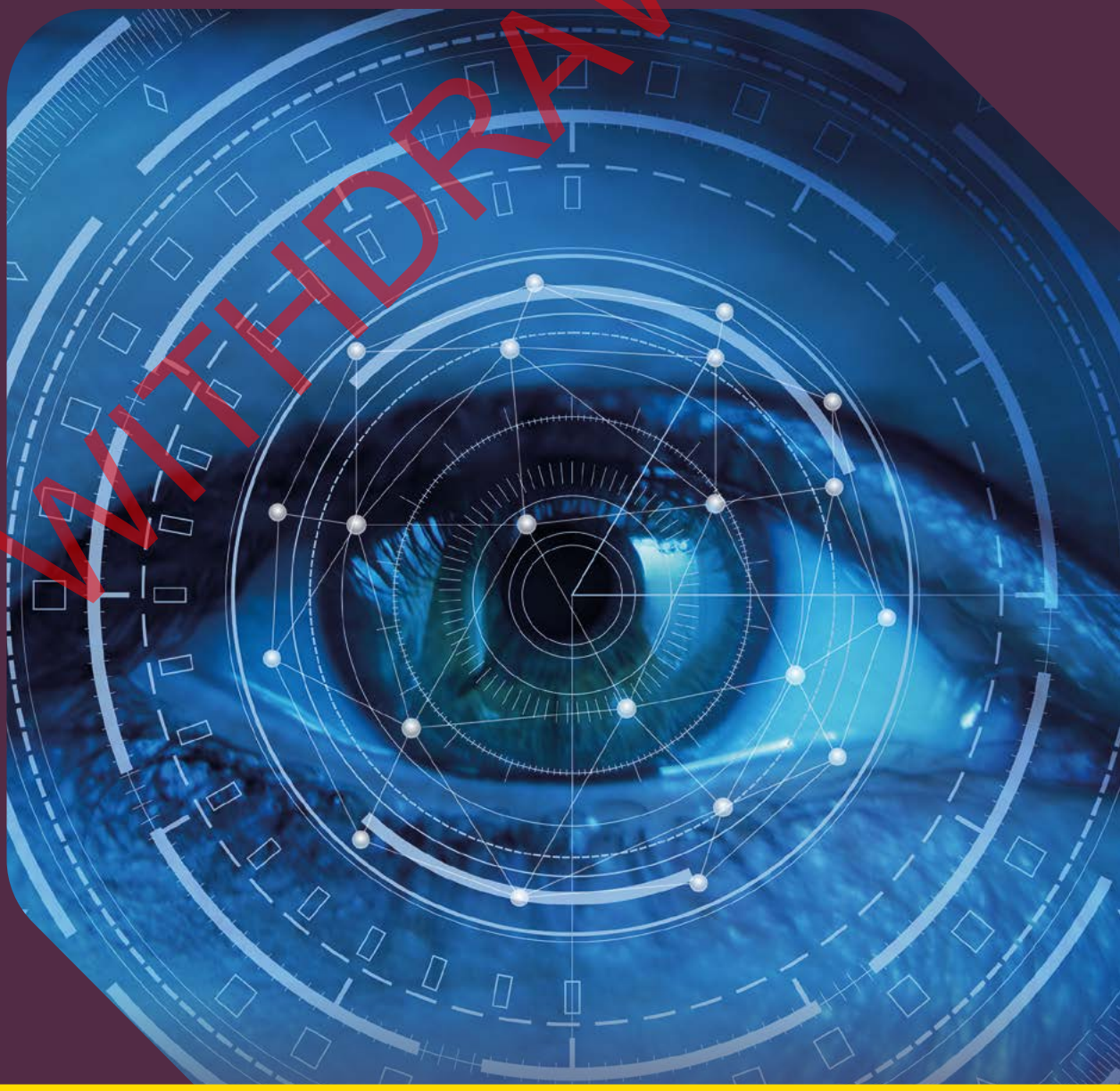
Ministry of Defence

NATO OTAN

Allied Joint Publication-3.10.2

Allied Joint Doctrine for Operations Security and Deception



Edition A Version 2

NATO STANDARD

AJP-3.10.2

ALLIED JOINT DOCTRINE FOR OPERATIONS SECURITY AND DECEPTION

Edition A Version 2

MARCH 2020

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

NATO STANDARDIZATION OFFICE (NSO)

Intentionally blank

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

6 March 2020

1. The enclosed Allied Joint Publication, AJP-3.10.2, Edition A, Version 2, ALLIED JOINT DOCTRINE FOR OPERATIONS SECURITY AND DECEPTION, which has been approved by the nations in the Military Committee Joint Standardization Board is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 6518.

2. AJP-3.10.2, Edition A, Version 2, is effective upon receipt and supersedes AJP-3.10.2 , Edition A, Version 1, which shall be destroyed in accordance with the local procedure for the destruction of documents.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database ((https://nso.nato.int/nso/) or through your national standardization authorities.

5. This publication shall be handled in accordance with C-M(2002)60.

Zoltán GULYÁS
Brigadier General HUN(AF)
Director, NATO Standardization Office

Intentionally blank

Allied Joint Publication-3.10.2

Allied Joint Doctrine for Operations Security and Deception

Allied Joint Publication-3.10.2 (AJP-3.10.2), dated March 2020, is promulgated in the United Kingdom, in accordance with the UK national comment, as directed by the Chiefs of Staff

Director Concepts and Doctrine

Intentionally blank

RECORD OF NATIONAL RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS

Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.

Intentionally blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
USA	Reservation 1. The United States recommends removal of glossary/lexicon terms and definitions that are not NATO Agreed, quoted verbatim from NATOTerm, correctly cited IAW AAP-47 Allied Joint Doctrine Development, correctly introduced or revised IAW AAP-77, NATO Terminology Manual, nor have terminology tracking forms submitted. This reservation will be lifted when the relevant NATO terms and definitions are corrected (see matrix for any specificity with terms). Reservation 2. The United States recommends using the term 'international law' in place of 'humanitarian law' (when expressed) as the term is misused per national understanding and compliance with the Geneva Conventions. Reservation 3. The United States expects that approved text will be harmonized with capstone and operations keystone AJPs otherwise United States personnel will use national joint doctrine to overcome variances. Reservation 4. The United States recommends paragraph 1.4 text be stricken that mischaracterizes perfidious conduct and incorrectly attributes First 1977 Protocol Additional to the 1949 Geneva Conventions. The United States does not interpret the law of armed conflict to prohibit capturing an adversary by resort to perfidy and the United States is not a party to the Additional Protocol I and does not necessarily accept that provision (Art 37) as customary international law.
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

Intentionally blank

Table of contents

Related documents ix
Preface xi

Chapter 1 – Fundamentals 1
Section 1 – Introduction 1
Section 2 – Operations security 3
Section 3 – Deception 4
Section 4 – Principles 6
Principles of operations security 6
Principles of deception 6
Section 5 – Key responsibilities 7
Operations security responsibilities 7
Deception responsibilities 8
Section 6 – Counter-deception 9
Section 7 – Training 9

Chapter 2 – Operations security 11
Section 1 – Introduction 11
Section 2 – Understanding 11
Section 3 – Operations security process 12
Annex 2A – Critical information and indicators 15
Annex 2B – Operations security measures 21

Chapter 3 – Deception 25
Section 1 – Introduction 25
Section 2 – Deception process 28
Section 3 – Understanding 31
Section 4 – Operations planning process 32
Section 5 – Execution 35
Terminating the deception 37
Section 6 – Assessment 38

Annex 3A – **Cognitive factors in deception** 41
Annex 3B – Intelligence requirements to support deception 45
Annex 3C – Deception techniques 47
Annex 3D – Deception story development 49
Annex 3E – Deception matrix to support the operations planning process 51

Lexicon

Part 1 – Acronyms and abbreviations Lex-1
Part 2 – Terms and definitions Lex-3

Related documents

MC 0422/5, *NATO Military Policy for Information Operations*.

AJP-01, *Allied Joint Doctrine*.

AJP-2, *Allied Joint Doctrine for Intelligence, Counter-intelligence and Security*.

AJP-3, *Allied Joint Doctrine for the Conduct of Operations*.

AJP-5, *Allied Joint Doctrine for the Planning of Operations*.

AJP-6, *Allied Joint Doctrine for Communication and Information Systems*.

AJP-3.5, *Allied Joint Doctrine for Special Operations*.

AJP-3.6, *Allied Joint Doctrine for Electronic Warfare*.

AJP-3.19, *Allied Joint Doctrine for Civil-military Cooperation*.

AJP-3.12, *Allied Joint Doctrine for Military Engineering*.

AJP-3.14, *Allied Joint Doctrine for Force Protection*.

AJP-3.20, *Allied Joint Doctrine for Cyberspace Operations* (SD3).

AJP-3.9, *Allied Joint Doctrine for Joint Targeting*.

AJP-3.10, *Allied Joint Doctrine for Information Operations*.

AJP-3.10.1, *Allied Joint Doctrine for Psychological Operations*.

AJP-3.4.4, *Allied Joint Doctrine for Counter-Insurgency* (COIN).

USA Joint Publication 3-13.4, *Military Deception*.

Intentionally blank

Preface

Scope

1. Allied Joint Publication (AJP)-3.10.2, *Allied Joint Doctrine for Operations Security and Deception* addresses the planning, execution and assessment of operations security (OPSEC) and deception and their integration into North Atlantic Treaty Organization (NATO) joint operations. It details OPSEC and deception principles, roles, responsibilities and relationships with other staff functions in supporting the operation plan. OPSEC and deception are positioned as discrete information activities that are not exclusively coordinated by information operations planners. Counter-deception is addressed, but this is a separate process and not the primary responsibility of OPSEC or deception staffs.

Purpose

2. The purpose of AJP-3.10.2 is to provide direction and guidance to NATO commanders and their OPSEC and deception staff. It positions OPSEC and deception as key activities that support the principles and operational considerations of joint operations and must be considered from the outset of the operations planning process. It emphasises the importance of these activities to commanders and staffs.

Application

3. NATO OPSEC and deception doctrine is primarily for use by NATO forces at the operational level but it is also a useful reference for all levels. It can also be a useful framework for operations conducted by a coalition of NATO partners, non-NATO nations and other organizations. It provides a common baseline for achieving interoperability on operations, crises prevention and exercises.

Intentionally blank

Chapter 1 – Fundamentals

Section 1 – Introduction

1.1. Allied Joint Publication (AJP)-3.10.2, *Allied Joint Doctrine for Operations Security and Deception* provides direction and guidance for the planning, execution and assessment of operations security (OPSEC) and deception across the full scale of military operations to preserve Alliance freedom of action. It details OPSEC and deception principles, roles, responsibilities and relationships with other staff functions.

1.2. Surprise and security are two of the twelve principles of joint and multinational operations;[1] OPSEC and deception support these principles. AJP-5, *Allied Joint Doctrine for the Planning of Operations* identifies the need to consider building deliberate surprise in the operations design and highlights that the side that is able to generate information advantage is in a position to seize the initiative; OPSEC and deception will be key to achieving surprise and seizing the initiative.

1.3. OPSEC and deception planning are required against all adversaries.[2] It is critical that OPSEC and deception planning is taken into account from the outset of the planning process at the strategic, operational and tactical echelons of command. The manoeuvrist approach to operations applies strength against vulnerabilities, often through indirect means, using ingenuity as opposed to physically destroying a capability. NATO must achieve an intellectual edge by developing innovative and disruptive thinking. Commanders, planners and operators should be agile thinkers and decision-makers encouraged to outmanoeuvre adversaries. OPSEC and deception are separate but mutually supporting processes that can save resources and lives, while causing adversaries to waste combat power with inappropriate or delayed actions. OPSEC and deception are force multipliers, which support the commander achieving their objectives by providing greater freedom of action.

1.4. **Legal.** Provided it is not perfidious or otherwise prohibited by law or policy, deception is a legitimate military activity and is a ruse of war. In an armed conflict, deception must comply with the Law of Armed Conflict (LOAC), as reflected in customary and treaty law, including Article 37 of the First 1977 Protocol Additional to the 1949 Geneva Conventions. National caveats and interpretations will also apply. LOAC permits ruses of war as acts intended to mislead an adversary or induce them to act recklessly, which do not infringe a rule of international law. Deception techniques must not constitute perfidious acts. Perfidy is described as an act inviting the confidence of an adversary, to lead them to believe they are entitled to, or obliged to accord, protection under the rules of international law

[1] Allied Joint Publication (AJP)-01, *Allied Joint Doctrine*.
[2] For military operations, NATOTerm defines adversary as: 'a party acknowledged as **potentially hostile** and against which the legal use of force may be envisaged'. This publication will use the term adversary to also mean enemy, and therefore also hostile, as this is how most Allied joint publications use the term.

applicable in armed conflict, with intent to betray that confidence.[3] LOAC prohibits the killing, injuring or capturing of an adversary by resort to perfidy. In situations under the threshold of an armed conflict,[4] LOAC does not apply. However, the use of deception might be subject to other legal or policy limitations, including rules of engagement.

1.5. **The information environment.** The information environment comprises two main facets; firstly, the cognitive, virtual and physical spaces that exist within it and secondly, the interrelationships between them. Current technology provides individuals and groups with the ability to create, store, manage, control, manipulate and transmit information quickly and easily. This has in turn created an increased dependency on information and information technology by states and other actors. Information is subject to preconception, bias, agenda, manipulation and interpretation by both the transmitter and receiver. The modern environment brings challenges with the extensive proliferation and sophistication of information collection tools and technologies. Simultaneously, it provides greater access to opinions and a more intimate understanding of motivations, as well as numerous new conduits for projecting specific perceptions and information to targets and audiences. The information age exposes warfare to greater public scrutiny because of the proliferation of digital media[5] channels, smartphones and other smart devices. An understanding of this environment and an ability to operate within it are vital, as it will present both a threat and an opportunity for OPSEC and deception. As with all relevant activity, OPSEC and deception must be coherent with the strategic narrative.

1.6. **The relationship with information operations.** OPSEC and deception are discrete information-related activities and not coordinated solely by information operations (Info Ops). Info Ops is the staff function that coordinates information activities to create effects on will, understanding and capability. To maintain credibility of the overall messaging, the information activities within OPSEC and deception plans have to be coordinated with Info Ops, as with any other discrete process or capability, if not compartmentalized for security reasons. This will ensure that other NATO-related activities such as military public affairs (PA) and civil-military cooperation, which have no role in planning or executing deception, do not contradict the promotion of the narrative.

1.7. **Achieving a behavioural response.** Deception is a psychological process and seeks a behavioural response, be it action or inaction. For the purposes of this publication, a behavioural response is a cognitive reaction to a stimulus that then

[3] Examples of perfidy are: the feigning of an intent to negotiate under a flag of truce or of a surrender; the feigning of an incapacitation by wounds or sickness; the feigning of civilian, non-combatant status; and the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other states not party to the conflict.
[4] Including internal disturbances and tensions, such as riots, isolated and sporadic acts of violence or other acts of a similar nature.
[5] Digital media is any medium of communication using digital content. It can be either one-way or two-way communication. Social media is the communication channel where all users become contributors.

provokes a decision to act or remain inactive. Annex A to Chapter 3 addresses cognitive factors in deception in more detail.

Section 2 – Operations security

1.8. OPSEC is defined as: 'the process that gives a military operation or exercise appropriate security, using passive or active means, to deny an adversary knowledge of the essential elements of friendly information, or indicators of them'.[6] The aim of OPSEC is to deny critical information and indicators to adversaries. For the purposes of this publication, OPSEC indicators are detectable signs of activity and publicly available information that could be interpreted to derive intelligence on friendly forces. The OPSEC process is an essential activity that protects plans and operations by identifying and safeguarding EEFI and indicators. It promotes the development of recommended measures to reduce the vulnerabilities of Allied forces' mission critical and sensitive information to exploitation. OPSEC actions are proactive measures that reduce the adversary's ability to detect and determine friendly intentions, dispositions, strengths and weaknesses. Through coordination, OPSEC will enhance, but not replace, traditional security protection procedures by providing specific purpose and context for their actions, both to deny access and to manipulate understanding, as illustrated in Figure 1.1. Countersurveillance may support OPSEC by identifying adversary surveillance capability that is targeting a defined EEFI.

[6] This is a modified term and definition and will be processed for NATO Agreed status. The existing NATO Agreed definition for OPSEC is: 'the process which gives a military operation or exercise appropriate security, using passive or active means, to deny the enemy knowledge of the dispositions, capabilities and intentions of friendly forces'.

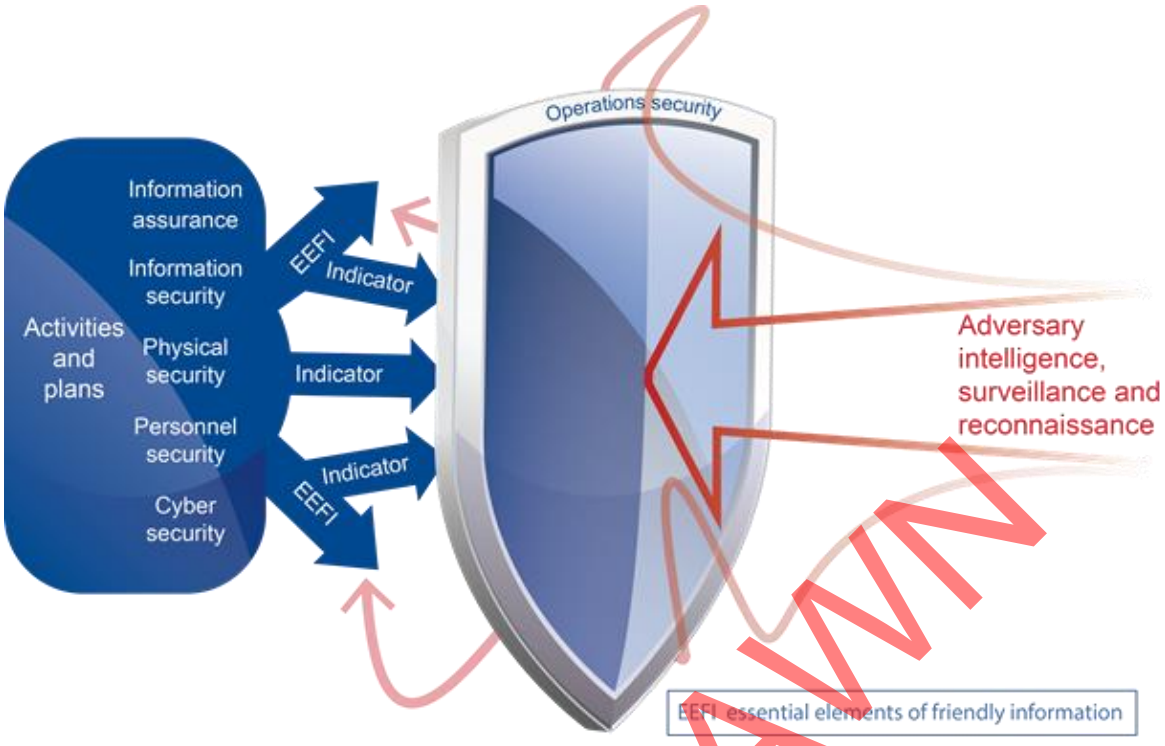


Figure 1.1 – OPSEC in relation to traditional security procedures

1.9. **Essential element of friendly information.** An EEFI is defined as: 'critical information about intentions, requirements, capabilities and vulnerabilities that, if compromised, could threaten the success of operations'.[7] EEFI are a vital part of the commander's critical information requirement (CCIR)[8] and allow the staff to plan and implement information protection measures, such as those provided by OPSEC and deception.

Section 3 – Deception

1.10. Deception is defined as: 'deliberate measures to mislead targeted decision-makers into behaving in a manner advantageous to the commander's objectives'.[9] The aim of deception is to exploit the advantage gained from misleading the targeted adversary decision-maker; the focus is on influencing behaviour through shaping attitudes and perception. The basis of this response involves various aspects of heuristics, nudging of heuristics and human thinking, the latter otherwise known as

[7] This term amends a new term and definition that is currently being processed for NATO Agreed status.
[8] CCIR cover all aspects of the commander's concern including friendly forces information requirement and priority information requirement.
[9] This is a modified term and definition and will be processed for NATO Agreed status. The existing NATO Agreed definition for deception is: 'those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests'.

cognition.[10] Deception explicitly targets the decision-maker[11] critical to creating the required behavioural response. The decision-maker may be at any level in any environment and may be indirectly targeted by influencing groups or sensors. This requires in-depth analysis of target preconceptions, likely responses and information preferences. Effective deception targets an identified decision-maker and their decision-making process. If deception does not target decision-makers, supported by in-depth analysis, it will unlikely result in outcomes that benefit friendly forces. Deception creates and reveals the false, and masks real friendly intentions, strengths, vulnerabilities and dispositions to increase or reduce ambiguity in the adversary. Deception is a commander's responsibility with defined staffing requirements. Deception staff are not responsible for counter-deception; the detection of deception against friendly forces is a J2 responsibility. The response to the detection of deception against friendly forces is a command-led J3/5 responsibility. Deception and counter-deception must be coordinated.

1.11. **The relationship between operations security and deception.** Although OPSEC and deception are mutually supportive they are discrete processes. These processes need to be integrated at all levels to maximize effective support to friendly operations, activities, plans and capabilities. Importantly, conflating them in a manner that would erode legal and policy restraints placed on deception should be avoided.

1.12. **Security of deception planning.** The security caveats placed upon deception planning and the classification of the deception plan itself must be agreed with the commander and must at least reflect the classification of the operation plan itself.[12] Compartmentalization of planning within a staff and between headquarters may be required and national caveats may also apply. The trust required in working with host nation forces and within an Alliance of nations must also be taken into account.

1.13. **The difference between deception, concealment and camouflage.** Concealment and camouflage are techniques primarily used to counter surveillance but can also be used to support the creation of a deception. They are tools and techniques used more generally for masking activity and capability. Concealment is to not allow something to be seen, or to hide something.[13] Camouflage is more specifically the use of natural or artificial material on personnel, objects or tactical positions with the aim of confusing, misleading or evading the enemy.[14] They may be used, or deliberately not used, as part of a deception plan to create a false impression of reality, or to draw attention away from a reality that is to be hidden, or disguised. Commanders are responsible for general camouflage and concealment instructions, which should reside within unit standing operating procedures.

[10] For further detail on cognition, see Annex A to Chapter 3.
[11] For the purposes of AJP-3.10.2, a decision-maker is understood to be a person or artificial intelligence responsible for decision making within an adversary or population's hierarchy. The decision-maker may be at any level of the hierarchy and in any environment but must be able to influence the reinforcement of, or create a change in, behaviour.
[12] See *NATO Security Policy* set out in C-M(2002)49 and C-M(2002)60.
[13] Concise Oxford English Dictionary (COED).
[14] NATOTerm.

Section 4 – Principles

1.14. OPSEC and deception are essential features of the character of conflict. They contribute to the principles of surprise, security and freedom of movement of Allied, joint and multinational operations. The principles of operational security and deceptive behaviour have endured for centuries, and commanders should provide direction for their consideration within contemporary warfare.

Principles of operations security

1.15. **Operations security is the commander's responsibility.** Although all personnel have an individual security obligation it is the commander's responsibility to ensure OPSEC. It is also the duty of all personnel to protect any EEFI to which they have access.

1.16. **Identify the essential elements of friendly information that operations security must protect.** The commander must approve and prioritize the EEFI. It is essential to protect indicators to ensure the success of the operation.

1.17. **Manage the risk.** Effective OPSEC requires a realistic assessment of the adversary's ability to collect data on EEFI, as well as the potential negative effect that could result from this knowledge. Risk management must include all potential channels as both friendly vulnerabilities and means of risk treatment.

1.18. **Integrate early and evaluate continuously.** Integrate OPSEC within the operations planning process (OPP)[15] and evaluate it continuously throughout operations. It should be actively monitored for integrity and relevance and be part of any operation.

1.19. **Protect the planning process.** The planning process itself must be secure. If it is not, the risk is future operations are compromised from the outset.

1.20. **Continuous assessment.** OPSEC is a continuous cyclical process. Modify the OPSEC plan to reflect changes in the operating environment. Continuous assessment of intelligence counter-intelligence and OPSEC analysis will provide feedback to modify OPSEC plans according to requirements.

Principles of deception

1.21. **Create a behavioural response.** Deception must focus on creating a desired behaviour. This behavioural outcome must meet the commander's intent.

1.22. **Reinforce existing beliefs.** It is important to understand what the adversary is predisposed to believe (including how they expect friendly forces to act) and what

[15] For the sequence of planning activities in the OPP, see AJP-5, *Allied Joint Doctrine for the Planning of Operations*.

they are predisposed to disbelieve. It is easier to reinforce a belief than to change it and difficult to convince them of something they would ordinarily reject.

1.23. **Target the decision-maker.** Deception targets the decision-maker. The targeted decision-maker must be able to detect deceptive events, process them and subsequently act upon them. The decision-maker may be at the tactical, operational or strategic level.

1.24. **Be credible, consistent, verifiable and executable.** Deception must be:

- credible in their minds – is it believable;
- consistent with the narrative of the operation and the strategic communications framework – does it make sense in context with what is happening;
- verifiable by their collection assets in the time required – can it be satisfactorily confirmed;
- verifiable by friendly forces collection assets – can we confirm the adversarial reaction; and
- executable in terms of the actions required over the time period available to do so – can we actually do this in a timely manner.

1.25. **Multiple approaches.** Creating effects through joint action (the combined application of the joint functions of manoeuvre, fires, information and civil-military cooperation) will ensure an integrated approach. The greater the number of channels used, the greater the likelihood of the deception being perceived as credible.

1.26. **Conceal the real and reveal the false.** Draw attention away from real dispositions and intentions, while simultaneously attracting attention to false intentions. Alternatives require the adversary to evaluate them.

Section 5 – Key responsibilities

Operations security responsibilities

1.27. **Commander.** The commander has overall responsibility for OPSEC. They will provide guidance for all operations, exercises and other activities, as part of the OPP. The commander's military PA activity and all civil-military interaction (CMI) must be in accordance with the OPSEC direction.

1.28. **Operations security officer.** The OPSEC officer, primarily a member of the operations staff, has the following responsibilities:

- providing guidance on how OPSEC can support the commander's intent by protecting operations;
- integrating OPSEC into the OPP;

- coordinating with intelligence staff to assess threat, intent and capabilities of adversaries and actors within the operating environment;
- coordinating with staff to apply the OPSEC process required to protect EEFI and indicators by reducing vulnerabilities to adversarial collection;
- developing the OPSEC plan and coordinating its execution and review;
- continuously monitoring and reviewing OPSEC control measures and adjusting accordingly; and
- coordinating relevant information activities, according to OPSEC requirements on a need-to-know basis, within the Information Activities Coordination Board (IACB).[16]

1.29. **Chief J2.** Chief J2 will provide threat data and assessments to support OPSEC. J2 will also assist with assessing the effectiveness of OPSEC.

Deception responsibilities

1.30. **Commander.** The commander must decide where the deception officer is most effectively located within the headquarters and must establish a close working relationship with the deception officer, providing clear direction and guidance on deception requirements. The commander maintains authority and centralized control to ensure the deception plan remains in support of the operation. Command of deception should be at the lowest level that is consistent with execution authority, OPSEC and supporting centralized control.

1.31. **Deception officer.** The deception officer must work closely with the commander and has the following responsibilities:

- establishing a deception working group;
- providing guidance on how deception can support the commander's intent;
- integrating the deception plan into the OPP;
- developing and executing the plan and monitoring and evaluating its implementation;
- coordinating deception across all staff functions (including red teaming); and
- coordinating activity, according to security requirements and on a need-to-know basis, within the IACB and the Joint Targeting Coordination Board (JTCB).

1.32. **Chief J2.** Chief J2 ensures the intelligence estimate meets the requirements of the deception plan, assessing and analyzing adversarial methods and capability for collection. J2 should also provide an assessment of how the deception target thinks, decides and acts. Focused intelligence is essential to the successful planning, execution and assessment of deception.

[16] Refer to AJP-3.10, *Allied Joint Doctrine for Information Operations*.

Section 6 – Counter-deception

1.33. **Description**. Counter-deception is a staff function that seeks to identify and counter adversarial deception aimed at undermining the will, understanding and employment of friendly forces. It is not the role of the deception staff to perform counter-deception, but rather the responsibility of the chief of the intelligence staff to detect adversarial deception and the responsibility of the chief of the operations staff to coordinate the appropriate response. Given their subject matter expertise, in practice it is likely that deception staff can support the intelligence and operations staff. It is important that the deception staff do not assume responsibility for counter-deception, as this could confuse and undermine their own deception work.

1.34. **Expect to be deceived**. Just as friendly forces should routinely employ deceptive techniques to undermine adversaries, so the commander should expect adversaries to attempt to do the same to friendly forces. It is thus imperative that the staff remain alert to the possibility of potential adversarial deception and understand adversarial tactics, techniques and procedures and the wider political and cultural context in which their approach to deception sits. Consequently, it is natural that the task to detect adversarial deception sits with the intelligence staff as part of the intelligence support to operations.

1.35. **Active counter-deception**. Active counter-deception comprises the activities required by the commander once intelligence confirms that adversarial deception is underway against friendly forces. The commander will seek to ensure their own EEFI remain protected and may task additional joint intelligence and collection capabilities to reveal the true dispositions and intentions of adversarial forces. The commander will then require a series of actions and managed information releases, planned to cause adversaries to continue expending time, effort and resources to reinforce a deception plan that they believe is working. This is not as simple as telling the adversary what they want to hear but involves a culturally sensitive and nuanced approach to information release and posture, presence and profile. Such active counter-deception, led by the planning staff, will require careful coordination across the headquarters and, in particular, with counter-intelligence efforts.

Section 7 – Training

1.36. Training is not the focus of this publication but it is important that OPSEC and deception training serves two purposes. First, it raises awareness of the requirement for OPSEC and deception, stimulates the imagination and thought processes, and improves skills. Secondly, it raises the alertness of individuals to detect actions conducted to breach OPSEC and to detect deception itself. Commanders and staff need to have the skills to identify EEFI, mitigate vulnerabilities, plan, execute and assess activities and detect counter-activity.

1.37. In training, avoid two particular pitfalls. Firstly, exercises should avoid overly compressed timelines and rigid events lists, as OPSEC and deception plans require

time and flexibility to mature. Secondly, balance concerns about revealing techniques against the benefits of the training.

Chapter 2 – Operations security

Section 1 – Introduction

2.1. Commanders must ensure operations security (OPSEC) is practised during all phases of operations. OPSEC is a process that identifies and protects essential elements of friendly information (EEFI) and indicators of friendly force actions.

Section 2 – Understanding

2.2. OPSEC must be looked at both through the friendly force perspective (what do we think is important and need to protect) and the adversarial perspective (what do they think is important, or need to know). This requires a thorough understanding of the adversary's intent and their ability to exploit vulnerabilities.

2.3. Seemingly unimportant information can be aggregated to form a more complete picture of operations and planned activities. Information sharing media and technical tools such as social media, smart phones and geo-tagging enable the gathering and sharing of large amounts of seemingly unconnected information. OPSEC staff must evaluate the risk to operations of publicly available information aggregated over time. Adversaries will attempt to gather information at all times during training, preparations to deploy, deployment and the operation. OPSEC must consider those EEFI and indicators that are continuous.

2.4. The planning process itself will be subject to adversarial information gathering. It is important that the operations planning process (OPP) is subject to the OPSEC process. Compromising the planning process compromises all subsequent activity.

2.5. J2 support to operations security. Intelligence and counter-intelligence plays a key role in the OPSEC process and J2 directly supports OPSEC by analyzing the threat from reporting and identifying vulnerabilities through assessments. J2 should support OPSEC in identifying, analyzing and evaluating the following.

- What does the adversary already know?
- Where could the adversary collect information against friendly forces?
- What capabilities does the adversary have to collect this information?
- What are the adversarial tactics, techniques and procedures in place to achieve this collection?
- Where is the most likely deployment of the adversarial collection capability?

Section 3 – Operations security process

2.6. OPSEC is more than a collection of specific rules and instructions. As a cyclical process, it should be applied to any operation or activity to deny EEFI to adversaries. It is conducted in a five-step process that is continuous across all phases of operations, including post conflict. It is not linear but is a continuous cycle, as illustrated in Figure 2.1, and outlined below, with the need to continually identify EEFI and indicators as the central requirement.

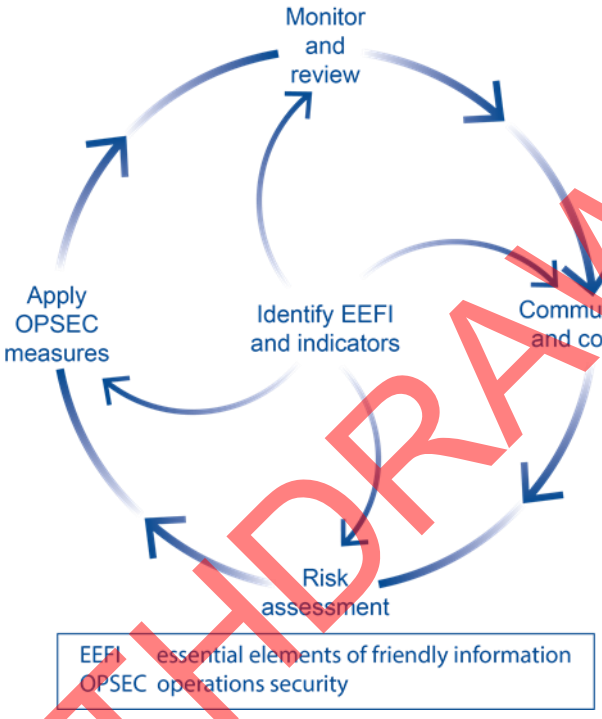


Figure 2.1 – The five-step OPSEC process

2.7. **Step 1: Identify EEFI and indicators.** The OPSEC process must establish the context of the risk. The OPSEC staff must ensure that EEFI and indicators specific to the plan, operation or activity are captured from the relevant staff. The intentions, requirements, capabilities and vulnerabilities of component commands and formations will form the basis of the EEFI, which are relevant to all elements of the operations framework.[17] As essential information changes through phases of the operation, the operations framework should be updated accordingly. New threats, or the agreement of new EEFI, will require a reassessment of risk and existing measures.

[17] Allied Joint Publication (AJP)-01, *Allied Joint Doctrine* describes the core activities of the operations framework as: shape; engage; exploit; protect; and sustain.

2.8. **Step 2: Risk assessment.** OPSEC assessments are the responsibility of OPSEC-trained staff, although they will require supporting information from other staff. The OPSEC staff must work closely with the intelligence staff to identify the risk, analyze the risk and evaluate the risk.[18] Planning or conducting operations and activities will increase the likelihood of indicators and create vulnerabilities for exploitation, particularly with civil-military interaction (CMI). An OPSEC vulnerability exists when the adversary is capable of collecting EEFI, analyzing them and has the time to act and exploit the situation. OPSEC assessments establish a baseline signature for the respective units.

a. **Risk identification.** The OPSEC staff must consider the activity of planning itself, as well as the conduct of activity, from an adversarial perspective to determine where vulnerabilities lie. They must consider both these elements of OPSEC risk to support course of action (COA) development, analysis, validation and comparison, to determine which COA is most supportable from an OPSEC perspective.

b. **Risk analysis.** The risk analysis is balanced between the probability of adversary collection and the impact of successful adversary collection. Determining the level of risk is important, as this justifies the requirement for OPSEC, which may have effort, cost and time implications. The OPSEC staff must identify which channels, including open-source intelligence, could detect the EEFI and provide this information to the adversary.

c. **Risk evaluation.** For each vulnerability identified, the OPSEC staff will evaluate the intent and capability of adversaries to collect, analyze and exploit friendly force EEFI and indicators. This will require coordination across the staff and must include the resources required, synchronization, operations assessment and termination arrangements for the plan to be executed efficiently

2.9. **Step 3: Apply OPSEC measures.** Once the commander has selected the COA, the OPSEC staff should identify the relevant OPSEC measures required to treat risks and finalize the plan to enforce them. This must include the resources required, synchronization, operations assessment and termination arrangements. This process is continually fed from risk assessment. It may involve not taking the risk and ceasing activity, or taking and perhaps increasing the risk to seize an opportunity. It may also involve removing the risk source or changing the consequences, which could include deception. All friendly forces have a role to play in applying OPSEC measures.

2.10. **Step 4: Monitor and review effectiveness of OPSEC measures.** The OPSEC staff must evaluate the risk treatment provided by the OPSEC process. This should be a planned part of the process and must allow for continuous monitoring and review. OPSEC plans can fail if EEFI are disclosed unintentionally. Continual monitoring and reviewing of the OPSEC process is essential. It identifies the:

[18] Refer to AJP-3, *Conduct of Operations* for more information on risk evaluation tools.

- effectiveness of the OPSEC process;
- requirement for any additional OPSEC actions; or
- requirement to adjust existing measures, or change existing plans.

Effectiveness of OPSEC should be considered from the adversary's perspective. Monitoring should be conducted when conditions or mission profiles dictate, or to identify if activity has created a change in signature. This review will determine the likely protection of critical information from adversarial intelligence collection capabilities.

2.11. **Step 5: Communicate and consult at all stages.** The OPSEC staff must ensure the validated EEFI list is promulgated to all staff. Communication and consultation with commanders and staff should take place during all stages of the OPSEC process. OPSEC must be coordinated with other staff branches to ensure feedback on the effectiveness of OPSEC and be executed across the joint force. This communication is important to address the perception of risk and should address the risks identified, the causes, their consequences (if known) and the measures required to treat the risks. Those responsible for the release of information should therefore have the required information to consider OPSEC before publicly releasing information. OPSEC staff must ensure the aggregation of North Atlantic Treaty Organization (NATO) CMI, military public affairs releases, command information, social media and contracting documents do not reveal EEFI.

Annex 2A – Critical information and indicators

2A.1. The following provides examples of information that might be critical and indicators that are associated with the information and its management. The criticality of the information will depend upon the circumstances and operating environment: negotiation, deterrence, shaping, combat, stabilization or transition to civil authority. Equally what is an essential element of friendly information (EEFI), and therefore what is an indicator to it, will depend upon the assessment of the threat, vulnerabilities and the risk. This list is not all-inclusive and is offered to stimulate thinking about what kinds of actions can convey indicators that reveal EEFI. Adversaries will not be able to collect information on all indicators and, equally, there will not be a requirement to hide all indicators, unless they are EEFI.

2A.2. **Military force capabilities.** The following are examples of information and indicators of information that would identify force capabilities.

a. The presence and type of units for a given location, area or base.

b. Friendly reactions to adversarial exercises or hostile actions.

c. Movement of aircraft, ships and ground units in response to friendly sensor detections of hostile units.

d. Routine and predictable patterns in performing the organizational mission that reveal the sequence of specific actions, use of capabilities, or when they are accomplished.

e. Personnel training in protective equipment or practising decontamination.

f. Actions, information or material that:

(1) connect the mobilization or assignment of reserve forces with specific commands or units;

(2) indicate numbers of personnel and their state of training or experience;

(3) reveal equipment or systems availability or reliability; or

(4) reveal tactics, techniques, and procedures for training, equipment or system operational tests and evaluations.

2A.3. **Command and control capabilities and behaviours.** The following are examples of information and indicators of information that would identify command and control intentions and behaviours.

a. Unusual actions with no apparent direction reflected in communications.

b. Association of particular commanders with patterns of behaviour under stress or in varying tactical situations.

c. Actions, information or material that:

(1) provide insight into the volume of orders and reports needed to accomplish tasks;

(2) show unit subordination for deployment, mission or task;

(3) identify target selection and priorities;

(4) reveal problems of coordination between the commander's staff elements;

(5) reveal the period between the occurrence of a need to act or react and the action itself taking place;

(6) reveal the need for higher commands to authorize certain types of activity; or

(7) reveal critical nodes of control, communication and resupply.

2A.4. **Communications.** The following are examples of information and indicators of information that would be identifiable from communications.

a. Unusual testing of radio equipment.

b. Establishing new communications networks. Without conditioning to desensitize, the sudden appearance of new communications networks could prompt the implementation of additional intelligence collection.

c. Suddenly increasing traffic volume, or conversely imposing radio silence, when close to the time of starting an operation, exercise or test. Without conditioning, unusual surges or periods of silence may draw attention and prompt them to focus their intelligence collection efforts.

d. Set call signs for particular units or functions and unchanged, or infrequently changed, radio frequencies.

e. Distinctly identifiable message characteristics that indicate particular types of activity.

f. Requiring check-in and check-out with multiple control stations before, during and after a mission (frequently connected with air operations).

g. Formal or personal use of social media, including family member sites.

2A.5. **Equipment and system capabilities.** The following are examples of information and indicators of information that would identify specific equipment capabilities.

a. Unencrypted emissions during tests and exercises.

b. Public media, particularly technical journals.

c. Finance data that provides insight into a system.

d. The equipment or system hardware itself.

e. Information on test and exercise schedules that allows adversaries to better plan the use of their intelligence collection capabilities.

f. Deployment of unique units, targets and sensor systems to support tests associated with particular equipment or systems.

g. Unusual or visible security imposed that highlights their significance.

h. Notices that might highlight test areas.

i. Stereotyped use of location, procedures and sequences of actions, when preparing for and executing test activity.

j. Use of advertisements indicating that a company:

(1) has a contract on a classified system or component of a system;

(2) possesses technology of military significance; or

(3) has applied particular principles of physics and specific technologies to sensors and the guidance components of weapons.

2A.6. **Preparations for operations or activities**. The following are examples of information and indicators of information that would identify sensitive data during the preparatory phase of operations or activities.

a. Special supplies provided for participating elements.

b. Requisitioning of unusual volumes of supply items by a particular date.

c. Increased pre-positioning of stocks.

d. Embarking special units, installing special capabilities and preparing unit equipment with special paint schemes.

e. Procuring large or unusual numbers of maps and charts for specific locations.

f. Medical arrangements such as mobilizing medical personnel, stockpiling pharmaceuticals and blood, and marshalling medical equipment.

g. Focusing friendly joint intelligence, surveillance and reconnaissance collection capabilities against a particular area of interest.

h. Requisitioning or assigning an increased number of linguists of a particular language or group of languages from a particular region.

i. Initiating and maintaining unusual liaison with foreign nations for support.

j. Providing increased or tailored personnel training.

k. Holding rehearsals to test concepts of operation.

l. Increasing the number of trips and conferences for senior officials and staff members.

m. Arranging for tugs and pilots.

n. Requiring personnel on leave to return to their duty locations.

o. Declaring unusual off-limits restrictions.

p. Preparing units for combat operations through equipment checks and required readiness levels.

q. Accommodation or transportation arrangements for particular personnel or units.

r. Taking large-scale action to change mail addresses or arrange for mail forwarding.

s. Posting information on routine orders.

t. Storing boxes or equipment labelled with the name of an operation or activity or with a clear unit designation outside a controlled area.

u. Employing uncleared personnel to handle materiel used only in particular types of operations or activities.

v. Providing unique or highly visible physical security arrangements for loading or guarding special munitions or equipment.

w. Requesting unusual or increased meteorological, topographical or societal information for a specific area.

x. Setting up a wide-area network over commercial lines.

y. New or increased contracting activity.

z. Initiating, increasing or decreasing civil-military cooperation (CIMIC) liaison with non-military actors in a particular time and place.

2A.7. **The execution phase of operations or activities.** The following are examples of information and indicators of information that would transition to an execution phase.

a. Unit and equipment departures from normal bases.

b. Identification of friendly forces through communications security violation or physical observation of unit tactical symbols.

c. Stereotyped procedures and predictable reactions to adversarial actions.

d. Alerting the civilian population or any non-military organization in the operations environment.

e. Dumping rubbish.

2A.8. **Post engagement transition.** The following are examples of information and indicators of information that would identify force transition.

a. Repair and maintenance facilities' schedules.

b. Movement of supporting resources and maintenance personnel.

c. Medical-related activity.

d. Assignment of new units from other areas.

e. Search and rescue activity.

f. Personnel orders.

g. Discussion of repair and maintenance requirements in unsecure areas.

Intentionally blank

Annex 2B – Operations security measures

2B.1. The following list of operations security (OPSEC) measures is a guide only. The measures are applied to protect information that might be critical and indicators that are associated with the information and its management, as identified from Annex 2A. Development of specific OPSEC measures is as varied as the specific vulnerabilities they offset. They will depend heavily upon the North Atlantic Treaty Organization (NATO) capabilities available, the legal restraints a nation may be operating under, and the adversary's collection capabilities they are required to defeat. Measures can be broken down into operations and logistics measures, technical measures and administrative measures.

2B.2. **Balance of risk.** When considering OPSEC measures, the commander and staff should consider the potential impact of implementing OPSEC with operations in terms of time, resources, personnel or interference with associated operations. This impact should be balanced by the risk to the mission of an adversary being able to exploit a particular vulnerability. This will help determine which OPSEC measure is appropriate and sustainable without mission degradation.

2B.3. **Operations and logistics measures.** The following OPSEC actions may mitigate the risk of revealing operations and logistics EEFI.

a. Randomize the performance of functions and execution of missions. Avoid repetitive or stereotyped tactics, techniques and procedures for executing operations.

b. Employ force dispositions and command and control arrangements that conceal the location, identity and command relationships of major units.

c. Conduct support activities in a way that will not reveal intensification of preparations before initiating operations.

d. Transport supplies and personnel to combat units in a way that conceals the location and identity of the combat units.

e. Operate aircraft at low altitude to avoid radar detection.

f. Minimize the reflective surfaces that units or weapon systems present to radars and sonars.

g. Use darkness to mask deployments or force generation.

h. During hostilities, use physical destruction and electronic attack against the adversary's ability to collect and process information. Military actions in support of OPSEC may include engagements against the adversary's communications network, signals intelligence sites, radars, fixed sonar installations, reconnaissance aircraft and ships.

2B.4. **Technical measures.** The following technical measures may reduce the risk of revealing EEFI.

a. Improve resilience to cyberattacks, implementing appropriate risk mitigation measures based on the results of cyber intelligence.

b. Prepare for electronic attack by ensuring that appropriate electronic protective measures are in place.

c. Limit unsecure email messages to non-military activities and do not provide operational information.

d. Use encryption to protect voice, data and video communications.

e. Maximize terrain masking.

f. Use screen jamming, camouflage, smoke, background noise, added sources of heat or light, paint or weather conditions to mask activity.

g. Deactivation of flight tracking devices in the air domain and automatic identification systems in the maritime domain.

2B.5. **Administrative measures.** The following administrative measures may reduce the risk of revealing EEFI.

a. Limit unsecure telephone communications.

b. Avoid routine notices that reveal timings for events.

c. Conceal budgetary transactions,[19] supply requests and arrangements for services that reveal preparations for activity.

d. Conceal the issue of orders, the movement of specially qualified personnel to units, and the installation of special capabilities.

e. Control waste disposal or other housekeeping functions.

f. Follow normal leave and administrative patterns to the maximum extent possible prior to starting operations.

g. Ensure that personnel discreetly prepare for their families' welfare.

h. Provide family OPSEC briefs to inform family members of the need for OPSEC.

i. Ensure that personnel are aware of OPSEC vulnerabilities presented by online social networking and use of smartphones and other smart devices when

[19] For some NATO states concealing budgetary transactions may not be in accordance with their national laws.

posting information about changes in personal or unit routines that could indicate operations planning or other details.

j. Ensure that adequate policy and procedures are in place for shredding or destroying documents.

k. OPSEC training provided to all personnel involved in the operation or activity.

Intentionally blank

Chapter 3 – Deception

Section 1 – Introduction

3.1. Deception at the operational level misleads an adversary about the joint force commander's (JFC's) conduct of operations in their joint operations area, to preserve freedom of action. Operational-level deception may support a strategic deception plan, involving force elements and resources outside of the joint operations area. Operational-level deception may require coordination with the strategic headquarters and other government departments and may require approval of the strategic commander. Operational-level deception will also direct deception plans down to the tactical level and the component commanders, as tactical action can have strategic effects and consequences.

3.2. Operational-level deception operates within the medium to short term. It aims to achieve a positive result that supports the commander's plan. Planned centrally, it maintains operations security (OPSEC) and continuity from the strategic to the tactical level. It should unfold logically and realistically, feeding the adversary with the combat indicators they would expect to see, yet not so obviously as to raise suspicion. Adversarial intelligence must have enough time to collect and interpret false information, but not sufficient time to conduct too thorough an analysis.

3.3. **Appropriate conditions to conduct deception.** Consider deception if favourable conditions for its successful execution exist and it is likely to provide significant advantage. This is a decision for the JFC and their staff based upon the experience and judgment. Conditions when using deception may be appropriate include when:

- the adversary has an advantage that cannot be overcome without using deception – force strengths, capability, agility or situational awareness;
- the adversary has known preconceptions that can be exploited;
- the adversary has known flaws in their decision-making process;
- the adversary is under pressure to act;
- deception will enhance OPSEC;
- deception will enhance the effectiveness of a conventional approach; or
- a target can only be influenced indirectly.

3.4. **Risk.** Deception planners must understand the risks involved in carrying out deception and must utilize the risk management process in presenting courses of action (COA) to the commander. Deception should be considered a high risk activity if:

- appropriate conditions to conduct deception do not exist;
- the target has a record of detecting deception;

- the understand process is incomplete or inconclusive – the target's likely behaviour in relation to the use of deception cannot be anticipated with any accuracy;
- insufficient knowledge exists of the adversary command and control and intelligence capability; and/or
- the adversary becomes aware that they are being deceived then the plan may not only fail but it could lead to adverse consequences by encouraging detailed re-evaluation of friendly forces COA.

3.5. **How much deception is required?** Deception can be effective even with a small amount of information placed across a wide variety of channels. For both ambiguity decreasing deception and ambiguity increasing deception the consistency of the deception input is important. In both cases, multiple channels used with consistent data will increase the likelihood of target audience acceptance, as verifiability is obtained. Planners should employ only as many deceptive activities as required for the targeted decision-maker to take the action (or inaction) that will create the desired exploitable advantage.

Operation DESERT STORM (1991) – The Hail Mary[20] deception play

'The movement of the enemy's columns into battle can be ascertained only by actual observation – the point at which he plans to cross a river by the few preparations he makes, which become apparent a short time in advance; but the direction from which he threatens our country will usually be announced in the press before a single shot is fired. The greater the scale of preparations, the smaller the chance of achieving a surprise.'[21] Although Clausewitz was discussing strategic reserves in this passage, he identifies the opportunity for achieving surprise by deception, while also alluding to the challenges and opportunities of operating within the information environment of his time. General H Norman Schwarzkopf (commander of the coalition forces deployed on Operation DESERT SHIELD during the 'Gulf War' 1990/1991) also understood this.

A large-scale deception operation was critical to the coalition's plan to liberate Kuwait from the Iraqi forces of Saddam Hussein. The Iraqi forces were deployed in a series of defensive lines focused on preventing the forced withdrawal of Iraqi forces from illegally occupied Kuwait from a coalition of 39 nations, deployed on the Saudi Arabia border and afloat in the Persian Gulf, against which the Iraqis had numerical superiority. Through **multiple approaches** from the political to the operational level, the coalition deception plan **reinforced the existing beliefs** of the Iraqi high command that the coalition would not attack through Iraq but only through Kuwait and in doing so they would approach from the east incorporating an amphibious landing. A deception operation was a **credible, consistent, verifiable and executable** option, as Iraqi forces faced a coalition that appeared to be deployed to fight another protracted attritional Iran-Iraq war (1980-88) – warfighting the Iraqis were well prepared for, channelled by a desert to the west that the Iraqis believed was too difficult to navigate in or manoeuvre through. The coalition, however, was designed for manoeuvre warfare, with air,

[20] A 'Hail Mary' is an American sports term for a desperate sports play with little chance of success.
[21] Carl von Clausewitz, *On War*, Oxford University Press, page 149.

intelligence and technological superiority and, critically, an ability to navigate by global positioning system (GPS). Schwarzkopf believed Western news media was a major source of intelligence for the Iraqi command and **targeted the decision-makers** through this media. The **behavioural response** sought was for the Iraqi forces to maintain their defensive dispositions, including holding their Republican Guard Forces (the identified centre of gravity) in reserve, with a firm focus on an amphibious-enabled assault in the east.

Figure 3.1 – Operation DESERT STORM

Multiple approaches from the operational to the tactical level were used to **reveal the false** marine assault from the Persian Gulf and **conceal the real** redeployment of forces from the coast to the western flank from which they could outmanoeuvre the Iraqi defensive line. United States Marine Corps briefings, preparations and training were well covered by the news media and reinforced by psychological operations (PSYOPS) products. A relief in place, dummy positions, noise deception, electronic signature deception, and active engagement of Iraqi forces combined with overt manoeuvring of formations, maintained the appearance of an assault focused in the east. The major land force[22] moved west, with coalition air and artillery attacks neutralizing the Iraqi's ability to see beyond the lines of sight being left open to them. A deception force of some 20,000 troops faced an Iraqi defensive force of some 80,000 troops by the time

[22] Some 100,000 troops and 20,000 vehicles with 60 days supplies.

the coalition launched the real Operation DESERT STORM offensive that outflanked and trapped the Iraqis in Kuwait. Deception operations were maintained throughout, to convince the Iraqis that a major assault would still materialize from the east. The 'Hail Mary' play set the conditions for the successful conclusion of Operation DESERT STORM.[23]

Section 2 – Deception process

3.6. Deception is as much about thinking as executing and needs to be a creative process. The six-step deception process below outlines the required approach to enable deception at the joint level.

Figure 3.1 – The six-step deception process

[23] Bibliography for this vignette box: *Deception in War* (Jon Latimer); *Military Deception: Hiding the Real – Showing the Fake* (Major Mark Johnson and Major Jessica Meyeraan); and T*he Role of the Media in The Operational Deception Plan for Operation Desert Storm* (Lt Col Douglas Armor).

3.7. **The operations planning process.** The operations planning process[24] (OPP) defines the sequence of planning activities as:

- initiation;
- mission analysis;
- COA development;
- COA analysis;
- COA validation and comparison;
- commander's COA decision; and
- concept of operations (CONOPS) and plan development.

3.8. **Relationship of the deception six-step process with the operation plan.** The deception plan supports the operation plan (OPLAN). It is nested and integrated within the OPLAN to achieve coherence, yet forms a discrete and often compartmentalized area of planning effort. Deception planning happens parallel to all stages of the OPP. It contributes to the understanding generated in the initiation, it takes its direction from mission analysis and a skeleton deception plan supports COA analysis, validation and comparison. The skeleton deception plan will outline four basic elements for each COA: objective; target; story; and plan. After COA selection, the deception plan itself (the plan within the plan) is further developed. Figure 3.2 illustrates this relationship.

[24] See Allied Joint Publication (AJP)-5, *Allied Joint Doctrine for the Planning of Operations*.

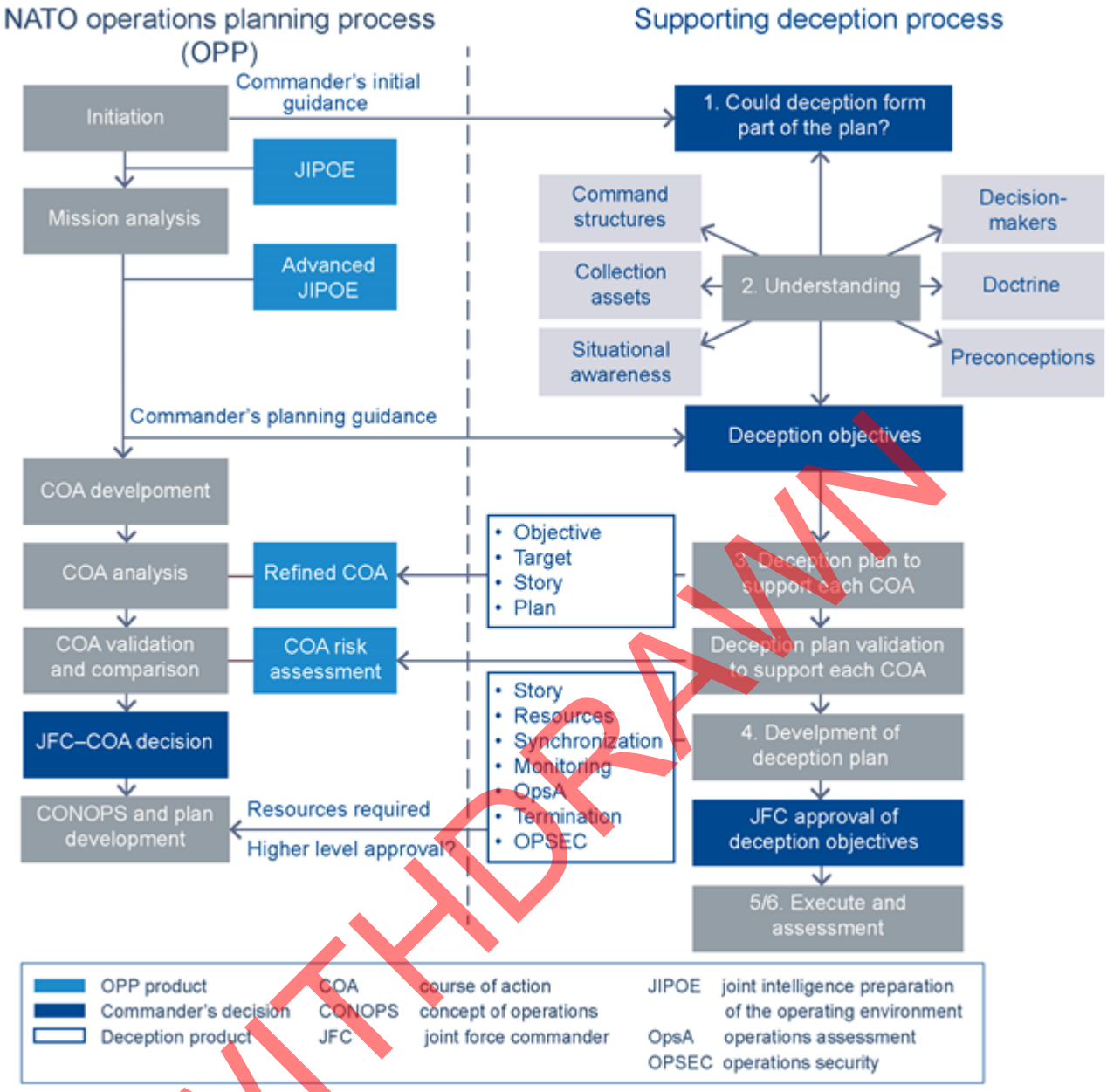


Figure 3.2 – The relationship between the OPP and the deception six-step planning process

3.9. At initiation, the JFC will provide initial planning guidance and warning orders based upon the mission and current understanding of the operating environment. At this stage deception planning staff should evaluate the possibilities for deception to be part of the OPLAN.[25] Mission analysis will identify intent, outcomes, objectives and any situation change. Outputs from mission analysis are initial operations design

[25] Deception is contained in Appendix 3 (Opsec and Deception) to Annex UU (Info Ops) but may also be contained in a separate fragmentary order (FRAGO).

and the commander's planning guidance, which will contain deception objectives, if required, and should provide sufficient information to initiate deception planning.

Section 3 – Understanding

3.10. Understanding provides the foundation for successful deception, allowing the deception planner to assess the adversary's vulnerabilities (collection assets in the physical and virtual spaces of the information environment) and preconceptions (cognitive space). The deceiver must think like the adversary and not project their own assumptions and values onto them. Deception staff must also recognize their own biases and assumptions, and those of the organization to which they belong. It is important to be cautious of mirror imaging, the belief that the adversary will behave in a similar manner to friendly forces.

3.11. **Intelligence support to deception.** Intelligence is the foundation of a deception plan. The joint intelligence estimate[26] is essential in providing the deception planner with the potential instances in which deception could thrive, as well as the chances of its success. The intelligence estimate will seek to understand the totality of the operating environment, ranging from battlespace area evaluation to a detailed understanding of the societal factors and an analysis of the adversary's capabilities and intentions. It is essential that J2 collects against the totality of the adversary's command, control and decision-making apparatus, with particular attention paid to trying to understand what assessments adversarial intelligence is making; this will allow the deception planner to scope the possibility of a deception plan. It is also critical for the J2 branch to assist the deception planner to understand the overall information environment, to include the social media landscape and the way information flows in the country or countries forming the joint operations area. Understanding the relationships between populations and civil society and both hostile organizations and friendly forces is critical. These relationships present a potential channel of influence, as well as a potential channel for risk of exposure of friendly force intent. A list of intelligence requirements to support deception is at Annex 3B.

3.12. **Command structures.** Knowledge of the adversary's command structure and command and control practices is essential, in particular which decisions occur at which level and by whom. If a flat command structure exists with relatively few collection or analysis assets, they may struggle to cross-reference material (a risk to the deception plan) or may overlook deceptive information completely. Command structures and intelligence apparatuses associated with modern militaries may have the ability to process large and complex data sets of information but their hierarchical structures may expose vulnerabilities when they have to react quickly to events.

3.13. **Collection assets.** The deception planner must identify what adversarial collection assets are actually available to enable adversarial detection of deception. This will determine the ways and means used to create the deception effect. It will also

[26] AJP-2, *Allied Joint Doctrine for Intelligence, Counter Intelligence and Security,* page 6-1, paragraph 6.3.

identify the timeline within which a behavioural response could be expected or identified.

3.14. **Situational awareness.** The extent to which the adversary is already aware of friendly force intentions should be established. It should include what friendly forces have already said about their intentions and the development of their strategic narrative.

3.15. **Decision-makers.** The deception planner must evaluate which key leaders or decision-makers are most appropriate to exhibit the required behavioural response to meet the commander's desired effect. Factors to be considered in this evaluation include identifying:

- structures within the adversary's chain of command;
- trusted sources of information of the targeted decision-maker; and
- biases, prejudices and preconceived ideas of the adversary that create vulnerability to deception.

3.16. **Doctrine and preconceptions.** It is critical to have a detailed and accurate knowledge of adversary perceptions, actions, doctrine, tactics, techniques and procedures and their situational awareness of friendly force intentions and plans. Predispositions based on beliefs, values and stereotypes govern adversarial reactions. This can allow the deceiver to gain an advantage from a motivational bias, where the deceiver can use supporting evidence to strengthen the target's predispositions and make them believe what they expect to believe. It is generally easier to maintain an existing belief than to change it.

Section 4 – Operations planning process

3.17. **Initiation.** In the joint intelligence preparation of the operating environment,[27] operations planners should identify the requirement or opportunity for deception and know if the force has any part in a higher-level deception plan. Based on a realistic assessment of the likelihood of success and a risk/benefit analysis, the deception planner will recommend whether deception is appropriate and what resources would be required to make a plan successful. This requires an analysis of the time available, the level of friendly force understanding, the availability of resources, the adversarial collection and analytical capability and their ability to react to the plan and change their behaviour. The commander should issue initial guidance on a need-to-know basis as to whether or not deception is likely to form part of the plan and, if it will, provide priorities for resources to support the deception planning.

3.18. **Mission analysis.** Wherever possible, the deception and mission analysis develop in unison, integrating real and simulated events to develop the desired picture. It is important to see events from an adversarial perspective, to determine which indicators they must detect to come to the desired conclusion, bearing in mind the

[27] Also known as the comprehensive preparation of the operational environment (CPOE) in NATO's comprehensive operations planning directive (COPD).

adversary's doctrine, personalities, existing knowledge and preconceptions. On approval of the COA and deception objective, the deception plan development begins with the mission objectives; the behaviour required from whom and whether it is a specific action or inaction.

3.19. **Course of action development, analysis, validation and comparison.** The initiation and mission analysis have identified potential decision-makers to target. During COA development, the deception planner will produce deception plans to support each COA. Each COA will be analyzed for its strengths and weaknesses with the deception element considered alongside the main plan. The COA analyses should also identify the expected adversary's reaction. This allows the commander to validate the benefit gained from deception against the resource cost. The deception plan will be the one that best supports the commander's chosen COA and will require further development during the CONOPS and plan development. Each deception plan should use the following framework.

a. **Objective.** The JFC's planning guidance, developed from mission analysis, should provide deception goals and objectives, which may be different for each COA. The deception objective is a concise statement of what the commander wishes the adversary to do, or not to do, and how it will contribute to successful completion of the mission. This will provide the deception planner with a clear aim. The objective is expressed as a positive result, such as 'deception will ensure the adversary does not commit its reserve due to the belief that they are threatened from another flank/direction'. The target, story and plan are variable and manipulated to form different approaches to achieve the objective.

b. **Target.** The target decision-maker(s) identified during the understanding phase becomes the focus of the story and the plan. This is because they can change the behaviour of the adversary to meet the deception objective. Knowledge of the target decision-maker's traits: speed of decision-making; clarity of information required before issuing orders; willingness to accept risk; and which collection assets they most trust should be taken into account as part of the target selection process.

c. **Story.** Develop a story that will convince the target to behave in the desired way using the deception techniques and maxims outlined in Annex 3C. A method for developing a credible, verifiable, consistent and measureable deception story is at Annex 3D. Seek to reduce the adversarial collection and analytical capability to detect the deception and thus reduce their chance of making the true sense of what is happening.

d. **Plan.** The plan will detail the deception and the resources required to execute and monitor the adversary's reaction to it. Activities should be sequenced to maximize the portrayal of the deception story for the required period. Identify the timelines required to deliver the activity, for the target to evaluate it and subsequently act upon it. The time available for planning will affect what is

achievable. A matrix for presenting the outline deception plan to support COA development, analysis, validation and comparison is at Annex 3E.

3.20. **Concept of operations and plan development.** Once the commander has selected the COA, consider consulting deception planners from component commands to identify how their forces can support the deception plan. There needs to be vertical and horizontal coordination of deception plans. Horizontal coordination may be required at the joint level to make sure that one deception plan does not undermine another. Vertical coordination is required to confirm that tactical deceptions do not undermine operational-level deception plans. In turn, any operational-level deception should not undermine or expose the strategic plan. Coordination will have to take place not just between deception planners at various levels but also between deception planners and other staff planners. For example, the deception planner may require the adversary to monitor electronic warfare transmissions and therefore their capability to do so should not be jammed or destroyed via the targeting process.

a. **Resources.** The planner must identify the activities and indicators that require resourcing to deliver the developing story and its monitoring. These activities may be delivered by component commands; the deception planner must be satisfied that the indicators being shown to the adversary can be discovered and identified.

b. **Synchronization.** A sequential plan should be developed with a detailed list of necessary resources, as failure to implement a stage, or a deviation in timings, could result in a misinterpretation of the indicators, or could compromise the operation. The plan should include the desired adversary's reaction to each event, for use in the monitoring process. Sequence the deception to maximize the portrayal of the deception story.

c. **Monitoring.** Feedback is paramount; a resourced collection plan will facilitate exploitation of the deception. The intelligence collection plan will attempt to identify if the deception is being accepted, rejected or deceptively countered. Nominate deception-related priority intelligence requirements and establish named areas of interest and target areas of interest.

d. **Operations assessment.** The deception plan should include the desired reaction to each significant sequence of events, so that the deception planner knows whether the adversary is responding and behaving in the desired manner. This desired reaction may itself become a commander’s critical information requirement in its own right. The operations assessment (OpsA) process will enable the measurement of progress and outcomes of the deception and assist the commander in evaluating the benefit of the deception. See Section 6 for more detail on OpsA.

e. **Termination.** The termination of a successful deception must be included in the plan. Even when the deception is successful, commanders and their staffs may wish to keep all, or elements, of it undisclosed. Consider if the termination plan itself requires deceptive activities to hide the original deception. Early

termination may also be required if the deception is compromised. The termination element to the plan should incorporate the following:

(1) a description of each potential termination scenario;

(2) the steps for initiating termination of the deception in each of the scenarios; and

(3) identifying the commander who has termination authority.

3.21. **Operations security.** Supporting capabilities require enough knowledge to accomplish their tasks without drawing undue attention to their activities. It is important to coordinate deception planning with the OPSEC process to reduce the adversary's ability to detect and determine the planned deception. This coordination does not solely rest within the planning phase; it must also take place through the execution and at termination. For OPSEC purposes, give the deception plan an operation name and do not refer to it as the deception plan.

3.22. **Plan approval.** The commander may review the deception plan and approve it as part of normal operations, or may wish to compartmentalize the approvals process due to sensitivities. Consult the legal advisor (LEGAD) and the political advisor (POLAD), and where appropriate information operations (Info Ops), prior to seeking approval. The approval authority for deception at the operational level will initially be Supreme Allied Commander Europe (SACEUR); SACEUR may delegate authority. Certain capabilities or assets used to implement deception may also require approvals at a higher level than the JFC; address this as early as possible. The operational-level targeting process will provide guidance on any restraints or constraints during target development.

3.23. **Plan distribution.** The deception plan should be distributed as an annex to the OPLAN only for those staffs that require knowledge of its existence. To reduce the risk of compromise, units and formations involved in the implementation of deception should know only enough to fulfil their role in the plan but not to compromise the overall plan.

Section 5 – Execution

3.24. **Persistent presence and disclosure.** The requirement for OPSEC means that monitoring any alterations to friendly force plans and activities is as important as adversarial activity. It ensures that commanders who are not aware of the deception plan do not inadvertently alter the target, the story, or resources for the plan, through lack of awareness. Decide which staff officers and subordinate commands should be aware of the deception plan. The output of macro-level boards such as the Information Activities Coordination Board (IACB) and Joint Targeting Coordination Board (JTCB) should be monitored.

3.25. **Situational awareness.** Executing a deception plan may be extremely complex and will involve extensive coordination between many separate elements of the force

and potentially elements external to the force. It will be implemented over a period of days or even, in some cases, weeks. It will contain many interdependent events, with seemingly minor occurrences (and their subsequent implantation in the adversarial mind) many days previously, giving credence to later, larger events. Therefore, changes to the plan require detailed consideration of all available intelligence derived from the monitoring process. It is also possible that later changes, unless very carefully implemented, could compromise earlier stages of the operation by revealing inconsistencies.

3.26. **Coordination.** Within the execution phase, coordination within the staff is critical to ensuring activities occur as planned. This will ensure early detection of any failure to execute the plan as intended. Any changes to the operations deception plan during the execution phase will also require close coordination within the staff.

3.27. **Synchronization.** Tight control of the synchronization of events is required to allow events to unfold at a pace that allows the adversary to build up the desired picture. This will ensure events unfold as would be expected from the adversarial perspective. Deception staff must ensure they are aware of any failure of execution in accordance with the plan, to evaluate the requirement for corrective action. This requires agreement within the staffs. An inherent danger of deception is the risk of deceiving or confusing friendly forces, so personnel or commanders should be briefed thoroughly, but on strict need-to-know basis.

3.28. **Monitoring.** J2 should focus on the measure of effectiveness (MOE) included in the deception plan, to determine whether an adversary is responding in the manner intended. If there are no identifiable activities indicating the required behaviour, the intelligence section should be asked to identify the reasons. While the deception may have implanted the desired impression in the adversarial intelligence organization, it may be that the commander is unwilling or unable to react to it in the desired way. Any intelligence effort to monitor deception MOE should not in itself compromise the deception by paying undue attention to a particular part of the operation. There is a need to continually monitor the methods used to communicate the deception story to ascertain the need for modification. This will involve close coordination with J2. Through monitoring, it can be decided when the deception plan should be terminated.

3.29. **Modifying the deception.** There are circumstances under which modifications to the deception plan will be appropriate but where termination is not yet required. It may then be necessary to reduce the flow of indicators, increase the flow of indicators, or change the indicators themselves. Such circumstances may include when: the adversary has suspicions about the indicators fed to them; counter-deception has been identified: events have caused the indicators to have been missed; or the way the adversary receives information is not as first predicted. The deception may also need to be modified due to operations failure such as: the wrong target has been chosen for the deception; the adversary collection assets are more limited than thought and cannot verify the deception; or that the story is not believable or consistent.

Terminating the deception

3.30. The deception should be terminated in a manner that protects the interests of the deceiver. The objective of a successful termination of a deception plan is to conclude the deception without revealing the deception. This will involve terminating each deception event in a manner that does not leave suspicious evidence.

3.31. Termination of the deception plan can occur due to a number of reasons. Some examples are below.

a. **Success.** The deception plan is successful and the operations objectives are achieved.

b. **Failure.** The operation has failed and there is no benefit in continuing the deception.

c. **Change of mission.** The operational situation may have changed, leading to a revision of operations objectives, which makes the current deception plan obsolete.

d. **Change of situation.** The operational situation changes and although not requiring a revision of operations objectives, it requires a re-evaluation of the benefit and risks of the deception. This may lead the commander to end the deception component.

e. **Compromise.** It is believed the deception has been recognized.

f. **Timing**. Execution of the deception does not proceed in alignment with other related activities, or the speed at which the adversary is reacting to the deception does not support the overall operation sufficiently to succeed.

3.32. The actual method of terminating a deception event will depend on how the target would expect the event to conclude. This will play to their preconception and bias. Termination actions include: remaining silent about deception, denial, and creating a further deception to mislead.

3.33. The JFC will hold the authority to terminate the execution of military deception. However, the JFC may delegate termination authority to component commanders if rapid decisions are required to protect scarce military resources. This will still usually require coordination with higher-level command prior to decisions taken at the component level.

Section 6 – Assessment

3.34. Deception OpsA design must be part of the initial planning process. OpsA monitors progress during the execution of the operation and provides evidence-based support for evaluating the success or failure of the deception plan. Integrating OpsA into the deception planning cycle could also enable identification of potential second

and third order effects and unintended consequences. OpsA measures progress using measure of performance (MOP) and MOE. MOP refers to actions being executed as planned and MOE is metrics aimed at monitoring if the plan is on track. Key elements of an evidence-based approach are as follows.

a. **Evidence.** Information used to establish proof.

b. **Source.** A place, person or thing from which the evidence originates.

c. **Indicator.** Data used to point out or demonstrate a state or level.

d. **Data.** Facts and statistics used for reference or analysis.

3.35. **Deception assessment process.** The assessment plan must support the deception plan's previously agreed theory of behaviour change, and the measurable behavioural outcome that it seeks to achieve. NATO doctrine[28] has developed the four stages of OpsA, interpreted as follows for deception.

a. **Stage 1 – Assessment design and support to planning.** Designing assessment is part of the initial planning phase of the operation. It will support COA development, analysis, validation and comparison. It requires a collection and analysis plan to be resourced, and should identify how evidence will be gathered, interpreted and recommendations made.

b. **Stage 2 – Developing a data collection plan.** Data collection articulates the procedure for collecting indicators and their time-sensitive monitoring, as they relate to the measurable behavioural outcome. Collect the evidence used to underpin the assessment from a variety of sources. This is the mixed methods approach, collecting both qualitative and quantitative data. Quantitative data (i.e., what people do) provides numbers and allows analysis of data across time (also known as trend analyses). Qualitative data (i.e., what people say) provides an understanding of the context and meaning that underpins the quantitative data.

c. **Stage 3 – Data collection and treatment.** The collection and treatment of evidence should be conducted continuously during the execution phase of the operation. To achieve this, it is necessary to establish a baseline of evidence prior to the execution phase beginning.

(1) **Establish a baseline before the operation.** All assessments require an evidential baseline; a pre-operation baseline to gauge progress during the operation against eventual outcomes post-operation. If the deception plan does not establish a baseline, the staff will not be able to establish what has changed as part of the deception plan, or understand eventual success or failure.

[28] AJP-3, *Allied Joint Doctrine for the Conduct of Operations*.

(2) **Monitor the plan.** Planned, periodic monitoring not only helps to inform decision points, but it also helps to understand if the situation has changed, therefore supporting the common operational picture (COP). Be aware that additional or alternative sources and indicators could emerge during the execution of the deception. Therefore, periodically the collection and monitoring plan should be reviewed and updated if required.

3.36. **Stage 4 – Analysis, interpretation and recommendations.** Conduct analysis, interpretation and recommendations continuously. A sound deception story, well executed with a robust analysis plan, based on a mixed methods approach, will allow robust analysis. This in turn will allow recommendations to support agreement on desired effects and contribute to the overall evidence required to inform the commander's decision-making process.

Intentionally blank

Annex 3A – Cognitive factors in deception

3A.1. The aim of deception is to achieve an observable behavioural response in the deception target. The cognitive approach attempts to understand how functions such as attention, perception, memory, reasoning, sense-making, problem solving, emotion and decision-making are organized and operate within the human brain to produce behaviour (see Figure 3A.1).

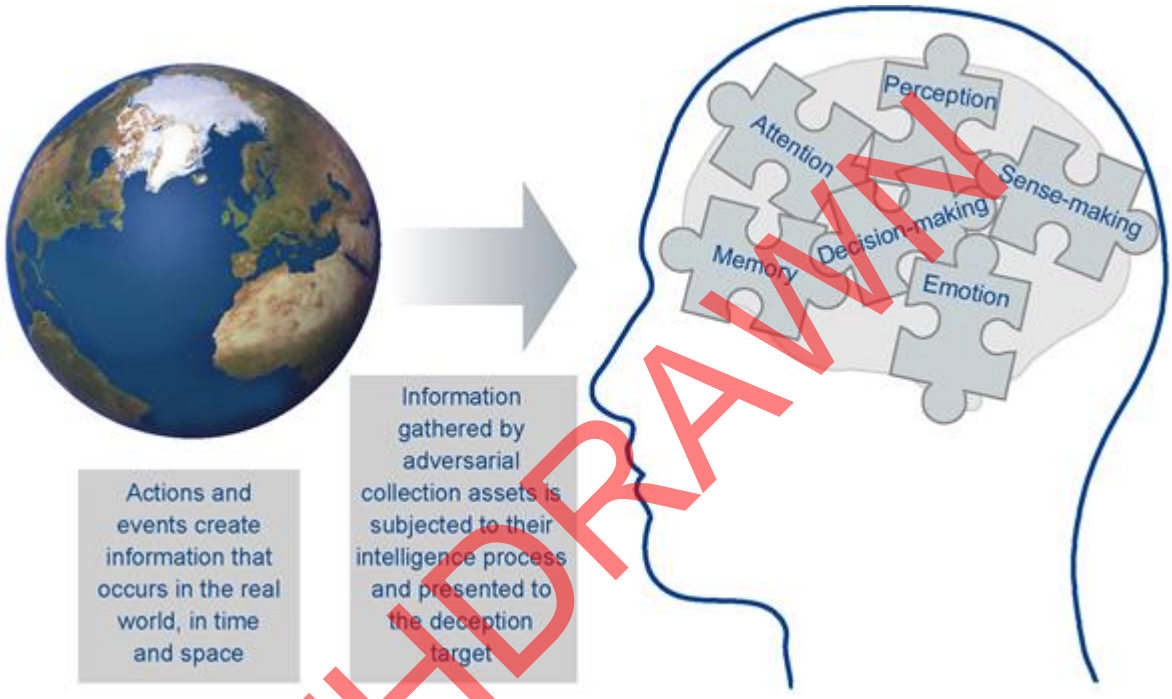


Figure 3A.1 – A basic representation of human cognition

3A.2. The cognitive functions combine to help an individual make sense of their environment; this is commonly referred to as ‘sense-making’. In simple terms, the deception planner needs to consider the following from the target’s perspective:

- what do I notice (attention);
- how do I perceive it (perception);
- what does this mean (sense-making);
- how do I feel about it (emotion); and
- what do I do about it (decision-making)?

The culmination of all of this is a behavioural response, expressed by the deception target as some form of action (do something), or inaction (do nothing). Therefore, cognition is a dominant factor, not just for deception, but also for operations security (OPSEC) and counter-deception.

3A.3. Knowledge of human cognition has developed significantly. Modern science has helped to develop the discipline of cognitive neuroscience and cognitive psychology has identified how the human brain is prone to systematic errors and biases. Humans are no longer viewed as 'rational actors' that methodically process information devoid of impulse and emotion. Specific areas of the brain do not process information in a sequential manner for specific functions, but rather, multiple regions of the brain are involved in simultaneous processing across different functions. The brain is an economical and efficient organ designed to get the job done, as opposed to an organ optimized to do the job perfectly. Therefore, successful deception exploits how the brain processes information.

Social influences on cognition and decision-making

3A.4. Cognitive processes occur inside people's heads but also between people in teams and social groups. Therefore, it is necessary to consider the social factors that influence sense-making and decision-making involved in OPSEC, deception and counter-deception. The inclusion of social factors within human cognition is known as social cognition, or the socio-cognitive approach. Findings from social psychology are useful in understanding how social factors can influence group behaviour and task performance because this underpins sense-making and decision-making. This is important because the eventual outcome of any deception plan is to influence adversarial decision-making. Some of the theories and concepts within social psychology that have been found to influence decision-making include groupthink, group polarization, minority influence, group cohesiveness, conformity and obedience. As with the cognitive perspective, these social concepts hold opportunities and challenges for creating behavioural outcomes in terms of OPSEC, deception and counter-deception.

Historical example – Yom Kippur War

The following example illustrates how cognitive and social factors can influence sense-making and decision-making in order to deceive. On the 6th October 1973, Egyptian forces executed a successful surprise attack on Israel by crossing the Suez Canal at the start of the Yom Kippur War. Israel underestimated the Egyptians by holding **preconceived**, and **socially-agreed**, **beliefs** and **attitudes** that Arab Forces generally lacked effective unity, as well as poor command and control – this is what Israel's politicians and military commanders were **willing to accept**. The Egyptians deliberately **reinforced** these **perceptions** at the strategic level through diplomatic channels, which appeared to point at policy disagreements with neighbouring Arab countries. At the operational level, the Egyptians repeatedly mobilized and demobilized their forces, **establishing a pattern of activity**. The Egyptians staged numerous deployments into the area by deploying large quantities of men and equipment, as well as constructing tank ramparts and practising river crossings, thereby creating both **illusions** and **distractions**. Egypt also stood down some 20,000 troops prior to offensive action.

Initially, Israel paid **attention** to the Egyptian behaviour by mobilizing their own forces. The repeated Egyptian behaviour, which was **credible, consistent and verifiable**, **conditioned** Israel's **perceptions** and their **expectations**, which influenced their **sense-making** and **decision-making**. Eventually, Israel's **behaviour** was one of **inaction**, mostly ceasing to react to the Egyptian movements and not fully mobilizing in response. The result was that on the 6th October 1973 Egyptian forces executed a successful surprise incursion across the Suez Canal by doing precisely what they had practised, but not concluded, on the many previous occasions.

Paradoxically, this example also demonstrates the importance of knowing one's adversary. Ultimately, Israel was able to mount a successful counterattack because Egypt failed to assess the consequences of launching their attack over the Jewish religious holiday of Yom Kippur; during the holiday, most Israeli reservists were at home and therefore, easy to contact. In addition, during Yom Kippur unnecessary travel was disapproved of, therefore most of the roads were clear. Israel was able to rapidly mobilize men and advance to contact with the Egyptians.

Intentionally blank

Annex 3B – Intelligence requirements to support deception

3B.1. The following are examples of intelligence requirements on the adversary that should be considered; their priority may change based on situation.

a. Capabilities and weaknesses of intelligence, surveillance and reconnaissance (ISR) capabilities, including those of North Atlantic Treaty Organization (NATO) partners and international organizations.

b. Capability to process and analyze information and intelligence.

c. Capabilities and weaknesses of the command, control, communication and information systems.

d. Profiles of key leaders and military commanders and advisors, including analysis of their decision-making processes and identification of biases/preconceived perceptions.

e. Analysis of the relationship between the military command and the national decision-making apparatus. Deceiving the military command might be fruitless if it cannot influence its national government.

f. Historical assessment of susceptibility to deception in recent conflicts.

g. Identification of suitable avenues to exploit in the deception plan at the operational and strategic level.

h. Current intelligence on the order of battle, force dispositions and any changes or re-deployments because of deception.

i. Identifying necessary operations security (OPSEC) measures in support of the deception plan, including neutralizing or destroying ISR capabilities.

j. Monitoring progress and effectiveness of deception plan.

k. Assessment of deception doctrine, tactics, techniques and procedures.

l. Counter-intelligence support to deception.

Intentionally blank

Annex 3C – Deception techniques

3C.1. Deception techniques have developed from social science, historical evidence and operational lessons learned. Consider the following deception techniques, to assist in developing the deception plan.

a. **The obvious solution.** Reinforce the impression of taking an obvious or expected approach to achieving the objective, whilst actually taking a different course of action (COA). This approach links with the false routine.

b. **The false routine.** Condition the target by repetition to believe you are pursuing an apparently standard routine, whilst in fact preparing a quite different COA. This approach links with the obvious solution.

c. **The substitution.** Lead the target to believe nothing has changed by covertly substituting the false for the real, and vice versa.

d. **The lure.** Present the target with what appears to be a sudden or ideal opportunity they must exploit, whilst in fact luring them into a trap. This approach links with the deliberate leak.

e. **The deliberate leak.** Deliberately disseminate information via agents, or other clandestine links, in such a way the target audience believes they have obtained a piece of vital intelligence through skilful intelligence work. This approach links with the lure.

f. **The mistake.** Lead the target to believe valuable information has come into their possession by mistake, through a breach of security, negligence or inefficiency. This approach links with the piece of bad luck.

g. **The piece of bad luck.** Convince the target they have acquired information of vital importance by accident, because of a train of circumstances over which friendly forces had no control. This approach links with the mistake.

3C.2. **Deception maxims.** The following maxims also apply.

a. **Magruder's principle.**[29] It is generally easier to induce a deception target to maintain a pre-existing belief than to deceive the deception target into changing that belief.

b. **Jones' Dilemma.**[30] Deception becomes more difficult as the number of sources available to the deception target with which to confirm the real situation increases. However, the greater the number of sources that are deceptively manipulated, the greater the chances the deception will be

[29] United States Joint Chiefs of Staff, (2017), Joint Publication 3-13.4, *Military Deception*. Washington DC, USA: US DOD.
[30] *Ibid*.

believed. Confirmation of the deceptive information by a number of credible sources can help to reinforce the deception.

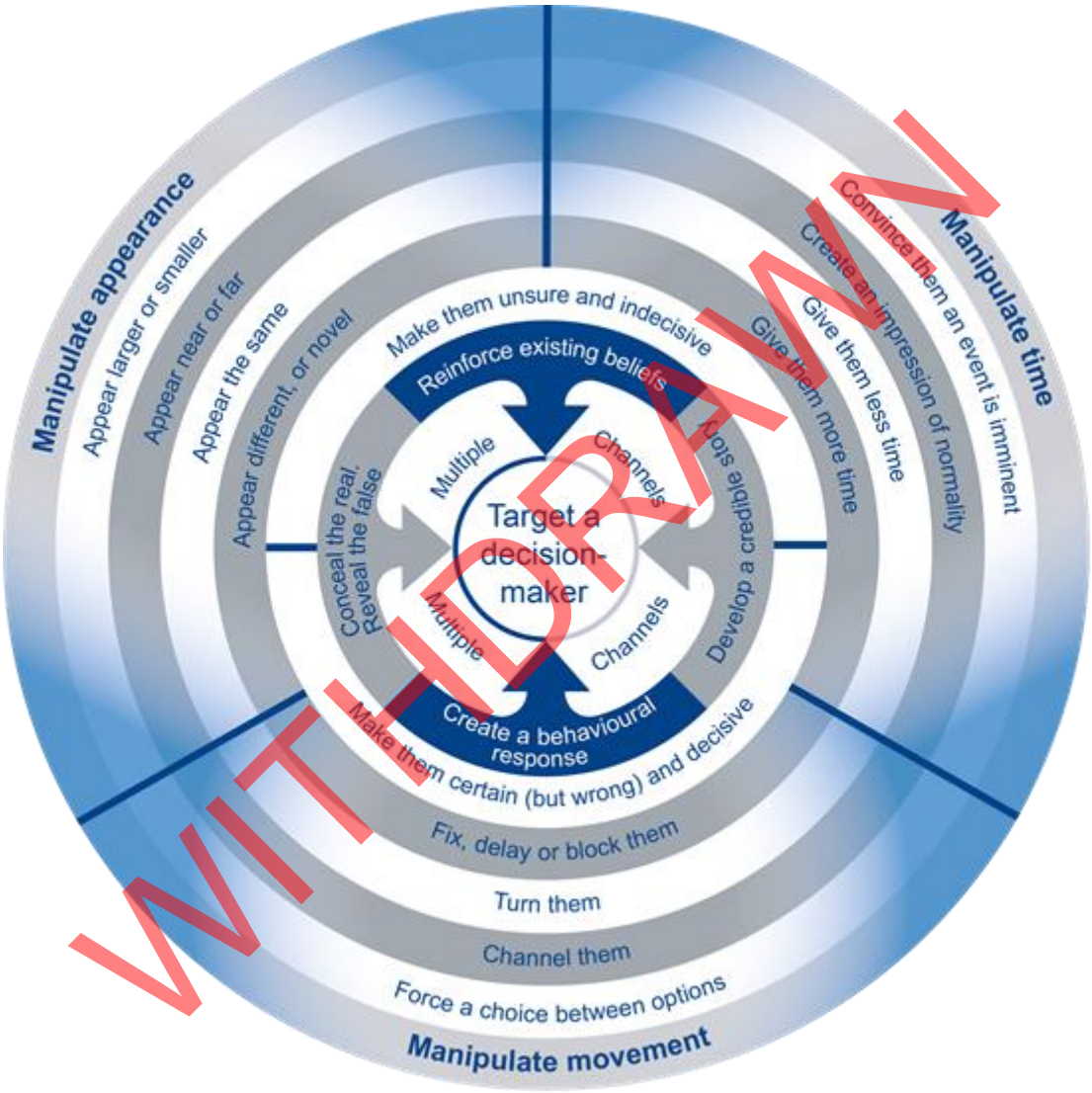
c. **The inability to process small change in indicators over time.** Deception targets have proven vulnerable to not detecting small changes in essential elements of friendly information (EEFI) and indicators, even if the cumulative change over time is large.

d. **Ambiguity enhancing or ambiguity reducing.** Ambiguity enhancing deception causes the targeted decision-maker to become increasingly uncertain of the situation. Ambiguity reducing deception causes the targeted decision-maker to become certain, decisive and yet wrong.

Annex 3D – Deception story development

3D.1. 'All warfare is based on deception. Therefore, when capable, feign incapacity; when active, inactivity… Offer the enemy a bait to lure him: feign disorder and strike him… Pretend inferiority and encourage his arrogance.'[31] This Sun Tzu maxim can be applied to a basic model to support development of a deception story. The model shown in Figure 3D.1 is offered as an example of such a tool.

Figure 3D.1 – Deception story development model



[31] Sun Tzu, *The Art of War*.

Intentionally blank

Annex 3E – Deception matrix to support the operations planning process

3E.1. An example of how to present the development of the deception plan, to support course of action development, analysis, validation and comparison is below in Figure 3E.1.

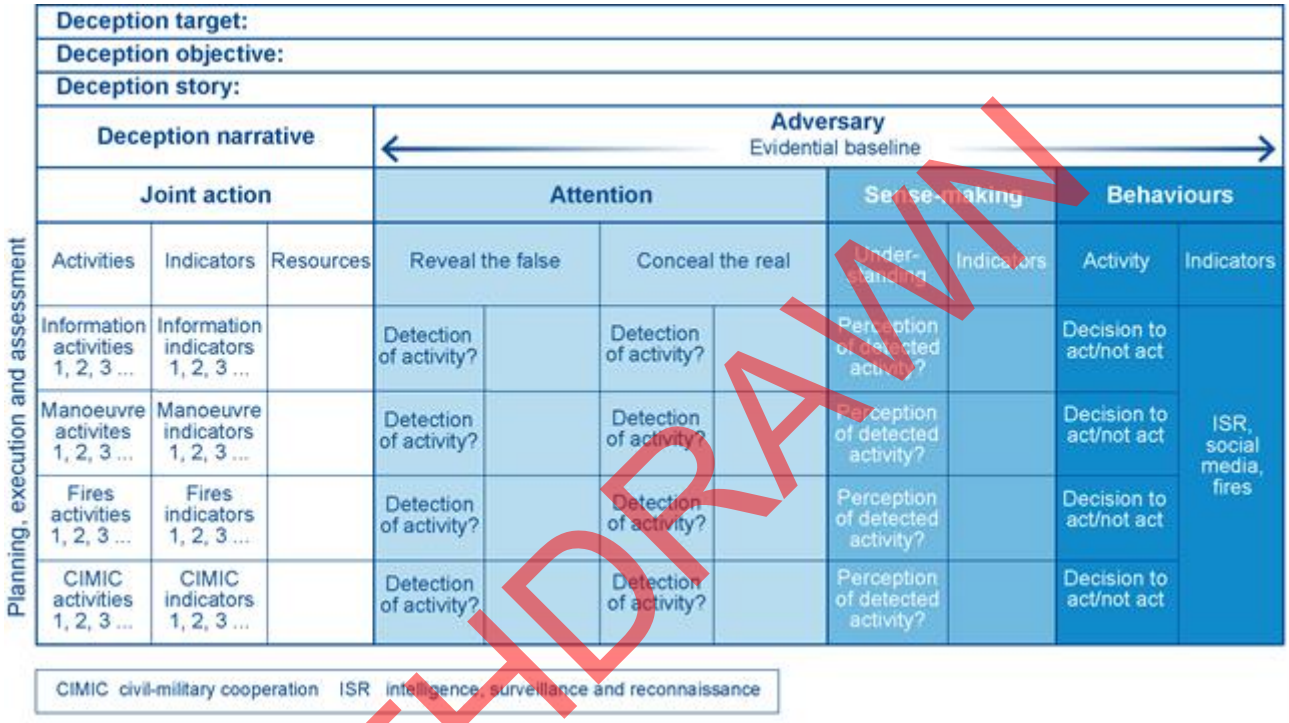


Figure 3E.1 – Deception matrix to support the operations planning process

Intentionally blank

Lexicon

Part 1 – Acronyms and abbreviations

AJP	Allied joint publication
CCIR	commander's critical information requirement
CIMIC	civil-military cooperation
CMI	civil-military interaction
COA	course of action
CONOPS	concept of operations
COP	common operational picture
COPD	comprehensive operations planning directive
CPOE	comprehensive preparation of the operational environment
EEFI	essential elements of friendly information
FRAGO	fragmentary order
IACB	Information Activities Coordination Board
Info Ops	information operations
ISR	intelligence, surveillance and reconnaissance
JIPOE	joint intelligence preparation of the operating environment
JTCB	Joint Targeting Coordination Board
JFC	joint force commander
LEGAD	legal advisor
LOAC	Law of Armed Conflict
MOE	measure of effectiveness
MOP	measure of performance
NATO	North Atlantic Treaty Organization

OPLAN	operation plan
OPP	operations planning process
OpsA	operations assessment
OPSEC	operations security
PA	public affairs
POLAD	political advisor
PSYOPS	psychological operations
SACEUR	Supreme Allied Command Transformation Europe

Part 2 – Terms and definitions

actor
A participant in an action or process. (COED)

adversary
An opponent. (COED)

A party acknowledged as potentially hostile and against which the legal use of force may be envisaged. (NATO Agreed)

asymmetric threat
A threat emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting his weaknesses to obtain a disproportionate result. (NATO Agreed)

camouflage
The use of natural or artificial material on personnel, objects or tactical positions with the aim of confusing, misleading or evading the enemy. (NATO Agreed)

civil-military interaction
A group of activities, founded on communication, planning and coordination, that NATO military bodies share and conduct with international and local non-military actors, both during NATO operations and in preparation for them, thereby mutually increasing the effectiveness and efficiency of their respective actions in response to crises.
(NATO Agreed)

concealment
Not allow to be seen; hide. (COED)

countersurveillance
All measures, active or passive, taken to counteract hostile surveillance. (NATO Agreed)

course of action
In the estimate process, an option that will accomplish or contribute to the accomplishment of a mission or task, and from which a detailed plan is developed. (NATO Agreed)

cyberattack
An act or action initiated in cyberspace to cause harm to communication, information or other systems, or the information that is stored, processed or transmitted on these systems. (AJP-3.20, Allied Joint Doctrine for Cyberspace Operations V1 SD3. Not NATO Agreed)

deception
Deliberate measures to mislead targeted decision-makers into behaving in a manner advantageous to the commander's objectives.
(This term and definition modifies an existing NATO Agreed term and/or definition and will be processed for NATO Agreed status)

defensive cyber operations
Defensive actions in or through cyberspace to preserve friendly freedom of action in cyberspace.
(AJP-3.20, Allied Joint Doctrine for Cyberspace Operations V1 SD3. Not NATO Agreed)

distraction
A thing that diverts someone's attention. (COED)

diversion
Something intended to distract someone's attention. (COED)

electronic attack
Use of electromagnetic energy for offensive purposes. (NATO Agreed)

electronic protective measures
That division of electronic warfare involving actions taken to ensure effective friendly use of the electromagnetic spectrum despite the enemy's use of electromagnetic energy. There are two subdivisions of electronic protective measures: active electronic protective measures and passive electronic protective measures. (NATO Agreed)

electronic warfare
Military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects. (NATO Agreed)

essential element of friendly information
Critical information about intentions, requirements, capabilities and vulnerabilities that, if compromised, could threaten the success of operations.
(AJP-3.10.2, Allied Joint Doctrine for Operations Security and Deception. This term is a new term and definition and will be processed for NATO Agreed status)

human intelligence
Intelligence derived from information collected by human operators and primarily provided by human sources. (NATO Agreed)

illusion
A wrong or misinterpreted perception of a sensory experience. A deceptive appearance or impression. (COED)

indicators
In operations security indicators are detectable actions and publicly available information that can be interpreted to derive intelligence on friendly forces.
(This term and definition only applies to this publication)

information activities
Actions designed to affect information or information systems.
Note: Information activities can be performed by any actor and include protection measures.
(NATO Agreed)

information environment
A part of the operating environment comprised of the information itself; the individuals, organizations and systems that receive, process and convey the information; and the cognitive, virtual and physical space in which this occurs.
(AJP-3.10, Allied Joint Doctrine for Information Operations. Not NATO Agreed.)

information operations
A staff function to analyse, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and North Atlantic Council approved audiences in support of Alliance mission objectives.
(AJP-3.10, Allied Joint Doctrine for Information Operations. Not NATO Agreed.)

information requirement
In intelligence usage, information regarding an adversary or potentially hostile actors and other relevant aspects of the operating environment that needs to be collected and processed to meet the intelligence requirements of a commander. (NATO Agreed)

named area of interest
A geographical area where information is gathered to satisfy specific intelligence requirements. (NATO Agreed)

NATO military public affairs
The function responsible for promoting NATO's military aims and objectives to audiences to enhance awareness and understanding of military aspects of the Alliance.
Note: This includes planning and conducting external and internal communications, and community relations. (NATO Agreed)

operations security
The process that gives a military operation or exercise appropriate security, using passive or active means, to deny an adversary knowledge of the essential elements of friendly information, or indicators of them.
(This term and definition modifies an existing NATO Agreed term and/or definition and will be processed for NATO Agreed status)

open-source intelligence
Intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access. (NATO Agreed)

perception
The ability to see, hear, or become aware of something through the senses. (COED)

AJP-3.10.2(A)(2)

Designed by the Development, Concepts and Doctrine Centre

Published by the Ministry of Defence
This publication is available **at www.gov.uk/mod/dcdc**