Ministry of Defence

NATO OTAN

Allied Joint Publication-10.1

Allied Joint Doctrine for Information Operations

Edition A Version 1

NATO STANDARD

AJP-10.1

ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS

Edition A Version 1

with UK national elements

JANUARY 2023

NORTH ATLANTIC TREATY ORGANIZATION
ALLIED JOINT PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

Intentionally blank

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

26 January 2023

1. The enclosed Allied Joint Publication AJP-10.1, Edition A, Version 1, ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS, 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 2518.

2. AJP-10.1, Edition A, Version 1, is effective upon receipt and supersedes AJP-3.10, 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.

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

Dimitrios SIGOULAKIS
Lieutenant General, GRC (A)
Director, NATO Standardization Office

Intentionally blank

Allied Joint Publication-10.1

Allied Joint Doctrine for Information Operations

Allied Joint Publication-10.1 (AJP-10.1), Edition A, Version 1,
dated January 2023,
is promulgated in the UK in July 2023 with UK national
elements as directed by the Chiefs of Staff

Director Development, Concepts and Doctrine Centre

Authorisation

The Development, Concepts and Doctrine Centre (DCDC) is responsible for publishing strategic trends, joint concepts and doctrine. If you wish to quote our publications as reference material in other work, you should confirm with our editors whether the particular publication and amendment state remains authoritative. We welcome your comments on factual accuracy or amendment proposals. Please contact us via email at: DCDC-DocEds@mod.gov.uk

Copyright

Distribution

All DCDC publications can be demanded from the LCSLS Headquarters and Operations Centre.
LCSLS Help Desk: 01869 256197 Military Network: 94240 2197

Our publications are available to view and download on defnet (RLI) at: https://modgovuk.sharepoint.com/sites/IntranetUKStratCom/SitePages/development-concepts-and-doctrine-centre-dcdc.aspx

This publication is also available on the Internet at: www.gov.uk/mod/dcdc

Adopting NATO doctrine

The UK places NATO at the heart of its defence. In doing so the UK should strive to achieve maximum coherence and interoperability with, and between, our closest allies and partners. Where possible the UK will adopt NATO doctrine (Allied joint publications) rather than producing national doctrine (joint doctrine publications). Where it cannot, the UK will ensure it remains compatible. As a result the UK doctrine architecture comprises:

- NATO Allied joint publications distributed in the UK for use on coalition operations as appropriate;
- NATO Allied joint publications promulgated as UK national joint doctrine; and
- UK joint doctrine publications promulgated as UK national joint doctrine.

Where an Allied joint publication is promulgated as UK national doctrine, the cover will carry both the MOD and NATO emblems. These publications may contain UK national element additions, which explain a particular UK approach, clarify a UK definition, or aid understanding. These additions will be clearly identified as boxes with the UK flag icon. All photos and captions are also UK national additions. The original NATO text will not be modified. The UK additions take precedence where terms and processes differ.

Intentionally blank

Record of 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	The United States does not support glossary/lexicon terms and definitions and shortened word forms (abbreviations, acronyms, initialisms) that are neither NATO Agreed, quoted verbatim from NATOTerm, correctly cited IAW AAP-47 Allied Joint Doctrine Development, correctly introduced/ revised IAW AAP-77 NATO Terminology Manual, nor have terminology tracking forms submitted. Department of Defense (DoD) terminology views regarding terms and definitions applicable to the United States can be found in the DoD Dictionary of Military and Associated Terms. The United States uses the term "law of war" to describe that part of international law that regulates the resort to armed force; the conduct of hostilities and the protection of war victims in international and non-international armed conflict; belligerent occupation; and the relationships between belligerent, neutral, and non-belligerent States. Sometimes also called the law of armed conflict or international humanitarian law, the law of war is specifically intended to address the circumstances of armed conflict. The legal views of the Department of Defense (DoD) regarding the law of war applicable to the United States can be found in the DoD Law of War Manual. The United States supports doctrinal content that is harmonized with NATO's capstone and operations keystone doctrine publications as well as within and between other NATO Allied Joint Doctrine publications. United States personnel are directed to use national joint doctrine to overcome variances between U.S. joint doctrine and Allied Joint Doctrine publications [ex. command relationships, joint operations principles, physical domain and other domain categorization, subject matter expertise language usage and other related terminology]. Department of Defense (DoD) joint doctrinal content can be found in joint doctrine publications

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

Summary of changes

Record of summary of changes for Allied Joint Publication (AJP)-10.1(A)
• Describes and expands on the key the changes introduced in AJP-01(F) that affect information operations (Info Ops) such as: o The continuum of competition. o The key tenets of doctrine that introduces the additional tenet of the behaviour centric-approach and the updated comprehensive approach. o The updated description of environments, the operating environment and the effects dimensions. o Audiences and their sub-categories of public, stakeholder and actor. o The comprehensive understanding of the operating environment (CUOE) which fuses together understanding from the joint intelligence preparation of the operating environment and the information environment assessment (IEA). o NATO's approach to strategic communications (StratCom).
• Describes and expands on the new keystone publication AJP-10 StratCom which introduces the J10 StratCom directorate at the operational level and how the vertical integration of StratCom, in conjunction with the horizontal integration of Info Ops across a headquarters, is achieved through the StratCom direction and guidance documents of the StratCom frameworks, the StratCom implementation guidance and the integrated communications plan or StratCom annex (Annex SS) to the operation order.
• Describes and expands Info Ops as the 4 components of the staff function: analyse, plan, integrate and assess. o **Analyse.** This explains the understanding processes within the IEA and its contribution to the CUOE. o **Plan.** Using the inputs from the IEA the planning section has been updated to highlight the contribution of Info Ops to the operations planning process. o **Integrate.** Using the new information activities working group as the primary battle rhythm forum to plan and integrate information activities and describe how Info Ops staff participate and contributes to battle rhythm forums across the headquarters. o **Assess.** Using the IEA to predict the cognitive impact of activity and to track the behavioural conditions of audience groupings to feed the operations assessment process.

Intentionally blank

Related documents

Policy and Military Committee documents

PO(2009)0141	*NATO Strategic Communications Policy*
MC 0628	*NATO Military Policy on Strategic Communications*
MC 0422/6	*NATO Military Policy on Information Operations*
MC 0402/3	*NATO Military Policy on Psychological Operations*
MC 0411/2	*NATO Military Policy on Civil-Military Cooperation*
MC 0457/3	*NATO Military Policy on Public Affairs*
MC 0665	*NATO Military Vision and Strategy on Cyberspace as a Domain of Operations*
MC 0471/1	*NATO Targeting Policy*

Allied joint publications

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-2.1	*Allied Joint Doctrine for Intelligence Procedures*
AJP-2.2	*Allied Joint Doctrine for Counter-intelligence and Security Procedures*
AJP-2.3	*Allied Joint Doctrine for Human Intelligence*
AJP-2.4	*Allied Joint Doctrine for Signals Intelligence*
AJP-2.7	*Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*
AJP-2.9	*Allied Joint Doctrine for Open Source Intelligence*
AJP-3.1	*Allied Joint Doctrine for Maritime Operations*
AJP-3.2	*Allied Joint Doctrine for Land Operations*
AJP-3.3	*Allied Joint Doctrine for Air and Space Operations*
AJP-3.5	*Allied Joint Doctrine for Special Operations*
AJP-3.6	*Allied Joint Doctrine for Electronic Warfare*
AJP-3.9	*Allied Joint Doctrine for Joint Targeting*
AJP-3.10.1	*Allied Joint Doctrine for Psychological Operations*
AJP-3.10.2	*Allied Joint Doctrine for Operations Security and Deception*
AJP-3.14	*Allied Joint Doctrine for Force Protection*
AJP-3.19	*Allied Joint Doctrine for Civil-Military Cooperation*
AJP-3.20	*Allied Joint Doctrine for Cyberspace Operations*
AJP-10	*Allied Joint Doctrine for Strategic Communications*

Allied administrative publications

AAP-47 *Allied Joint Doctrine Development*
AAP-77 *NATO Terminology Manual*

Additional NATO publications

Allied Command Operations (ACO) *Comprehensive Operations Planning Directive*
ACO Directive 080-070, *Joint Targeting in the ACO*
ACO Directive 095-002, *ACO Strategic Communications*
ASCP-01, *NATO Strategic Communications Training Standards*
NATO Strategic Communication Handbook
NATO Bi-SC Information Operations Reference Book
NATO Bi-SC Psychological Operations Handbook
NATO Engagement Handbook
NATO Operations Assessment Handbook
NATO Bi-SC Directive 040-001, *Integrating UNSCR 1325 and Gender Perspective into the NATO Command Structure*
NATO Code of Conduct,
NATO Policy on Preventing and Responding to Sexual Exploitation and Abuse
NATOTerm

Other relevant Allied publications

Multinational Capability Development Campaign (MCDC), *Military Strategic Communication Handbook*

UK related documents

Joint Doctrine Publication (JDP) 0-01, *UK Defence Doctrine*, 6th Edition
JDP 0-50, *UK Defence Cyber and Electromagnetic Doctrine*
JDP 2-00, *Intelligence, Counter-intelligence and Security Support to Joint Operations*
JDP 0-01.1, *UK Terminology Supplement to NATOTerm*
Defence Operating Model
Cyber Primer, 3rd Edition
Joint Tactics, Techniques and Procedures 3.81, *Integrated Action: An operational level guide to the audience-centric approach for commanders and staff*

Contents

Intentionally blank

Preface

Context

1. NATO operates in a highly competitive, fragmented and dispersed environment that requires a behaviour-centric approach to meet the challenges of enduring strategic competition. Information operations (Info Ops) is applicable in peace, crisis and conflict throughout the continuum of competition. It provides a comprehensive understanding of the information environment and, in particular audiences, the ability to plan specific activities for cognitive effect and provides support to planning of all activities in the engagement space, which are then assessed to enable refinement of plans to meet objectives.

Scope

2. Allied Joint Publication (AJP)-10.1, *Allied Joint Doctrine for Information Operations* outlines the principles, relationships and processes for Info Ops. It explains how the Info Ops staff ensures consistency, coordination and synchronization of information activities, with a focus on the operational level to support commanders' objectives.

Purpose

3. AJP-10.1 provides guidance to NATO commanders and their staffs to use Info Ops as the staff function for the horizontal integration of strategic communications direction and guidance through planning and coordinating information activities throughout the full spectrum of activities and operations. It clarifies the role of Info Ops staff within the communication directorate (or similar staff element), emphasizing their horizontal consistency responsibilities and their key contribution to joint operations.

Application

4. AJP-10.1 primarily details Info Ops processes at the operational level, but the principles and thought processes can be applied at all levels. It can also be a useful framework for operations conducted by a coalition of NATO partners, non-NATO nations and other organizations.

Linkages

5. The principal enabling document for Info Ops is Military Committee (MC) 0422, *NATO Military Policy for Information Operations*, which is coherent with MC 0628, *NATO Military Policy for Strategic Communications*. AJP-10.1 builds on the landscape provided by AJP-01, *Allied Joint Doctrine* and the principles and processes outlined in AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, AJP-5, *Allied Joint Doctrine for the Planning of Operations* and AJP-10, *Allied Joint Doctrine for Strategic Communications*.

Intentionally blank

Chapter 1

Chapter 1 lays out the strategic context in which contemporary operations are framed. It outlines the continuum of competition, where sub-threshold activity is particularly prevalent in the information environment and explains how NATO addresses emerging threats. The key doctrinal tenets are described, as well as the instruments of power and the joint functions, highlighting the significance of information, audiences and behaviours in achieving objectives.

1

> “Attitudes are more important than facts.”
>
> Karl A. Menninger

Chapter 1

Context

1.1 Chapter 1 sets the context for information operations (Info Ops), drawing on the doctrinal landscape from NATO's capstone doctrine, Allied Joint Publication (AJP)-01, *Allied Joint Doctrine*, which outlines the broad philosophy and principles underpinning what NATO stands for and how it is to be employed. This publication has been influenced by the *NATO Military Strategy*, the first revision since 1969, the *Concept for the Deterrence and Defence of the Euro-Atlantic Area* (DDA) and the new *NATO Warfighting Capstone Concept* (NWCC) for how the Alliance will operate and fight over the next 20 years. This chapter examines the threats faced by the Alliance today, outlines the continuum of competition, where sub-threshold activity is particularly prevalent in the information environment, and explains how NATO addresses these threats through its strategy and campaign themes. The key doctrinal tenets to support NATO's approach to operations are described, as well as the instruments of power and the joint functions, highlighting the role of information within them. An explanation of environments, engagement space, operational domains and effect dimensions will be highlighted before concluding with an introduction to strategic communications (StratCom).

Section 1 – Strategic threats and the continuum of competition
Section 2 – NATO's strategy, campaign themes and types of operations
Section 3 – Key tenets of doctrine
Section 4 – Instruments of power and joint functions
Section 5 – Operating environment
Section 6 – Strategic communications

Section 1 – Strategic threats and the continuum of competition

1.2 **Threat.** NATO is an international alliance that was established to guarantee the freedom and security of its members through political and military means and, as such, it is confronted with a continuously changing strategic situation that challenges its aims, objectives and desired end states. The Alliance is challenged by adversaries who seek to undermine its cohesion and credibility by using a wide spectrum of confrontational actions, especially

during crisis operations. Adversaries assume different identities and may not be constrained by accepted sociocultural patterns (such as the legal, ethical and moral norms), pervasive public opinion and media scrutiny, which all apply to NATO's members. As an alliance of nations dedicated to the rules-based international order (RBIO), it needs to protect its credibility and its centre of gravity – Alliance cohesion.

1.3 **Information Age.** An increasingly digitized and interconnected world that provides easy access to technology offers the ability to deliver real time audience-tailored communication to report, command, inform, influence, persuade, confuse, coerce or deceive. As an increasing number of people spend more time conducting an ever widening range of activities in cyberspace, information and narratives have an increasing influence on conflict and instability. All NATO's actions, images and words are observed, interpreted, packaged and redistributed and then acted upon by audiences according to their perspectives and desired objectives. The ability to exploit information through ever improving and accessible information technology provides universal opportunities.

1.4 **Continuum of competition.** Conflict used to be depicted in a spectrum with a sliding scale from peace to war, but it is now better articulated as a continuum of competition, as illustrated in Figure 1.1 and fully explained in AJP-01. The RBIO has evolved since its conception, after the Second World War, as a shared commitment by all countries to conduct their activities in accordance with international law and agreed rules such as regional security arrangements, trade agreements, immigration protocols and cultural arrangements. The RBIO can be viewed as a line of acceptable behaviour against which the Alliance judges other actors' activities. Above that line exists confrontation, where differences might no longer be reconciled, possibly leading to a state of crisis crossing the threshold into armed conflict. This is where escalation cannot be prevented or contained, leading to one party resorting to military force to compel their enemy to resolve the contradiction in their favour. Below this threshold varying states of competition exist where states and organizations cooperate to achieve the same objectives or clash in rivalry where actors have conflicting aims or contradictions. The majority of sub-threshold activity is covertly orchestrated by state and non-state, including proxy, adversaries seeking to undermine NATO's and its partners' security, the integrity of its democracies, its public safety, reputation or economic prosperity. Sub threshold activity is particularly prevalent in the information environment where information activities with hostile intent are widely used along with malicious cyberspace activity and targeted campaigns to sow distrust and potentially exacerbate turmoil amongst different audiences.

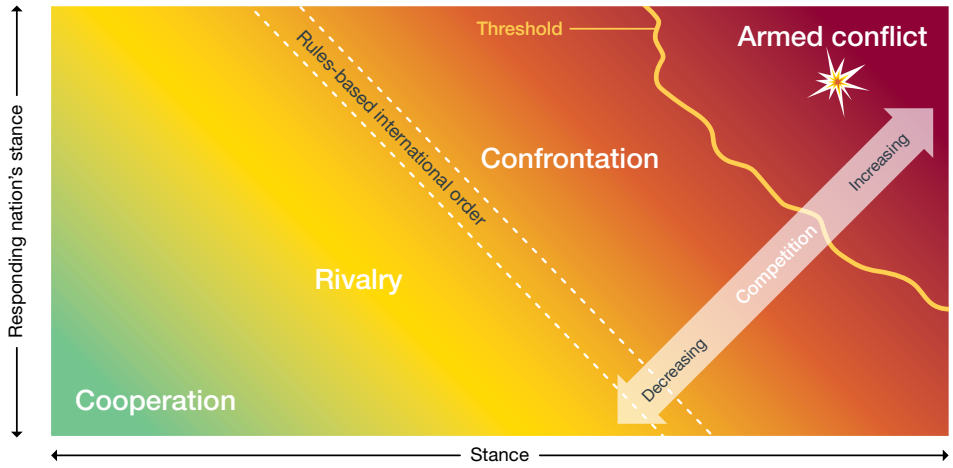


Figure 1.1 – The continuum of competition

Section 2 – NATO's strategy, campaign themes and types of operations

1.5 NATO's strategic concept[1] is based on three core tasks: deterrence and defence; crisis prevention and management; and cooperative security. The core tasks are applied through the core policies of deterrence and defence, projecting stability and the fight against terrorism.

1.6 NATO operates at the strategic, operational and tactical levels, which provides a framework to plan and integrate military activities across the operating environment. Operations are conducted within the four campaign themes of peacetime military engagement, peace support, security and warfighting which are shown in Figure 1.2, along with their relationship to the components of the continuum of competition. Information activities are prevalent in all the campaign themes as part of the behaviour-centric approach to inform and influence behaviour to achieve NATO's objectives. Further information on campaign themes is contained within AJP-01, *Allied Joint Doctrine*.

1 NATO 2022 *Strategic concept*

UK 1.1. The UK uses the term 'audience-centric approach' rather than 'behaviour-centric approach', but the meaning is broadly the same. An audience-centric approach recognises that people are at the heart of competition; it is their decisions and behaviours that determine how competition is conducted and resolved. An audience-centric approach is defined as: the understanding, planning, execution and monitoring of activity to influence audiences' attitudes, beliefs or behaviours to achieve desired outcomes.[1]

1 Joint Doctrine Publication (JDP) 0-01.1, *UK Terminology Supplement to NATOTerm*.

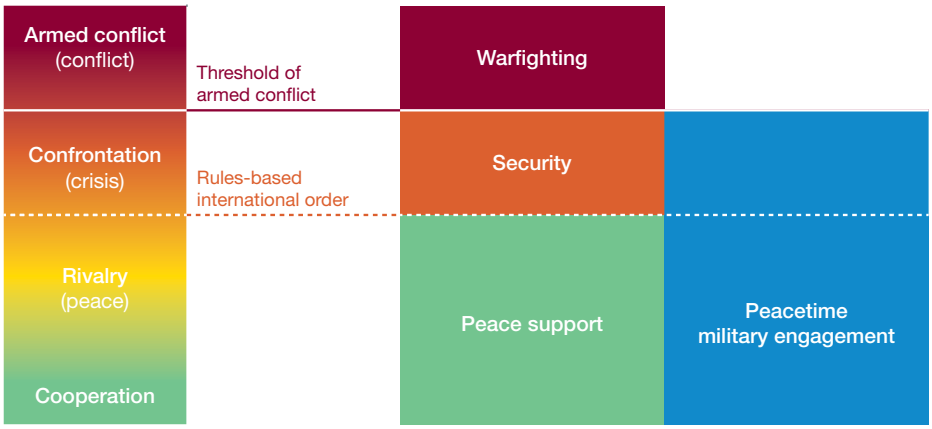


Figure 1.2 – Relationship between campaign themes and the continuum of competition

Campaign themes

1.7 **Peacetime military engagement.** Military engagement exists below the threshold of armed conflict and implies a supporting role to other instruments of power. This is, predominately for diplomatic reasons, to build trust and comprehensive relationships.

1.8 **Peace support.** This theme operates in the rivalry zone of the continuum of competition, supporting the RBIO and it is underpinned by the principles of projecting stability. The theme seeks to preserve peace or intervene early within a potential conflict to maintain stability, prosperity and the rule of law.

1.9 **Security.** The theme of security applies in the confrontation zone of the continuum of competition with the five principles of deterrence (credibility,

cognition, capability, competition and communication) being implicit in the theme's nature. The theme implies the Alliance detects, deters and, if required, responds to a strategic competitor's operating techniques, especially threshold shifting. The Alliance response might entail contesting the competitor's sub-threshold activity or conducting peace enforcement pre- or post-warfighting operations.

1.10 **Warfighting.** Warfighting occurs above the threshold of armed conflict (either international armed conflict or non-international armed conflict) and comprises combat operations conducted in accordance with the law of armed conflict and rules of engagement. Warfighting will usually be a series of high-intensity engagements through multiple operational domains with effects created in all dimensions. These actions would be a response to a significant form of armed aggression between one or more states, or a well-organized and resourced non-state actor. It is likely the enemy will combine unconventional and sub-threshold methods with their combat operations as part of an overall strategy. Warfighting is inherently linked to the imposition of will by an aggressor on an enemy or adversary by using physical force, noting that warfighting is also forced upon those that are being attacked.

Types of operations

1.11 Within the four campaign themes, numerous types of operations, described in AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, can be conducted and may relate to several of the themes. Info Ops plays an important role in all types of NATO operations and contributes to the continuous understanding, analysis and assessment of audiences and narratives, as well as planning and integrating specific activities for related effects.

1.12 **Combat operations.** Combat operations and the capability to conduct them are at the heart of NATO's purpose to provide direct defence of NATO, and its member states, against an aggressor. These operations are normally high tempo and involve large-scale manoeuvre, with a need to prioritize resources. Info Ops provides in-depth understanding, analysis and assessment of narratives, the information environment and the audiences involved, as well as the predicted and actual behavioural assessment of activities, thereby supporting consequence management and amplification of the narrative. It is likely that Info Ops will have been planning and integrating information activities prior to combat operations and will continue during combat, and after combat operations have ceased.

1.13 **Crisis response operations.** Crisis response operations include multifunctional operations, which contribute to conflict prevention and resolution, humanitarian purposes or crisis management in line with declared Alliance objectives. These operations may be as demanding and intense as combat operations and in many cases the military are unlikely to be the lead or primary organization, but they can make a significant contribution. Crisis response operations seek to counter irregular activities, which can be done directly or indirectly and consists of counter-insurgency (COIN), counterterrorism and counter-criminality. Further information on COIN operations can be found in AJP-3.27, *Allied Joint Doctrine for Counter-insurgency.* There are several other crisis response operations, such as the following.

a. **Military contribution to peace support.** Peace support operations are efforts conducted impartially to restore or maintain peace. Peace support efforts can include conflict prevention, peace-making, peace enforcement, peacekeeping and peacebuilding. The military contribution to peace support reflects a population-centric approach where NATO forces operate with no designated opponent. Impartiality is the fundamental difference that separates peace support from other types of operational-level themes. Peace support requires the combined efforts of military and civilian actors operating in a coordinated and, where possible, collaborative way to achieve commonly agreed strategic objectives. Info Ops will provide the audience understanding, analysis and assessment to enable the planning and integration of information activities, in line with the narrative, that can be used in conjunction with other military activities to support the peace process. For further information see AJP-3.4.1, *Allied Joint Doctrine for the Military Contribution to Peace Support*.

b. **Military contribution to humanitarian assistance.** Humanitarian operations are conducted to alleviate human suffering in an area where civil actors are normally responsible for doing so but they are unable or unwilling to adequately support a population. These operations aim to save lives, relieve suffering and maintain human dignity. In addition to comprehensive audience understanding and analysis of the information environment, communication is a critical aspect of humanitarian operations where the Info Ops staff will coordinate and integrate information activities to amplify the narrative, counter information activities with hostile intent, and inform and influence audiences in the engagement space. Further information can be found in AJP-3.4.3, *Allied Joint Doctrine for the Military Contribution to Humanitarian Assistance*.

c. **Military contribution to stabilization.** Stabilization is an approach used to mitigate crisis, promote legitimate political authority and set the conditions for long-term stability by using comprehensive civilian and military actions to reduce violence, re-establish security and end social, economic and political turmoil. A key aspect of stabilization is security sector reform (SSR), which requires a comprehensive approach with other government and international agencies dealing with judiciary and law enforcement agencies. SSR will seek to address two broad areas: the effectiveness of the security and justice services and their accountability. Pivotal to NATO's contribution to SSR (which is called security sector assistance) are: security force assistance; disarmament, demobilization and reintegration; and stability policing. Info Ops will provide the audience understanding, analysis and assessment to enable the planning and integration of information activities, in line with the narrative, that can be used in conjunction with other military activities to support stabilization. Further information can be found in AJP-3.4.5, *Allied Joint Doctrine for the Military Contribution to Stabilization*, AJP-3.16, *Allied Joint Doctrine for Security Force Assistance* and AJP-3.22, *Allied Joint Doctrine for Stability Policing*.

d. **Military contribution to non-combatant evacuation operations.** A non combatant evacuation operation (NEO) is an operation conducted to relocate designated non-combatants threatened in a foreign country to a place of safety. This relocation may be temporary or permanent and a place of safety may be located within the same country. NEOs have political, humanitarian and military implications and usually involve swift insertion of a force, temporarily occupying and holding key locations, such as an evacuation control centre, assembly points and embarkation sites, and withdrawing upon completion of the evacuation. In addition to comprehensive audience understanding and analysis of the information environment, communication is a critical aspect of NEO where the Info Ops staff will coordinate and integrate information activities to amplify the narrative, counter information activities with hostile intent, and inform and influence audiences in the engagement space. If military support is provided, Info Ops ensures the proper coordination and integration of StratCom direction and guidance. For further information see AJP-3.4.2, *Allied Joint Doctrine for the Military Contribution to Non-Combatant Evacuation Operations*.

Information operations ensure the proper coordination and integration of strategic communiations direction when conducting operations to police airspace and communicate deterrence

e. **Military contribution to sanctions.** The enforcement of sanctions is designed to encourage a nation to abide by international law or to conform to a resolution or mandate. Sanctions are generally a combination of denial of supplies, diplomatic and economic restrictions, and restricted freedom of movement. Military support could be: providing capabilities to enforce the imposed sanctions, such as embargoes of trade, personnel and services in to or out of a state; or policing and enforcing exclusion or no-fly zones designed to protect activities.

f. **Military contribution to freedom of navigation and overflight.** These operations are conducted to demonstrate international rights to navigate sea or air routes. The military contribution is a combination of monitoring assets and providing capabilities to regulate and police international airspace and sea routes. Communication of deterrence and incursion activity in line with the narrative is a key component of this type of operation. If military support is provided, Info Ops ensures the proper coordination and integration of StratCom direction and guidance.

g. **Extraction.** Extraction operations are where a NATO-led force conducts or assists in the withdrawal of military missions and units from a crisis region. This operation is most likely to be conducted in an uncertain or hostile engagement space and is often a contingency plan to deploy a dedicated force should the situation change, for example, loss of consent or inadequate control by the host nation. Info Ops ensures the proper coordination and integration of StratCom direction and guidance.

Section 3 – Key tenets of doctrine

1.14 **Key tenets of doctrine.** The doctrinal tenets represent the enduring aspects of doctrine. They apply across all campaign themes, the continuum of competition and all levels of operations.

a. **The behaviour-centric approach.** The behaviour-centric approach is the primary doctrinal tenet that focuses planning and execution of activity to appropriately inform and influence the attitudes and behaviour of audiences to attain the end state. This approach is about a comprehensive and persistent understanding of audiences and how they can affect our outcomes; it uses narrative-led execution to converge effects across all levels of operations to maintain or change attitudes and behaviours.

i. **Audience analysis.** A comprehensive and persistent understanding of audiences identifies points of influence which may change or reinforce an audience's attitudes or behaviours. An audience is defined as: 'any individual, group or entity whose interpretation of events and subsequent behaviour may affect the attainment of the end state.' NATO segments audiences into three categories – public, stakeholder and actor – as illustrated in Figure 1.3. Audience segmentation provides the commander with more focused understanding and enables subsequent effects optimization to achieve or maintain the desired behavioural changes. All audiences may be considered friendly, supportive, neutral, unsupportive or hostile. Audience analysis is explained in detail in Chapter 4.

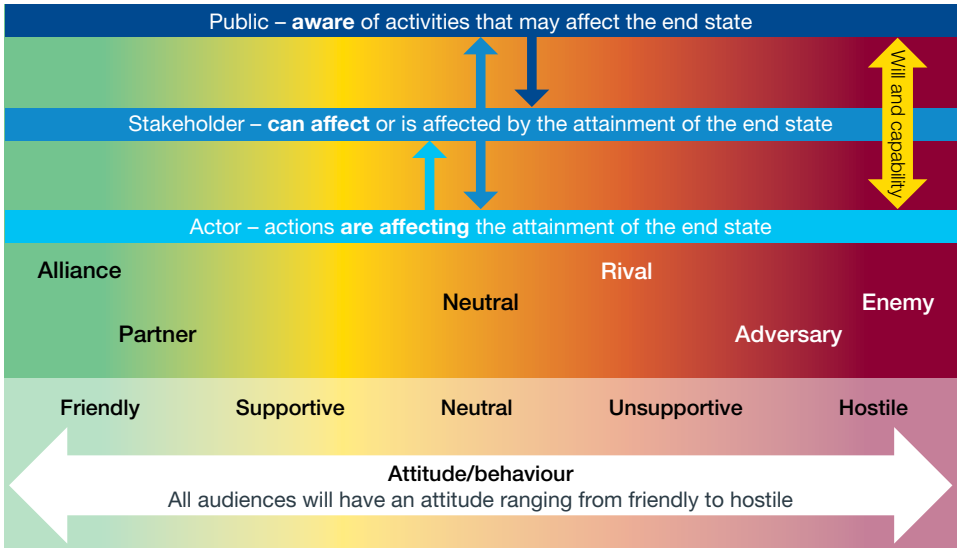


Figure 1.3 – Audiences in the operating environment

ii. **Narrative-led execution.** Narrative-led execution uses the narrative as an overarching expression of the whole-of-Alliance strategy to inform and influence audiences, and gives context to the campaign, operation or situation. The narrative gives audiences the meaning to a set of facts and actions, and to be successful NATO must demonstrate consistency in actions, images and words, ensuring they always reflect the strategic and micro narratives, and thus pre-empting any attempts to exploit gaps between what NATO does, shows and says. The narrative binds the Alliance vertically through the levels of operations, and horizontally across the instruments of power and with partners. The narrative is explained in more detail in Chapter 3.

b. **Manoeuvrist approach.** Commanders employ the manoeuvrist approach to achieve their behaviour-centric objectives in line with the narrative. The manoeuvrist approach represents an indirect approach that focuses on degrading the will to contest. It seeks to shape understanding, avoid an adversary's strengths and selectively target and exploit their critical vulnerabilities and other points of influence to disrupt cohesion and seize, maintain and exploit the initiative. This approach applies strength against identified vulnerabilities, including indirect ways and means of targeting the intellectual and moral component of an adversary's fighting power. Whilst the manoeuvrist

approach contains an element of attrition and annihilation (armed conflict is inherently violent with physical destruction), it is not its primary focus; it is focusing where the emphasis lies and on how the commander thinks about the execution and operational assessment of the mission they have been given.

c. **Comprehensive approach.** The comprehensive approach guides the commander in how to operationalize the whole-of-Alliance and partners coalition. It enables staff to orchestrate and integrate the most appropriate mix of political, military and non-military actions to inform and influence audiences and achieve a unified outcome. It supports the manoeuvrist approach by increasing capability and capacity, thereby allowing a commander to exploit a wider array of the adversary's vulnerabilities, while minimizing their own exposure to risk.

The integrated approach

UK 1.2. The UK equivalent of the comprehensive approach is the integrated approach, which describes Defence's intent to be more integrated across the operational domains and levels of operations, nationally across government and internationally with our allies and partners.

d. **Mission command.** Mission command is a command philosophy that guides the commander in how to delegate their command and empower their subordinates to achieve their objectives. Given the nature of competition and the manoeuvrist approach, it is paramount for the force to display initiative at all levels. It should seek to be the quickest to adapt and act with determination to create, rather than merely react to, the situation in line with the narrative.

Section 4 – Instruments of power and joint functions

1.15 **Instruments of power.** Nations seek to achieve their national and sectoral aims through the coordinated use of the four instruments of power: diplomatic, information, military and economic. These instruments are used to interact with other nations, but they also play a key role in supporting a nation's internal stability, cohesion and resilience. A nation does not necessarily need to excel in every instrument but draws strength from managing them concurrently to maximize their strategic advantage. The information instrument recognizes the prevalence of the Information Age, the increased importance of the information environment, the behaviour-centric approach and the role of information in influencing decision-makers. At the heart of the information instrument is the narrative, which guides operations and activities and must always be competed for.

1.16 **Joint functions.** The joint functions of manoeuvre, fires, command and control, intelligence, information, sustainment, force protection and civil-military cooperation (CIMIC) provide a framework of related capabilities and activities grouped together to help commanders integrate, synchronize and direct various capabilities and activities in joint operations. The joint functions framework operationalizes the manoeuvrist approach through a combination of manoeuvre, fires, information and CIMIC to affect the audience's attitude and behaviour. Amongst others, each of these joint functions perform deliberate activities to affect will, understanding and capability of decision-making directly by impacting a relevant audience's senses, state of mind and calculus. Further information of the joint functions can be found in AJP-3, *Allied Joint Doctrine for the Conduct of Operations*.

1.17 **Information as a joint function.** Information is critical for decision-making and how audiences are informed and influenced is dependent on the information available to them. The information function helps commanders and staff applying or using information to understand the impact of emerging and disruptive technologies, along with other functions, to inform and influence relevant audience perceptions, behaviour and decision-making. Key enablers are psychological operations, military public affairs, electromagnetic warfare, cyber and engagement activities, which must be coordinated and integrated throughout the planning process, support all activities and be consistent with the narrative.

UK 1.3. Information is employed as an instrument of the UK's national power by applying the UK's institutional narrative using information activities. This includes employing Defence strategic communication (Defence StratCom) in support of national interests. Defence StratCom generates the narratives that guide the planning of the campaign. More information on Defence StratCom can be found at paragraph UK 1.4.

Section 5 – Operating environment

1.18 **Environment.** Environments are used to describe the system surrounding activity from a physical and non-physical perspective. There is only one environment, but it can be analyzed from different perspectives depending on subject matter expertise to create multiple types of sub-environments such as information, maritime, urban, political and human. The information environment is the principal environment of decision-making; where humans and automated systems observe, conceive, process, orient, decide and act on data, information and knowledge. It is characterized by ubiquitous on-demand media and interpersonal hyper-connectivity that enables collaboration and information sharing on an unprecedented scale. Whilst there is a definite growth in access to information around the world, literacy as well as Internet penetration and unfettered access to it, remain significant discriminators. The information environment is explained in detail in Chapter 4, along with the associated understanding and assessment process: the information environment assessment (IEA).

1.19 **Operating environment.** Once a mission or task has been assigned, the understanding of the environment becomes focused into an operating environment. This combines the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander.

1.20 **Engagement space.** The engagement space[2] is the part of the operating environment where actions and activities are planned and conducted. When capabilities from operational domains are assigned to an operation, they are applied in an engagement space.

2 The engagement space and battlespace are synonyms.

The cognitive dimension is the decisive dimension – it is where effects on an individual's thinking are created, driving behaviour change

1.21 **Effect dimensions.** An effect is a change to the engagement space because of an action. Derived from objectives, effects bridge the gap between objectives and actions by describing what changes in the engagement space are required. To visualize these changes, the effect dimensions is used. Effect dimensions is an analytical construct that highlight the interdependencies of the engagement space, thereby gaining a better understanding of the consequences of actions. The elements that constitute dimensions are described below and are further explained in Chapter 4.

a. The **cognitive dimension** relates to the consequence on the audiences' perceptions, beliefs, interests, aims, decisions and behaviours. This dimension is shaped by culture and societal influences and it encompasses all forms of interaction (such as informational, economic and political) between them. The cognitive dimension is the decisive dimension to achieve an enduring outcome.

b. The **physical dimension** relates to the consequence on the audiences, the sub-surface, surface, airspace and space areas where all physical activities take place, and where audiences live, including all physical objects and infrastructure that support them. This dimension is

divided into a geographical and a physical layer, within which there are entities that can be engaged.

c. The **virtual dimension** relates to the consequences of activity on the storage, content and transmission of analogue and digital data. It also includes all supporting communication and information systems and processes.

Section 6 – Strategic communications

1.22 **Strategic communications.** The importance of the information environment to the current character of competition has resulted in the Alliance creating a new keystone doctrine publication, AJP-10, *Allied Joint Doctrine for Strategic Communications*. StratCom seeks to appropriately inform and influence audiences' attitudes and behaviours in pursuit of the desired end state through a narrative-led approach at all levels of command, in planned activities and by exploiting actions to target the cognitive dimension of the engagement space. NATO's approach to StratCom consists of three main elements.

a. **Understanding.** The process of understanding audiences is derived from the IEA and combined in a headquarters along with the joint intelligence preparation of the operating environment (JIPOE) and the assessment of assigned missions and tasks to facilitate comprehensive understanding of the operating environment (CUOE). The CUOE enables the commander to understand the physical, virtual and cognitive elements of the system within the engagement space that can be used or targeted to create effects. The effect dimensions highlight the interdependencies of the engagement space, thereby gaining a better understanding of the consequences of actions and helping to determine the supporting/supported effects needed to achieve our objectives. These effects help planners to design multi-domain activities, enabled by focused understanding through target audience analysis, to provide the requisite understanding and support the planning and execution of an activity.

b. **Integrated planning.** A behaviour-centric approach to planning and subsequent execution, supported by comprehensive understanding, will ensure that the resultant cognitive effect of actions, images and words will be considered and mitigated in line with the behavioural outcomes

required to achieve objectives. Info Ops must be integrated throughout the headquarters to ensure that activities are planned in line with the narrative.

c. **Narrative-led execution.** The Alliance should aim to demonstrate consistency in actions, images and words, ensuring they always reflect the institutional, strategic and micro narratives, and thus pre-empting adversary attempts to exploit gaps between what NATO does, shows and says through the use of soft power to mobilize, incite and disempower the population. The narrative-led approach uses the narrative as an overarching expression of the strategy to appropriately inform and influence audiences, and gives context to the campaign, operation or situation. The narrative binds the Alliance vertically through the levels of operations, and horizontally across the instruments of power and with partners.

Defence strategic communication – the UK context

UK 1.4. For the UK, Defence StratCom is how we communicate about Defence activities. It should, however, be also understood as an approach to planning and executing strategy using all the assets at Defence's disposal innovatively to communicate the UK government's strategic message. The UK defines Defence StratCom as: advancing national interests by using Defence as a means of communication to influence the attitudes, beliefs and behaviours of audiences.[2]

2 JDP 0-01.1, *UK Terminology Supplement to NATOTerm*.

Key points

- Information activities are prevalent in all campaign themes as part of the behaviour-centric approach to inform and influence behaviour to achieve NATO's objectives.
- The UK uses the term 'audience-centric approach' rather than 'behaviour-centric approach'. Both approaches recognise that people are at the heart of competition; it is their decisions and behaviours that determine how competition is conducted and resolved.
- Audiences are segmented into three general categories – public, stakeholders and actors – depending on their ability to affect our desired outcomes.
- A comprehensive and persistent understanding of audiences identifies points of influence that may change or reinforce an audience's attitudes or behaviours.
- Defence StratCom generates the narratives that feed information activities.

Chapter 2

Chapter 2 considers information operations as a staff function, its relationships with strategic communications and the communication capabilities of psychological operations and military public affairs (or media operations). Other capabilities and techniques likely to be integrated as information activities are also described.

> “Avoid people who say they know the answer. Keep the company of people who are trying to understand the question.”

Sir William Connelly

Chapter 2

Fundamentals

2.1 Chapter 2 explores information operations (Info Ops) as a staff function, its relationships with strategic communications (StratCom), the communication capabilities of psychological operations (PsyOps) and military public affairs (Mil PA), as well as additional capabilities and techniques likely to be integrated as information activities. It also outlines the training and education competencies expected of those performing the Info Ops staff function.

Section 1 – Strategic communications policy and definition
Section 2 – Information operations policy, related definitions and principles
Section 3 – Focus of information operations
Section 4 – Communication capabilities
Section 5 – Additional capabilities and techniques likely to be integrated as information activities
Section 6 – Engagement, presence, posture and profile
Section 7 – Training and education

Section 1 – Strategic communications policy and definition

2.2 **Strategic communications.** StratCom is used by all levels of command to appropriately inform and influence audiences' attitudes and behaviours through a narrative-led approach in pursuit of the desired end state. The StratCom staff ensures that all NATO activities are conceived, planned and executed with consideration of their desired outcome in the information environment. Actions, images and words are coordinated to carry a clear narrative in support of NATO's military and political objectives. StratCom provides the focused conception, planning, execution and evaluation of information activities and support to wider activities, enabled by a comprehensive understanding of audiences and how they exist in a contested information environment.

2.3 **Policy.** Military Committee (MC) 0628, *NATO Military Policy on Strategic Communications* provides military direction for StratCom and directs the establishment of a StratCom directorate, led by a director of communications (DirCom), within each NATO military headquarters. This groups together the Info Ops staff function and communications capabilities (Mil PA and PsyOps) to provide an organizational structure that coordinates and synchronizes their outputs, through the Info Ops staff, thereby enabling and maximizing their utility across all campaign themes within the continuum of competition.

2.4 **Definition.** StratCom is defined as: 'in the NATO military context, the integration of communication capabilities and the information staff function with other military activities, in order to understand and shape the information environment, in support of NATO strategic aims and objectives.'

Section 2 – Information operations policy, related definitions and principles

2.5 **Information operations.** The staff function that coordinates and integrates the StratCom direction and guidance horizontally within each NATO military headquarters is Info Ops, which is comprised of four functions: analysis, planning, integration and assessment. This staff function leads in the understanding of audiences, through the information environment assessment (IEA), to identify cognitive effects within audiences, which will be planned as information activities and coordinated with the joint targeting process. The Info Ops staff function is active throughout the headquarters either through planning and integrating information activities, with the primary purpose of creating cognitive effects, or more broadly supporting activities that are designed for physical and or virtual effect and have an informational element to them. As part of the behaviour centric approach to operations, the continual assessment of audiences and the impact of activities, through the IEA, is a critical contribution to operations assessment to determine if objectives have been achieved.

2.6 **Policy.** MC 0422, *NATO Military Policy for Information Operations* provides military direction for the implementation of Info Ops within NATO military structures. It provides the direction to analyze and assess the information environment, to plan, synchronize and integrate information activities, and to create desired effects. It establishes the links required for Info Ops to be integrated effectively within the NATO Command Structure and force structure. Info Ops focuses on three interrelated activity areas.

a. Information activities focused on always preserving and protecting the Alliance freedom of action in the information environment. This is achieved by defending the data, networks and information that supports Alliance decision makers and decision-making processes.

b. Information activities focused on behaviours, perceptions and attitudes of audiences as part of Alliance military operations to induce, reinforce, convince or encourage them in support of NATO objectives.

c. Information activities focused on countering an adversary's information activities, as well as their command and control functions and capabilities that support opinion forming and decision-making processes.

2.7 **Definitions.** The definition of Info Ops and related terms are as follows.

a. **Information operations.** A staff function to analyze, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and audiences in support of mission objectives. (NATO Agreed)

b. **Information activities.** Activities performed by any capability or means, focused on creating cognitive effects. (NATO Agreed)

c. **Communication activities.** For the purpose of this publication, communication activities are described as information activities performed by military public affairs and psychological operations capabilities.

d. **Information environment.** An 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. (NATO Agreed)

Information operations planners must identify the effects required and, by understanding the information environment, select the appropriate activities to create them

2.8 **Principles.** Info Ops is based on certain principles that shape its role within the planning and joint targeting processes, and thus directs the way in which information activities support the execution and achievement of the Alliance's objectives across the full range of NATO's campaign themes. The principles of Info Ops that apply across all operational themes throughout the continuum of competition are as follows.

a. **Comprehensive understanding.** The foundation for Info Ops is derived from understanding the commander's objectives, guidance and intent, the StratCom direction and guidance and a comprehensive understanding of the information environment, the audiences that inhabit it and how information impacts them in the operating environment.

b. **Narrative-led.** Actions, images and words, derived from the narrative, must be coherent with one another at all levels – strategic, operational and tactical.

c. **Effects focused.** Info Ops planners must identify the effects required to achieve the Alliance's objectives and then, through their understanding of the information environment, select the appropriate activity or combination of activities to create those effect.

d. **Integrated.** All activities will have a resultant cognitive effect and Info Ops staff must be integrated throughout the planning and targeting process to recognize and explain the behavioural change from activities.

e. **Agility.** Info Ops staff must be agile and responsive to a continually evolving information environment. They must persistently monitor, assess and evaluate effects in the operating environment to allow rapid adjustment to be made when required.

f. **Centralized planning and decentralized execution.** Due to the requirement to fully integrate the Info Ops staff, the principles of centralized planning and decentralized execution apply at all levels of command. Therefore, commanders should be prepared to accept risk and delegate authority to the lowest practical level within political constraints in line with the doctrinal tenet of mission command.

g. **Assessment.** A key part of Info Ops is an effective assessment of the short- and long-term effects of activities, directed towards objectives. It is recognized that behavioural change is not usually immediate. Attention is focused on indicators of desired change or desired sustainment of an audience's behaviour, such as political activity and expressions of unrest, or changes in the perception or attitude of the civilian population.

Section 3 – Focus of information operations

2.9 An audience group's effectiveness is a function of will, understanding and capability. They must have the will to act, an understanding of the situation and possess the capability to act. If any one of these elements is missing, decisions and actions will be affected. Activities coordinated through Info Ops focus directly on influencing will, affecting understanding and on those capabilities that promote understanding or the application of will. Therefore, they have applicability across the full spectrum of military operations.

2.10 **Will.** Will is the faculty by which an actor decides upon and initiates a course of action. It includes factors such as motivation, perception, attitude, beliefs and values and encompasses the intent to act or resist. Within the direction and goals of wider military operations, and mission-specific NATO

guidance, information activities are aimed at actors at any level capable of influencing the situation.

a. Information activities aim to reinforce or deter specific types of behaviour by affecting an audience's will. For adversaries, this could focus on undermining their cohesion by questioning the legitimacy of leadership and cause. Information activities may undermine an adversary's moral power base, separating leadership from its supporters (political, military and public), thus weakening their desire to continue and affecting their actions. Info Ops will also address attempts to influence NATO's will to maintain Alliance/coalition cohesion and enhance our freedom of action. Such attempts may come from adversaries, potential adversaries and other actors.

b. Information activities aim to protect those capabilities, such as friendly command and control systems (C2S) and communication and information systems (CIS) infrastructure, which allow a commander to exercise effective command, impose their will and seize and maintain the initiative. NATO may seek to protect approved parties' capabilities proactively by countering adversary information activities.

Vignette: Information activities in the 2020 Nagorno-Karabakh war

In September 2020, Azerbaijan launched an operation to recapture territory in Nagorno-Karabakh that had been lost to Armenia in the 1990s. Given its topography, geographical isolation and relatively poor infrastructure, access to the territory had always been limited, both physically and from an information perspective. Few foreign media teams or observers were able to access the territory as the war developed; reporting was patchy and verification of facts and claims from either of the warring sides was hard to achieve.

This complex and opaque information environment provided ideal conditions for both sides to conduct information activities. With the backing of Turkey and a significant technical and capability advantage, Azerbaijan was also able to use state powers to periodically deny Internet connectivity and control the domestic media environment. Armenia was supplied with Russian armaments, including extensive electromagnetic warfare assets, allowing it to conduct jamming of communications. State strategic

communication efforts on both sides had been shaping the narrative in the approach to the outbreak of fighting; claims of human rights abuses, war crimes and ethnic cleansing seemed easy to establish but harder to disprove, given the difficulty in accessing facts.

As the war progressed, the speed of Azerbaijan's advances and effectiveness of its drone operations began to create a crisis of confidence for Armenia. Azerbaijan capitalised on this, using social media to spread images that supported the idea of crumbling Armenian morale. Armenian counter-narratives focused on claims of torture and abuse of Armenian prisoners of war. Ultimately, Azeri narratives dominated, creating the conditions for successful operational-level Info Ops that contributed to a decisive victory for Azerbaijan.

While Armenia and Azerbaijan fought over Nagorno-Karabakh, their citizens battled on social media

Social media rhetoric from politicians, citizens and others helped influence political moves.

Analysis by Katy Pearce
December 4, 2020 at 7:45 a.m. EST

A family drives a truck loaded with a small house along a highway as they leave their home village in the disputed region of Nagorno-Karabakh on Nov. 18, before a cease-fire takes effect to halt weeks of fighting. (AP Photo/Sergei Grits)

© Washington Post

2.11 **Understanding.** In the context of decision-making, understanding is the perception and interpretation of a particular situation to provide the context, insight and foresight required for effective decision-making. This situation is interpreted through the prism of an audience's culture, environment and perception. Information activities seek to deny, degrade, disrupt or present the information available to an audience to affect perception and thereby understanding. They also aim to ensure the information available to friendly decision-makers is safeguarded and assured. In this way, shared understanding between allies and other approved parties will be possible, thus improving decision-making and effectiveness.

2.12 **Capability.** An actor's capacity for action is dependent upon their physical capabilities and their utility in a particular situation. Information activities will seek to affect those capabilities, such as C2S, CIS infrastructure and propaganda facilities that enable actors to understand a situation and apply their will.

a. Information activities seek to: degrade, disrupt, deceive, destroy or deny those capabilities that allow adversary decision-makers to increase their understanding and bolster, impose, apply and sustain their will to act effectively and (where appropriate) exercise command and control.

b. Information activities also seek to attack the source of an adversary's power base, splitting internal and external groupings and alliances. The aim is to influence their decision-making processes, thereby preventing them from taking the initiative.

c. Information activities also aim to protect capabilities. For example, friendly C2S and CIS infrastructure that allow the joint force commander to exercise effective command, impose their will and seize and maintain the initiative.

Section 4 – Communication capabilities

2.13 **Communication capabilities.** For the purposes of this publication, communication capabilities refer to the capabilities of PsyOps and Mil PA that are used to communicate as information activities.

a. **Psychological operations.** PsyOps are defined as: 'planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives.' The primary purpose of PsyOps is to influence approved target audiences to have a direct effect on both understanding and will, together with an indirect effect on capability. PsyOps contribute to security, understanding and awareness and can mitigate and contrast or counteract hostile information and disinformation against audiences of importance to NATO. For more detail, see Allied Joint Publication (AJP)-3.10.1, *Allied Joint Doctrine for Psychological*

Operations and MC 0402, *NATO Military Policy on Psychological Operations*.

b. **Military public affairs.** Mil PA is a capability responsible for promoting NATO's military aims and objectives by communicating, as part of strategic communications, accurate information to audiences in a timely manner. In addition to its responsibility for external communications with audiences, the Mil PA capability is also responsible for internal communications. This communication enhances awareness and understanding of the military aspects of the Alliance's role, aims, operations, missions, activities and issues, thereby reinforcing its organizational credibility. An AJP on Mil PA is in development but additional further information on the capability can be found in *NATO's Allied Command Operations and Allied Command Transformation Public Affairs Handbook* and MC 0457, *NATO Military Policy on Public Affairs*.

Vignette: agile use of information at the strategic level – observations from Russia-Ukraine war

Russia's illegal invasion of Ukraine in 2022 demanded an innovative response from Ukraine's allies, to create dilemmas for Russia and support Ukraine while avoiding escalation. As Russian disinformation aimed to divide European allies and cause disorientation, the UK responded by choosing to reveal Russian weaknesses and call out its disinformation. This gave rise to a phenomena of rapidly declassifying high-grade intelligence and releasing it to the media. Defence Intelligence began to issue daily media releases giving assessments, supported by imagery, to highlight Russian failures and Ukrainian successes where appropriate. Declassified intelligence was also used to publicly attribute Russian breaches of international law and to pre-empt and debunk attempts by Russia to divert international attention through disinformation.

Section 5 – Additional capabilities and techniques likely to be integrated as information activities

2.14 Whilst any military capability could deliver an information activity there are several capabilities that are more frequently planned, integrated and assessed by Info Ops. These capabilities should be based upon the mission, commander's direction and resources available.

2.15 **Cyberspace operations.** Cyberspace is far more than just the Internet. It includes networks and devices connected by wired connections, wireless connections and those that appear to be not connected at all. All devices that are reachable via cyberspace could be potential targets and potential threats. Adding to this ever-growing domain is the use of such technology in the expanding number of domestic goods, also known as the Internet of things. Cyberspace is not limited to, but at its core consists of, a computerized environment, artificially constructed and constantly changing. Cyberspace infrastructure is largely globally interconnected; however, geographic boundaries do apply in the context of jurisdiction, with national responsibilities. Cyberspace is not only in constant flux but, even more importantly, it may be used by anyone for almost any purpose. Cyberspace is also distinct in that its underlying physical elements are entirely human made, which is different from land, air and space, and sea. Risks in cyberspace may be managed through manipulation of the domain itself. Cyberspace operations intended to preserve own and friendly freedom of action in cyberspace and/or create effects to achieve military objectives are conducted through two types of operations: offensive cyberspace operations (OCOs); and defensive cyberspace operations (DCOs). All operations are approved through the joint targeting process and resourced through the sovereign cyberspace effects, provided voluntarily by Allies (Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)) mechanism. OCOs techniques and capabilities can be used to conduct information activities to create a multiplier effect to other information activities put in place. DCOs consist of measures to preserve the ability to use cyberspace with the purpose of enabling own freedom of action and force protection. Further information is contained in AJP-3.20, *Allied Joint Doctrine for Cyberspace Operations*.

UK cyber and electromagnetic considerations

UK 2.1. As described in Joint Doctrine Publication (JDP) 0-50, *UK Defence Cyber and Electromagnetic Doctrine*, Defence has chosen to consider capabilities and activities relating to cyberspace and the electromagnetic environment together, as a single operational domain. The cyber and electromagnetic domain is defined as: a domain comprising of capabilities which enable activities that maintain freedom of action by creating effects in and through cyberspace and the electromagnetic spectrum.[3]

UK 2.2. Defence does not deliver all cyber operations; it provides its part within a complex tapestry of UK national cyber capability. As such, Defence is not responsible for defending all of UK cyberspace or countering all these potential threats; it is a whole of society effort.

Cyber as a tool for information activities

UK 2.3. The influence role of cyber and electromagnetic power enables Defence to shape (for example, defeat, deceive, degrade, deny) adversary capabilities, allowing the behaviour of audiences and the course of events to be influenced as desired. The missions that make a particular contribution to influence activities are: offensive cyber operations; cyber information operations; counter cyber; and electromagnetic attack. Offensive cyber operations are defined as: activities that project power to achieve military objectives in or through cyberspace.[4] They may transcend the virtual dimension (for example, websites and social media feeds) into effects in the physical dimension (for example, causing computer hardware destruction) and, most importantly, directly influence the cognitive dimension of thoughts, beliefs, interests and perceptions of individuals and groups.

UK 2.4. Offensive cyber activity can be used to inflict permanent or temporary effects, thus reducing an adversary's confidence in their networks, information or other capabilities for a specific period. Offensive cyber operations may be used in isolation or in conjunction with other capabilities to create effect. Such action can support deterrence by communicating intent or threats. The link to influence activity is strong and at the operational/tactical level of operations there is a need to coordinate offensive cyber operations and Info Ops, where conditions and classifications allow. Further details are given in JDP 0-50, *UK Defence Cyber and Electromagnetic Doctrine* and the *Cyber Primer*.

3 JDP 0-01.1, *UK Terminology Supplement to NATOTerm*.
4 Ibid.

2.16 **Electromagnetic warfare.** Individuals and organizations, both non-military and military, use devices whose functionality depends on access to the electromagnetic spectrum (EMS). EMS management is critical for joint forces to operate freely within the electromagnetic environment (EME). Electromagnetic warfare is a key segment of electromagnetic operations and can provide the operational-level commander with a means to shape the EME to support NATO operations, whilst denying the same to the adversary or enemy. The development of electromagnetic warfare activities begins at the operational level by understanding the military objectives and analyzing desired effects. This leads to a selection of suitable electromagnetic warfare actions – electromagnetic attack, electromagnetic defence or electromagnetic surveillance – that can be applied individually or together with actions from other functional areas to create the desired effects. Effects created by electromagnetic warfare can be temporary or permanent and have the potential to minimize the use of force, hence avoiding unnecessary casualties and collateral damage. Electromagnetic warfare also supports the conduct of friendly information activities, such as cyberspace operations, deception and PsyOps. Further information is contained in AJP-3.6, *Allied Joint Doctrine for Electronic Warfare*.

2.17 **Civil-military cooperation and civil-military interaction.** Civil-military cooperation (CIMIC) is the joint function of capabilities that enables civil-military interaction (CMI) between the military and non-military audiences within the engagement space. CIMIC supports, facilitates or directly conducts CMI through activities such as civil-military liaison, key leader engagement (KLE), assessments of the civil environment, as well as planning and coordination with relevant non-military audiences within the joint operations area to inform the comprehensive understanding of the operating environment. The use of CIMIC capabilities and the conduct of CMI activities are based on the core interacting principles of: respect, trust, transparency, credibility and reliability, which information activities should not undermine. Info Ops and CIMIC staff are closely aligned in a headquarters to plan and integrate CMI activities, and to provide understanding based on interactions with audiences. The outcome of interacting with non-military audiences may well serve the StratCom goals set for an operation by executing collective civil-military activities, visible to the public, in favour of the military, thereby underlining unity of effort. CIMIC staff must be represented in the Information Activities Working Group at all levels of command, not only to identify information activity opportunities but also to address potential negative effects military or civil-military activities and operations may have on the perception of the public. Further information is contained in AJP-3.19, *Allied Joint Doctrine for Civil-Military Cooperation*.

Information operations and civil-military cooperation staff are closely aligned in a headquarters to plan and integrate civil-military interaction activities

2.18 **Physical destruction.** Through the joint targeting process, using a myriad of delivery means, targets could be affected to create a specific effect on the information position and decision-making ability of an audience, and therefore be an information activity. Such targets, will be identified through the IEA, developed and submitted by Info Ops for approval through the joint targeting process.

2.19 **Operations security and deception.** Operations security (OPSEC) and deception are discrete military activities which may be used as information activities. To maintain credibility of the overall messaging, the information activities within OPSEC and deception plans must be coordinated with Info Ops, as with any other discrete process or capability, if they are not compartmentalized for security reasons. This will ensure that other NATO-related activities such as Mil PA and CIMIC, which have no role in planning or executing deception, do not contradict the promotion of the narrative. From an Info Ops perspective, OPSEC and deception can be used to influence audiences and further detail is contained in AJP-3.10.2, *Allied Joint Doctrine for Operations Security and Deception.*

a. **Operations security.** The aim of OPSEC is to deny critical information and indicators to adversaries. 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 essential elements of friendly information (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. Counter-surveillance may support OPSEC by identifying adversary surveillance capability that is targeting a defined EEFI.

b. **Deception.** Deception is a psychological process that seeks a behavioural response, be it action or inaction. 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 learning, motivations for learning and human thinking, the latter otherwise known as cognition. Deception explicitly targets the critical decision-maker assessed as most likely to respond in the desired behavioural manner. 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 is unlikely to 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.

2.20 **Information assurance.** Information assurance is the protection and defence of information and information systems by ensuring their availability, integrity and confidentiality. Information assurance requires management processes to ensure the systems and networks employed to manage the critical information used by an organization are reliable and secure, and processes are in place to detect and counter malicious activity. Information assurance includes elements of physical security (for example, personnel and document security) and information security. Communications security

and computer security are integral elements of all military CIS operations and should be considered throughout planning and execution. Cyber defence activities are a pivotal element of CIS security – enabling delivery and management of CIS services in response to malicious actions perpetuated through cyberspace. Information should be protected to the correct level, ensuring that valid information is available to authorized users, and preventing valid information from being available to unauthorized persons. The degree of security provided should be consistent with: the requirements of CIS users; the vulnerability of transmission media to interception and exploitation; and the reliability and releasability of communications security hardware and software. Further information is contained in AJP-6, *Allied Joint Doctrine for Communication and Information Systems*.

2.21 **Emerging and disruptive technologies.** Emerging and disruptive technologies (EDTs) will impact resilience, including civil preparedness, by affecting critical infrastructure and public information (including Info Ops) anywhere across the Alliance. EDTs are changing the way NATO and its adversaries operate in times of peace, crisis and conflict. The private sector and academia are the driving force behind innovation in many EDTs; their speed of development, dual-use applicability and wider societal impact cause disruption, bringing both opportunities and risks.

Section 6 – Engagement, presence, posture and profile

2.22 **Engagement.** Traditionally, engagement has focused only on the key leader. While this remains important, recent operations have emphasized that engagement at all levels and all times can have a differential impact on behaviours, attitudes and perceptions of audiences. Engagements should be consistent, inclusive, culturally sensitive, credible, adaptive, balanced and pragmatic. Info Ops staff should be a key contributor to engagement planning if they do not own the headquarters process. Engagement can be broadly categorized as described below.

a. **Strategic engagement.** Strategic engagement can be considered as those engagements that are conducted at the strategic level to influence non-military instruments of power, in pursuit of strategic objectives. It will normally be directed or approved by NATO Headquarters or Supreme Headquarters Allied Powers Europe (SHAPE)

before being conducted. At the operational level, strategic engagement will normally be conducted by the commander, or exceptionally delegated to the deputy commander. Strategic engagements will not be delegated below headquarters joint force command level.

b. **Key leader engagement.** KLEs are engagements between NATO leaders and other key decision-makers to achieve defined goals. These planned engagements can be used to shape and influence leaders within the assigned operations areas or may also be directed toward specific groups such as religious leaders, civil society leaders (including women's groups where appropriate), academic leaders and tribal leaders (for example, to solidify trust and confidence in NATO forces). Regular interactions between key leaders and other headquarters within the NATO Command Structure should be considered as routine chain of command activity and not KLE. Info Ops supports these engagements by identifying and maintaining a database of all key leaders and their interrelationships. Detailed knowledge of key leaders' personalities, their leadership styles, ambitions, motivations, objectives (short- and long-term), current stances, dependencies, psychological profiles and personal histories, together with any previous target audience analysis conducted on the leader or the leader's primary home audience is essential to provide the context to plan appropriate information activities. A vital component in all plans will be to recognize the complex, adaptive relationships and dependencies that exist between actors. The Info Ops staff will integrate the commander's KLE plan, which contains information on the situational context (planning milestones), critical events, planned contacts of the command group and staff interactions with relevant actors, objectives, main themes or issues to be addressed, desired effects and assessment criteria.

c. **Soldier-level engagement.** In the contemporary operating environment, we recognize that operations are conducted amongst people. Soldiers[3] interact with local populations daily. Consequently, soldier engagement is likely to comprise most engagements; they can occur as a dynamic, chance opportunity or a deliberate, scheduled meeting. These interactions can bridge the difference between the aims and ambitions of local audiences and the NATO force, therefore soldiers have to be aware of the impact that their behaviour may have. To best exploit this potential opportunity, people in the engagement

3 'Soldier' in this context includes sailors, marines and air force personnel, as well as NATO civilians.

teams should be trained on how to engage with the local population by understanding the different perspectives and given a simple narrative, based on the institutional, strategic or micro narrative, that they can construct their engagement around.

2.23 **Engagement categories.** Key leader and soldier-level engagements fall into two main categories: deliberate and dynamic. As such, the categories differ in their planning and execution.

a. **Deliberate.** A deliberate engagement is a planned and anticipated personal interaction designed to create a specific outcome. These engagements may be face-to-face or interactions by other means, such as telephone or video conference.

b. **Dynamic.** Dynamic engagements are unanticipated or impromptu encounters for which specific planning has not been conducted. Encounters that will require engagement can occur as part of routine activity and soldiers' or leaders' ability to exploit them will depend heavily on training, experience and their understanding of the mission narrative.

People engaging with audiences should be trained to use messages based on the institutional, strategic or micro narrative

2.24 **Cultural understanding and engagement.** Understanding cultural sensitivities is essential and will shape engagement activity. The cultural calendar presents many opportunities, but understanding cultural sensitivities surrounding events may also preclude engagement and will be factored into planning. In some societies it may not be possible to directly engage with specific groups or demographics (such as women, specific castes or tribes) for cultural reasons; it may be desirable to engage with religious leaders due to their influential position in society. In such societies, special provision should be made to enable these types of engagement (which will generally be deliberate) through appropriate training in areas such as gender perspective in military operations, and preparing personnel to conduct them (for example, female and/or mixed engagement teams and/or personnel with experience or knowledge on specific religions). Emphasis should be placed on language skills and intercultural competency skills, minimizing the requirement to use interpreters.

2.25 **Presence, posture and profile.** The mere presence of a force has a significant and varying effect on perceptions of audiences. The force's presence, posture and profile (PPP), and that of its leadership, conveys a direct message to local audiences and a secondary message to global audiences through modern communications technology. Info Ops staff will advise during the planning process on how aspects of PPP will impact on the operating environment.

a. **Presence.** The presence or threat of deploying a force will have an impact on perceptions. Deploying even limited capability to the right place at the right time adds substantial credibility to messages delivered through other channels and provides a major contribution to deterrence.

b. **Posture.** The posture and conduct of force elements can be scrutinized by global audiences and make a considerable difference to the perceptions of all actors. Therefore, force posture must be deliberately considered and feature in prevailing cultural and threat factors.

c. **Profile.** The public profile of commanders at all levels will be of significant interest to many audiences. Their public role must be carefully analyzed and opportunities used to transmit key messages.

UK 2.5. Profile considerations should also include a force's combat profile. This could include, for example, deployment of weapon systems, carriage of personal weapons and equipment, and order of dress.

2.26 **Conduct and standards of behaviour.** A positive image may be impacted by the behaviour of a force. It is essential that all NATO personnel uphold the highest standards of personal and professional behaviour. Not complying with relevant standards and policies may undermine the effectiveness and credibility of the Alliance, the legitimacy of individuals and risk mission success. Further information is contained in the *Code of Conduct*, *NATO Policy on Preventing and Responding to Sexual Exploitation and Abuse* and the Bi-Strategic Command Directive (Bi-SCD) 040-001, *Integrating UNSCR 1325 and Gender Perspective into the NATO Command Structure*.

Section 7 – Training and education

2.27 Effective implementation of the Info Ops staff function requires organizations to be staffed with trained and experienced practitioners. Allied Strategic Communications Publication (ASCP)-01, *NATO Strategic Communications Training Standards* defines the minimum level of proficiency for all personnel assigned to positions within NATO to ensure Allies understand and agree the competency and experience standards required by individuals assigned to serve in NATO Info Ops positions.

2.28 Info Ops success is heavily dependent on the competence of individuals and the understanding of its application by commanders and their staff. This competence is determined by criteria including: ability; knowledge; understanding; capability; interaction; experience; and motivation. These can only be achieved by effective education and training, initially performed by the nations, then enhanced by NATO.

2.29 Info Ops personnel should be integrated into NATO military training and exercises to ensure that commanders and staffs are aware of the requirement and procedures to integrate information activities into planning and conducting operations, the effects of those integrated operations on the information environment, and the negative consequences of not integrating operations. Ideally, exercise scenarios should be situated in a real framework that will enable the IEA to be conducted and a baseline understanding be developed.

2.30 Prior to taking an Info Ops position, personnel should be qualified according to a specific training programme attached to the position/title assigned and/or through a national training programme. This programme should provide an understanding of the differences between national and NATO doctrine as well as tactics, techniques and procedures in place for the planning, conduct and coordination of NATO information activities.

UK 2.6. The Joint Information Activities Group (JIAG) develops and delivers the Info Ops and information activities training for Defence in support of UK operations. The JIAG delivers the following courses (further details of JIAG training can be found in 2022DIN07-019).

a. **Joint Information Operations Course.** The Joint Information Operations Course (JIOC) trains Info Ops practitioners to understand, plan, coordinate and assess information activities at the operational level. The course is also suitable for those working in Defence strategic communication and joint effects roles. It is aimed at operational-level planners.

b. **Military Psychological Operations Course.** The Military Psychological Operations Course (MPOC) provides the knowledge and skills required for employment in PsyOps roles at the tactical level, but they are applicable to operational-level roles. The course covers the processes, tools and techniques involved with planning and creating effects to achieve behavioural change on target audiences. MPOC is also suitable for those working in behavioural change processes in an operational context. It is aimed at tactical PsyOps practitioners and Info Ops staff.

c. **Audience Analysis Course.** The Audience Analysis Course (AAC) provides the knowledge and skills required for employment in audience analysis roles and related assignments. The course trains practitioners to select and analyse audiences to produce information packs in support of operational and strategic planning. It is aimed at analysts who are conducting baseline, mission and target audience analysis in support of Info Ops.

d. **Information Operations Foundation Course.** The Information Operations Foundation Course (IOFC) provides the foundation knowledge of Info Ops, covering offensive and defensive elements, open-source intelligence collection, audience segmentation and PsyOps.

e. **Defence Communicators Course.** The Defence Communicators Course (DCC) provides the knowledge and skills required for employment in media and communications roles up to the strategic level, focusing on news writing, imagery, working with journalists and digital media. DCC is aimed at media operations and StratCom practitioners.

Key points

- Info Ops is the staff function that coordinates and integrates the StratCom direction and guidance horizontally within NATO military headquarters.
- Info Ops leads in the understanding of audiences, through the IEA, to identify what cognitive effects can be created among audiences.
- Information activities aim to reinforce or deter specific types of behaviour by affecting an audience's will.
- Information activities aim to protect those capabilities that allow a commander to exercise effective command and seize the initiative.
- Information activities can, for example, degrade, disrupt, deceive, destroy and/or deny those capabilities that allow adversary decision-makers to increase their understanding.
- Information activities also seek to attack the source of an adversary's power base, splitting internal and external groupings and alliances.
- Whilst any military capability could deliver an information activity, there are several capabilities that are more frequently integrated and assessed by Info Ops: cyber and electromagnetic; CIMIC; physical destruction; OPSEC and deception; and information assurance.
- The JIAG develops and delivers the Info Ops and information activities training for Defence in support of UK operations.


GRAVITY

Chapter 3

The J10-Strategic Communications directorate and its staff products are explained in this chapter. The interaction of the information operations function across the headquarters is examined in detail. The UK's Strategic Communication Action and Effects Framework is also introduced.

3

> It is true of course, that I have a will of iron, but it can be switched off if the circumstances seem to demand it.

Bertie Wooster,
taken from P. G. Wodehouse,
Jeeves in the Morning

Chapter 3

J10-Strategic Communications directorate and headquarters interactions

3.1 Chapter 3 introduces the J10-Strategic Communications directorate (J10-StratCom) and its staff outputs before examining the role of the information operations (Info Ops) staff. It then explores how Info Ops interacts across the headquarters and the governance forums that Info Ops staff use and interact with.

Section 1 – J10-Strategic Communications and its staff products
Section 2 – The information operations staff
Section 3 – Staff interactions
Section 4 – Staff directorates
Section 5 – Headquarters' battle rhythm and governance

Section 1 – J10-Strategic Communications and its staff products

3.2 To optimize the delivery of strategic communications (StratCom) and the execution of the Info Ops staff function, Military Committee (MC) 0628, *NATO Military Policy on Strategic Communications* directed the establishment of an organizational structure that coordinates and synchronizes information activities to enable and maximize their utility across the continuum of competition in all campaign themes. This structure is focused on the vertical alignment of StratCom in the NATO Command Structure (NCS) and should not be seen as a rival to existing structures, nor a compartmentalized staffing process but as an opportunity to optimize the interaction and integration provided by Info Ops staff across the headquarters. The functions of J10 StratCom are covered in detail in Allied Joint Publication (AJP)-10, *Allied Joint*

Doctrine for Strategic Communications. This publication focuses on the role of the Info Ops staff within the directorate and the wider headquarters.

3.3 The Info Ops staff provide the horizontal StratCom integration within a headquarters. They provide the director of communications (DirCom) and the commander with an analysis and assessment of the information environment as part of the comprehensive understanding of the operating environment (CUOE). They plan, synchronize and continuously integrate information activities to create effects in support of the commander's objectives. The Info Ops staff within J10-StratCom retains its functional responsibilities for developing and updating planning products in support of J3 Operations and J5-Plans staff directorates. The Info Ops staff provides six distinct functions within J10-StratCom.

a. **Information environment assessment.** The Info Ops staff provide audience research, monitoring and analysis products and lead the information environment assessment (IEA) understanding process. The Info Ops IEA staff can be both stand alone or act as part of the J10-StratCom contribution to the wider headquarters and Alliance understand function.

b. **Information operations planning.** The Info Ops planning staff plan, synchronize and coordinate information activities, and support the development of the StratCom operational staff work. The Info Ops planning staff can either be stand alone or act as part of the J10-StratCom contribution to the operations planning process.

c. **Information activities synchronization and integration.** The Info Ops staff synchronizes and integrates information activities in coordination with other headquarters staff directorates and through the Information Activities Working Group (IAWG).

d. **Strategic engagement.** The Info Ops staff are the lead function for planning and synchronizing engagement, including liaising with the civil-military interaction (CMI)/civil-military cooperation (CIMIC) staff, and briefing and preparing personnel for engagement activity.

e. **Contribution to joint targeting.** The Info Ops staff may nominate and develop targets through the joint targeting process. They make sure information activities are synchronized and advise on anticipated second order effects on the behaviour of audiences from planned targeting

activity. They also contribute to consequence management by exploiting or mitigating the effects of munitions based targeting.

f. **Counter-hostile information activities.** This is a multidisciplinary effort that within J10-StratCom is led and coordinated by the Info Ops staff, in collaboration with the psychological operations (PsyOps) staff, to deliver agility and proactiveness within the information environment.

The UK government's approach to countering disinformation – the Enhanced Resilience Programme

UK 3.1. The Counter Disinformation and Media Development (CDMD) programme was established in 2016 within the UK government's Russia Unit as a response to Russia's increasingly aggressive use of Info Ops. The Kremlin invested extensively in disinformation tactics and made them central to its strategies to deny, distort and distract from its own hostile actions and to undermine democracy and institutions in target nations. It employed them to significant effect around the annexation of Crimea, the war in Syria, the Salisbury poisoning and the illegal invasion of Ukraine. CDMD has rapidly evolved into a major programme, delivering projects designed to identify Russian Info Ops and to provide counter-narratives, support key institutions to build societal resilience to Russian malign influence and support coordinated international responses. CDMD has transitioned into the Enhanced Resilience Programme, which is actively supporting national resilience to disinformation in countries across wider Europe.

3.4 **Narratives.** The narrative binds the Alliance vertically through the levels of operations, and horizontality across the instruments of power and with partners. NATO Headquarters will generate a narrative to guide Alliance operations and activity, which will then be refined as direction by the StratCom staff at Supreme Headquarters Allied Powers Europe (SHAPE) in a framework and implementation guidance, along with a communications plan. There are three types of narratives – institutional, strategic and micro – that are mutually supporting and form the basis for planning and executing NATO's activities. Further guidance on constructing and analyzing narratives can be found in AJP-10, *Allied Joint Doctrine for Strategic Communications*.

a. **Institutional narrative.** NATO's institutional narrative is rooted in the North Atlantic Treaty: 'A democratic, multinational alliance uniting across borders to guard, with courage and competence, against threats to our home.' This is elaborated in the communication strategy focused on the three communications pillars of 'NATO protects, NATO unites, and NATO strengthens', as well as providing direction on how to understand and engage to counter adversary information activities.

b. **Strategic narrative.** Strategic narratives drive the campaign themes and provide the political-military guidance for the activity. For an operation they will be developed by NATO Headquarters, in conjunction with the joint force commander, as an essential component of the planning process, seeking to establish and sustain the moral authority for NATO's actions and undermine support for its adversaries. It should include the previously described strategic attributes, state why and how NATO forces are engaged, towards what objectives, and what constitutes success. As missions often include the participation of non-Alliance partner nations and other non-military actors as part of the comprehensive approach, a mission-specific strategic narrative must be crafted to meet the expectations of the entire coalition and the host nation.

c. **Micro narrative.** Micro narratives act as local or regional narratives to support short-term objectives and activities. Micro narratives are focused to account for different languages, dialects, historical context, cultural and gender considerations. Micro narratives should be included in the courses of action decision-making criteria when planning.

3.5 **Frameworks.** The StratCom frameworks are the primary tool used by NATO to provide direction and guidance for the planning and execution of all activities. The generic structure of a framework is articulated in AJP-10, *Allied*

Joint Doctrine for Strategic Communications. This publication outlines: the aim of the framework and its duration; the narrative and core messages; the definitions of audiences and any relevant segmentation; the StratCom objectives and themes; and any relevant focus areas. Additionally, specific issues are covered in annexes outlining, for example, audience effects, risks and opportunities. Frameworks exist in three tiers depending on the level of operation.

a. Tier 1 – NATO strategic communications framework. Issued under the authority of the Secretary General to enable consistency across NATO diplomatic, military and non-military agencies to allow decentralized planning and execution of activities in line with the strategic narrative.

b. Tier 2 – Allied Command Operations strategic communications framework. SHAPE will produce a Tier 2 Allied Command Operations (ACO) StratCom framework for specific operations that may not be covered under the NATO StratCom framework or they may develop a supporting annex. In addition, SHAPE issues an annual framework to articulate StratCom objectives and priorities for the next 12 months.

c. Tier 3 – Strategic communications framework. NATO Command Structure and NATO force structure headquarters may generate their own Tier 3 frameworks to support specific activities or issues relevant only to their organization and its subordinates. A Tier 3 framework may only be issued if no Tier 1 or Tier 2 framework covers or exists for the specific activity that the command or force wants to conduct. Tier 3 frameworks need to be coordinated with SHAPE's Communications Division.

Strategic Communication Actions and Effects Framework

UK 3.2. The Chief of the Defence Staff (CDS) directive provides the strategic direction and guidance for every operation or framework involving UK Armed Forces. At the heart of the directive are the military strategic objectives (MSOs), which identify the key audiences and desired effects to be created on those audiences, as well as providing a short narrative to give the specific context for specific audience sets. The Strategic Communications Actions and Effects Framework (SCAEF) is included as an annex to the CDS directive. MSOs should be linked to intended effects, actions and evaluation, in terms of suitable metrics or indicators that are

realistic and can be monitored from when the information activities begin. Further details on the SCAEF, including a generic SCAEF structure and details of the phases, which includes assessment advice, are given in Joint Tactics, Techniques and Procedures (JTTP) 3.81, *Integrated Action: An operational level guide to the audience-centric approach for commanders and staff*.

Section 2 – The information operations staff

3.6 The Info Ops staff comprises a Chief Info Ops and sufficient supporting staff relative to the headquarters' size and function (such as planners, targeteers and information environment analysts). Info Ops staff's focus and responsibilities are determined by the command level and assigned mission. An operational-level headquarters requires a comprehensive staff to enable analysis, planning, operations, intelligence support and specialists to conduct targeting and operations assessment. At the tactical level, the need will focus more on specialists to deliver capability to achieve specific objectives. Within the headquarters, the Chief Info Ops is responsible for the following functions:

- providing the lead on analyzing the information environment and contributing to the CUOE;
- providing specific Info Ops input to develop the commander's direction and guidance;
- preparing Info Ops contributions to the commander's plans and orders;
- helping determine the desired effects to support operations objectives, the nodes or targets that could generate those effects and appropriate activities for inclusion in the joint targeting process;
- recommending priorities for information activities;
- assessing information activities and contributing to the overall operations synchronization and assessment; and
- coordinating with all principal functional staff areas, specialist staff and higher and subordinate headquarters on Info Ops matters.

Information operations staff provide the planning input regarding audiences and the information environment to describe the likely impact of planned activities

Section 3 – Staff interactions

3.7 **General.** To successfully meet the commander's objectives, Info Ops must be integrated and coordinated with all other joint force activities. To create the desired effects, headquarters, adjacent and subordinate commands, and the strategic-political level must achieve a coherent and synchronized approach. This is best realised by thoroughly coordinating effects within the engagement space and related military activities from the strategic to the tactical level within the overall StratCom framework. Commanders should ensure that any information activities likely to affect other areas are implemented with prior coordination (through Info Ops) and notification.

3.8 **The joint staff.** A headquarters will be organized to suit a mission and task in accordance with AJP-3, *Allied Joint Doctrine for the Conduct of Operations*. The headquarters will be made up of principal advisors and staff directorates. Info Ops staff have responsibility for planning and integrating information activities. They also provide the planning input regarding audiences and the information environment to describe the likely impact of planned activities and support the subsequent consequence management.

3.9 **Principal advisors.** The commander will usually have the three following principal advisors: the chief of staff (COS), the political advisor and the legal advisor (LEGAD). In addition, and dependent on the mission or task, additional

functional principal advisors will be used, such as a cultural advisor or gender advisor. The DirCom will perform the role of functional principal advisor to the commander for StratCom and the Chief Public Affairs Officer is the functional principal advisor for military public affairs as well responsible for engagement with the media. These are likely to also be a directorate lead to remain integrated in headquarters staff processes, which must not be undermined when executing their advisor role. From an Info Ops perspective, the principal advisors will also provide advice and guidance to J10 StratCom. Maintaining a strong relationship with the principal functional advisors is essential.

Section 4 – Staff directorates

3.10 The basic organization of a headquarters are the staff directorates, typically J1 to J10-StratCom, which provide staff supervision of related processes, activities and capabilities associated with the joint functions. They provide expertise for planning, decision-making, execution and assessment within the headquarters. StratCom is a whole of headquarters activity but it is likely that Info Ops will predominately interact and integrate with the following staff directorates.

3.11 J2 – Intelligence. NATO Intelligence is primarily focused on the actor category of audiences and specifically the adversary and enemy. NATO intelligence uses the joint intelligence preparation of the operating environment (JIPOE), along with the IEA to produce a CUOE[4] where a commander is able to fuse the understanding with analysis of missions and tasks to determine the effects required to attain the end state. The IEA focused staff within Info Ops should be closely aligned and integrated with the J2 branch so that fused understanding using common processes is completed to support the commander's decision-making. Further information on intelligence capabilities and procedures can be found in AJP-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security* and subordinate publications. The CUOE and the IEA are described in detail in Chapter 4 of this document. The NATO JIPOE process consists of three basic steps that are described below.[5]

4 ACO's *Comprehensive Operations Planning Directive* (COPD), Version 3, states that the terms CUOE and comprehensive preparation of the operating environment (CPOE) are often used synonymously. CPOE has traditionally been used to describe the appreciation of an environment, however, CUOE, with the use of the word 'understanding', better implies the need to acquire the knowledge and then interpret or comprehend its significance with regard to the crisis.

5 Some individual member states use different JIPOE/intelligence preparation of the battlefield processes with a different number of steps.

a. **Step 1 – Describe and evaluate the operating environment.** The first step assesses the effects of relevant factors concerning the operating environment on the activities conducted by both friendly and opposing forces. In relation to counterterrorism and force protection, this will include the threats to military and non-military operations, (for example, the ethnic distribution of the population and its loyalties). Some of the principal factors affecting the operating environment are terrain, infrastructure, information environment, protected areas, weather conditions, environmental conditions and medical factors. Info Ops will contribute to this step by providing deductions on the operating environment drawn from the IEA.

b. **Step 2 – Evaluate actors in the operating environment.** The aim of step 2 is to identify an actor's likely doctrinal courses of action, independent of terrain and weather constraints (i.e., how the actor fights according to their tactical doctrine or based on experience from previous operations). Threat evaluation consists of locating and identifying the actor, identifying their tactical doctrine or methods of operation, and predicting their doctrinal courses of action.

c. **Step 3 – Determine actor courses of action.** In step 3 of the JIPOE process, the results of the area evaluation are combined with the doctrinal courses of action and other overlays developed in the threat evaluation. The aim of threat integration is to identify how the operating environment will shape operations and turn it into practice.

3.12 **J3 – Operations.** The essential role of the J3-Operations staff, at all levels of command, is to act as the focal point through which the commander directs the conduct of an operation, ensuring unity of effort toward achieving mission objectives and the most effective use of resources to support immediate and planned operations. The J3 Operations staff may be comprised of sections or cells focused on operational domain and specialist capabilities depending on the mission or task. An Info Ops cell will be required, either ad hoc or on a permanent basis, to integrate information activities through the Information Activities Coordination Board (IACB) and act as the embedded staff from J10-StratCom. Further information on the conduct of operations and headquarters activities are found in AJP-3, *Allied Joint Doctrine for the Conduct of Operations*. Some specific areas of J3-Operations that will need to interact with Info Ops staff are joint effects and joint targeting.

a. **Joint effects.** Targeting at the military-strategic level is the responsibility of the joint effects function, managed by the Joint Effects

Branch at SHAPE. The Joint Effects Branch is responsible for the targeting function and ensuring all information activities are deconflicted, through the IACB, and synchronized with the joint effects function to ensure successful alignment of activities in the engagement space. At both the military-strategic and operational levels, Info Ops staff maintain a close working relationship with their respective joint effects' counterparts through various working groups and boards.

b. **Joint targeting.** Joint targeting is the process of selecting and prioritizing targets, matching the appropriate resources to them and taking account of operational requirements and capabilities, with a view to creating desired effects in accordance with the commander's objectives. Joint targeting is a multidisciplinary process, which requires participation from all joint force staff elements and component commands at all levels of command, along with various non military audiences. The Info Ops staff are responsible for generating audience understanding and assessment through the IEA to be presented and fused into the CUOE. Target audience analysis (TAA) is conducted to provide the requisite understanding to support the application of a capability as an activity. Target material produced by Info Ops staff is coordinated with the Centralized Targeting Capacity. Info Ops staff may nominate and develop target guidance via the joint targeting process, if necessary. An important role for Info Ops staff is to contribute to consequence management by exploiting or mitigating the effects of munitions-based targeting. Further information on the targeting process can be found in AJP-3.9, *Allied Joint Doctrine for Joint Targeting*.

3.13 **J5 – Plans.** The J5-Plans directorate assists the joint commander in preparing the operation plan and planning for future operations. It coordinates planning efforts within the headquarters and with higher, subordinate and adjacent commands and non military audiences. Planning is conducted within a headquarters for different time horizons with current operations focused on immediate shaping and execution of the existing plan; future operations look further ahead, with a focus on the next important change in objectives and priorities for subordinate forces. The guidance for NATO planning is found in AJP-5, *Allied Joint Doctrine for the Planning of Operations* and Supreme Allied Commander Europe's (SACEUR's) ACO's *Comprehensive Operations Planning Directive* (COPD) that covers the operations planning process and COPD planning process in detail. The Info Ops contribution to the planning process is covered in detail in Chapter 4.

3.14 **J6 – Communication and information systems.** The J6-communication and information systems (CIS) directorate staff ensures that adequate CIS support is provided for operations and that interoperable procedures are used across the joint force. The ability to communicate, process, manage and pass information is a key enabler for planning and executing information activities; the Alliance seeks information advantage to ensure it communicates and passes information through enabled and resilient CIS to support the conduct of activities that influence behaviour. Critical NATO CIS activities must be fully coordinated between the Info Ops staff, cyberspace operations and the J6-CIS directorate staff through the IACB. CIS doctrine can be found in AJP-6, *Allied Joint Doctrine for Communication and Information Systems* and cyberspace doctrine can be found in AJP 3.20, *Allied Joint Doctrine for Cyberspace Operations*.

3.15 **J9 – Civil-military cooperation.** The CIMIC staff provides a capability that supports a commander to achieve objectives across the full range of NATO campaign themes across the continuum of competition. The staff takes a leading role in gathering, assessing and reporting information regarding the civil environment in cooperation with other military functions. Info Ops is closely aligned to the J9-CIMIC directorate to align messages with key non-military audiences. It also provides the understanding of audiences from the IEA and may use CIMIC capabilities for information activities. Further information is contained in AJP-3.19, *Allied Joint Doctrine for Civil-Military Cooperation*.

An important role for information operations staff is to contribute to consequence management by exploiting or mitigating the effects of munitions-based targeting

Section 5 – Headquarters' battle rhythm and governance

3.16 Effective operations require synchronizing strategic, operational and tactical processes to ensure successful mission planning, preparation and execution. This process, called the battle rhythm, is a routine cycle of command and staff activities intended to synchronize current and future operations in accordance with the joint task force headquarters' decision cycle. Battle rhythm events in peacetime or baseline activities and current operations will differ from those in training, crisis or conflict. The COS establishes and maintains the battle rhythm in most headquarters, and it is expected that the following meetings, perhaps with different names dependent on headquarters style, will always be part of a routine cycle of the commander and staff at which J10-StratCom and its Info Ops staff will be present and expected to deliver input.

3.17 **Briefs.** The primary brief in a headquarters is the commander's brief, which is normally held at the beginning of the daily cycle to set the foundation for the staff effort for the next period. The commander would be briefed on the past and next 24 hours in detail before examining the next 48 hours in outline. The brief is delivered by the J3 Operations staff with input from all staff directorates, who attend to be aware of any refined direction and guidance from the commander. To prepare for the commander's brief, the directorates are likely to have their own brief beforehand using a similar approach. Info Ops staff will provide assessments from the IEA, notable changes to the behaviour baseline, as well as trends and predictions for the next 48 hours.

3.18 **Boards.** Boards are either command, which are decisional in their nature and chaired by the commander, or functional, which are aimed at getting functional guidance from a commander based on staff recommendations or focused on synchronization or resource allocation for an operation or activity.

a. **Joint Coordination Board.** The Joint Coordination Board (JCB) is a command board and the commander's principal meeting aimed at effects and activity synchronization, resolving potential areas of conflict and delivering the commander's priority guidance. The attendance is normally restricted to the commander, their principal advisors and component commanders. DirCom, as StratCom advisor, and Chief Public Affairs Officer as public affairs advisor will attend.

b. **Assessment Board.** The Assessment Board is a functional board where the operations assessment is presented to the commander. The aim is to get endorsement of the assessment and to receive the commander's direction and guidance for subsequent planning. Assessment provides a common understanding and enables the commander to refine direction and guidance for achieving objectives. The assessment aspect of the IEA will be a primary feed into the operations assessment cell, who lead on the Assessment Board. DirCom and/or J10-StratCom staff members provide advice on effects in the information environment and are focused on behavioural and attitudinal change in the audience analysis.

c. **Joint Targeting Coordination Board.** The Joint Targeting Coordination Board (JTCB) is a functional board that synchronizes joint targeting activities to provide the optimum approach for creating the desired effects in support of operational objectives. The JTCB reviews the outputs from the Joint Targeting Working Group (JTWG) via the Joint Fires and Effects Working Group (JFEWG). It gathers inputs from the targeting community, effects subject matter experts and the IAWG to prepare the target list for JCB review and the commander joint task force's approval. The board will: validate changes to the targeting database; issue direction and guidance to coordinate target material production (including TAA); update targeting guidance; approve the draft joint prioritized target list; and coordinate intelligence staff products to ensure intelligence gains/losses are accounted for. Additionally, a target validation board may be established within the JTCB; in this case the JTCB will also validate targets for inclusion on the joint target list. Info Ops staff will represent and share the IAWG targeting outputs and consider the predicted cognitive impact of targets as well as providing the behavioural assessment of other activities.

d. **Strategic Communications Coordination Board.** The Strategic Communications Coordination Board (SCCB) is chaired by the COS, but most often delegated to Director Communications Division (Dir ComDiv) or Chief Info Ops to direct the cognitive line of effort to support the strategic and/or operational objectives. It provides StratCom direction and guidance to the headquarters and specifically to the Info Ops staff to prioritise understanding analysis, and approve and guide the planning, integration and assessment of information activities. It reviews the outputs from the IAWG and Communications Engagement Working Group (CEWG) and approves what can be submitted to the JTCB as cognitive effect targets. It will also provide advice on possible effects in

the information environment created by other military actions. The SCCB liaises with all functional areas, especially with J2, J3, J5, J9, the LEGAD and with subordinate commands, as well as coordinating with outside agencies. The SCCB will prepare and approve the submissions to the JTCB, Assessment Board and the JCB. It normally meets weekly during operations and when required during peacetime to prepare information for the JCB.

e. **Information Activities Coordination Board.** The IACB provides a forum for approving, coordinating, deconflicting and monitoring all information environment related plans and activities for submission to the commander for approval. It ensures that information activities are coherent and synchronized with other activities. Within the scope of its assigned functions, the IACB will initially coordinate target nominations related to information and information systems to facilitate subsequent harmonization at the JTCB. It will also provide advice on possible effects in the information environment created by other military actions. The IACB liaises with all functional areas, especially with J2, J3, J5, J9, the LEGAD and with subordinate commands, as well as coordinating with outside agencies. Some headquarters have chosen to not convene the IACB and use the SCCB and IAWG in its place. The IAWG is explained further in Chapter 4.

f. **Joint Collection Management Board.** The Joint Collection Management Board (JCMB) is a J2-led functional board that coordinates the collection activities between the different service components and intelligence and operations staffs. The JCMB produces and approves the collection task list, resolves potential areas of conflict, and assigns execution responsibilities to deconflict and synchronize collection activities. The JCMB issues priority guidance across the service components to ensure that the overall joint intelligence, surveillance and reconnaissance effort is coordinated, prioritized, appropriately balanced and focused on the commander's objectives. Info Ops staff may request additional capabilities to enhance the IEA understanding.

3.19 **Working groups.** Working groups are permanent or ad hoc forums within a joint task force headquarters, formed around a specific function whose purpose is to provide analysis to users. They consist of a core functional group and other staff and components. The working groups prepare and rehearse submissions to their respective board. Info Ops staff are likely to be involved in working groups across the headquarters, but the following working groups are an example of those more commonly attended.

a. **Assessment Working Group.** The Assessment Working Group prepares the operations assessment to be presented to the commander as part of the CUOE for approval. Input from the IEA is essential to provide the cognitive impact of activities against the approved behaviour baseline.

b. **Joint Coordination Board Working Group.** The Joint Coordination Board Working Group discusses and refines options to be presented to the commander for command decisions at the JCB. It is attended by DirCom, who ensures options under consideration are coherent with the StratCom framework and consider cognitive effects aspects, and they provide recommendations on whether actions should be taken forward or suspended.

c. **Strategic Information Activities Working Group.** The Strategic Information Activities Working Group (SIAWG) is a SHAPE-level DirCom-led working group with subordinate headquarters. It coordinates and synchronizes all StratCom planning activities, assesses own and hostile narratives, and provides further StratCom direction and guidance. It normally meets weekly during operations and when required during peacetime to prepare information for the SCCB.

d. **Information Activities Working Group.** The IAWG is a DirCom-led working group with other staff directorates and subordinate headquarters. In line with direction and guidance from the SCCB, it ensures that information activities are coherent and synchronized with the cognitive line of effort and other activities in the engagement space. The IAWG will approve the input from Info Ops staff to the planning process and will coordinate target nominations related to information and information systems to facilitate subsequent harmonization at the JTCB. The IAWG liaises with all staff directorates, principal advisors and with subordinate commands, as well as coordinating with non-military organizations. It normally meets daily during operations and when required during peacetime to prepare information for the SCCB. The IAWG is explained further in Chapter 4.

e. **Communications and Engagement Working Group.** The CEWG is a working group with subordinate headquarters. It coordinates and synchronizes all information activities and engagement that use communication capabilities, and feeds into the SCCB. It normally meets daily during operations and when required during peacetime to prepare information for the SCCB.

f. **Joint Fires and Effects Working Group.** The JFEWG takes the output of the JTWG, IAWG and any other targeting working groups and ensures optimal effect capability selection and coordination to achieve the commander's objectives. Targeting staff will begin initial coordination of effect integration and synchronization. The JFEWG represents the final stage of target development prior to submission to the JTCB. Info Ops staff will represent and share the IAWG outputs and then consider proposals to achieve first order cognitive effects and assess second and third order cognitive effects resulting from of other military activities.

g. **Joint Targeting Working Group.** A JTWG may be established to prepare and staff targeting products before they are presented to the JTCB, via the JFEWG. It is normally supported by a staff who manage the joint targeting system, source up-to-date intelligence products (including battle damage assessments), produce targeting products and act as custodians of target folders. Info Ops staff ensures that the JTWG output is coherent with the IAWG outputs.

h. **Target Development Working Group.** The Target Development Working Group (TDWG) ensures that sufficiently developed targets are submitted to the JTWG. It assists in the coordination and deconfliction of target development activities. Info Ops staff may submit developed targets to the Target Validation Board (TVB) for validation, and/or recommend refinement to targets submitted by other organizations based on the predicted cognitive impact of a target being prosecuted.

i. **Civil-Military Interaction Working Group.** The Civil-Military Interaction Working Group (CMIWG) is a cross-functional forum created to holistically address the broad challenges of CMI for the headquarters. Info Ops staff will provide the audience assessment of non-military audiences to assist with engagement planning.

3.20 **Operational planning teams.** Operational planning teams are small planning groups focused on specific or specialist planning activity, with tailored membership depending on their task. Due to their coordinating and integrating role, Info Ops staff are likely to be included in all operational planning teams.

Key points

- The Info Ops staff provide the horizontal integration of StratCom within a headquarters. They provide the commander with analysis and assessment of the information environment as part of the CUOE. They plan, synchronise and integrate information activities in support of the commander's objectives.

- The Info Ops staff fulfil six functions within J10-StratCom: IEA; Info Ops planning; information activities synchronisation and integration; strategic engagement; contribution to joint targeting; and counter-hostile information activities.

- StratCom frameworks are the primary tool used by NATO to provide direction and guidance for the planning and execution of all activities.

- Defence uses the SCAEF to identify key audiences and desired effects to be created on those audiences for a particular operation or campaign.

- The assessment (monitor and evaluate) phase is crucial to understanding the effectiveness of actions within the information environment and to decide whether it is necessary to adjust the current approach.


IRESON A.T.

Chapter 4

Chapter 4 examines each of the four components of the information operations staff function: analyse, plan, integrate and assess. These components feed into the headquarters planning and integration processes; the procedures involved for each function are described, explaining the information environment assessment in detail. UK boxes highlight the UK's approach to audience analysis.

> People don't change their behaviour unless it makes a difference for them to do so.
>
> Sharon Stone

Chapter 4

Information operations

4.1 Chapter 4 examines each of the four components of the information operations (Info Ops) staff function: analyze, plan, integrate and assess. These components are not done in isolation and will feed into the headquarters planning and integration processes. It outlines the processes involved for each function and highlights where to find additional information.

Section 1 – Analyze
Section 2 – Plan
Section 3 – Integrate
Section 4 – Assess

Section 1 – Analyze

4.2 Info Ops is responsible for the information environment assessment (IEA), which is the primary tool for understanding and assessment from an audience perspective. The IEA, alongside the joint intelligence preparation of the operating environment (JIPOE), feeds into the comprehensive understanding of the operating environment (CUOE) to enable a commander to fuse the understanding with analysis of missions and tasks to determine the effects required to attain the end state.

4.3 **The cognitive hierarchy.** The foundation of conducting operations in the engagement space is to understand the cognitive hierarchy and the relationship between data, information, knowledge and understanding. This process raises information from the lowest level (data) to the highest (understanding). With understanding, decision-makers can make better decisions and more effectively control actions by their forces. The distinctions between the levels of the cognitive hierarchy are not always clear. To understand the importance of the cognitive hierarchy for the operations, we need to understand that data is not limited to cyber data. For example, a NATO activity is data. An audience who observes a NATO activity is observing data. When the observing data is processed by an audience in the cognitive layer, it becomes information (data-in-context). The audience then analyzes that information, and it becomes knowledge that then affects understanding which, finally, affects behaviour.

4.4 **The information environment.** The information environment[6] is the principal environment of decision-making; where humans and automated systems observe, conceive, process, orient, decide and act on data, information and knowledge. It is characterized by an extremely high demand for digital access to near-real time media and interpersonal virtual connectivity at an unprecedented scale. Some of today's very relevant characteristics are ubiquitous on-demand media and interpersonal hyper connectivity that enables collaboration and information-sharing on an unprecedented scale and with an unprecedented speed. All activities will have an effect in the cognitive dimension whether designed or because of action or inaction. Through a comprehensive understanding of the information environment, effects can be designed to influence the behaviour of audiences as they observe, orient and act on data, information and knowledge. The information environment is illustrated in Figure 4.1, which shows the dimensions and their layers within them.

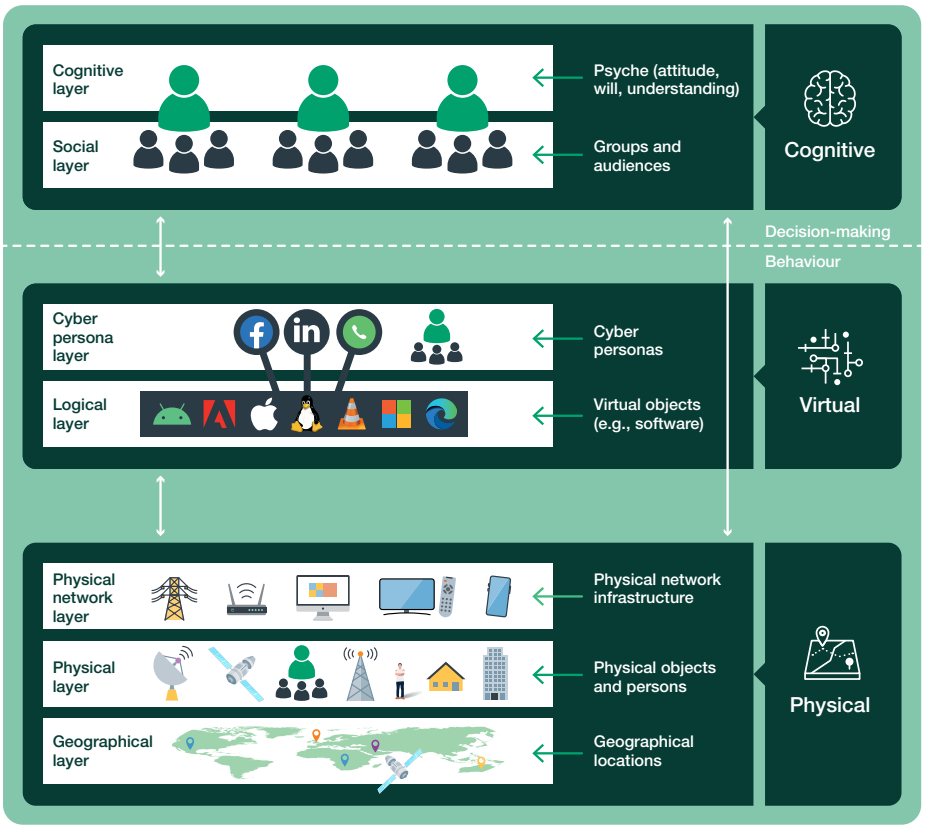


Figure 4.1 – The information environment

6 The information environment is defined as: 'an environment comprised of the information itself, the individuals, organizations and systems that receive, process and convey information, and the cognitive, virtual and physical space in which this occurs.'

The dimensions

4.5 The information environment is segmented into three dimensions: the cognitive; physical; and virtual. These dimensions are further segmented into seven layers, as shown in Figure 4.1, that provide greater fidelity to analyze more-than-communication functions and military means to generate attitudinal and behavioural change. The interconnected nature of the dimensions and their respective layers expand the opportunity to identify potential targets and to identify the interrelated aspects of the information environment. By envisioning the layers, excluding the cognitive, as potential communication channels, we expand both potential targets and tools available to achieve desired outcomes.

4.6 The **cognitive[7] dimension** is the decisive dimension because it is where cognitive effects affect individuals' thinking, which drives behaviours and decisions. All actions in other dimensions and their layers ultimately affect the cognitive dimension. It is comprised of two layers: cognitive and social.

a. The **cognitive layer** is where information is interpreted, but not transmitted, by individuals. This layer is intangible and therefore non-observable, and it comprises the audiences' will, cohesion, perceptions, beliefs, interests, values, aims, decisions and behaviours.

b. The **social layer** is where information comprises the ways in which individuals' behaviours are influenced by the pressures of the sociocultural environment, and where social networks and culture influence individuals' decision-making. It encompasses all forms of interaction, for example, between people in the economic and/or political spheres. One factor included in this layer would be key influencers within an audience. Factors such as their credibility, level of influence and reach would inform planners on how to produce more influence in a particular audience.

4.7 The **virtual dimension** is the virtual space in which audiences virtually interact. It is comprised of two layers: cyber-persona and logical.

a. The **cyber-persona layer** is how the personas of audiences manifest as online profiles and interact through followers and subscribers to digital content. This includes both public (for example, Twitter profiles)

7 Some nations refer to this dimension as the psychological dimension consisting of cognitive (logical thought), affective (emotion) and behaviour.

and other personas (for example, WhatsApp broadcast channel). Individuals could have multiple personas and non-sentient actors can also operate personas through artificial intelligence. In addition to their physical means, key influencers can impact an audience through the cyber-persona layer.

b. The **logical layer** contains less human-perceptible activity in the form of processing, storage and transmission of analogue and digital data and information. It is the virtual infrastructure where the dependencies, services and other resources are used to exchange data, such as social media services and file storage. This layer also includes network configurations, data and data transfer protocols, domain names and other electromagnetic or virtual processes. This layer is near-exclusive to the cyberspace domain where actions can affect the confidentiality, integrity or accessibility of data.

4.8 The **physical dimension** is made up of the geographic areas where audiences live, including all physical objects and infrastructure that support them. It is the space where physical activities take place and individuals, nations, states, cultures and societies interact. It is comprised of three layers: physical network, physical and geographical.

a. The **physical network layer** is the physical network infrastructure that underlies the virtual layers. The physical network layer is where the transmission and reception of unstructured raw data between a device and a physical transmission medium takes place. The physical network layer includes those capabilities that enable communication, such as radio masts, satellite transmitters and receivers and those which convert the digital bits into analogue signals or vice versa for transmission and reception. The components of the physical layer can be described in terms of a network topology.

b. The **physical layer** is where audiences interact and where all physical technical-communication and human infrastructure resides. The human infrastructure comprises those physical areas that facilitate communication, such as a market, meeting place or places of worship. Words and images are considered physical information and not virtual.

c. The **geographical layer** explores how audiences inhabit the Earth. It also looks at how physical geography and climate affects how audiences communicate.

Information environment assessment

4.9 A dedicated team within the Info Ops staff is responsible for the IEA and they are assisted by numerous stakeholders who provide specialist input and analysis. The IEA comprises people, processes and technology to support understanding, decision-making and the application of capability in the engagement space. An IEA handbook will describe the processes in detail. The IEA can be broken down into two main elements: analysis and assessment. The IEA is a continuous process that is enhanced with time and resource being applied to it. The assessment element is outlined in detail within Section 4 of this chapter. The analysis element can be broken down into several analysis processes, as illustrated in Figure 4.2.

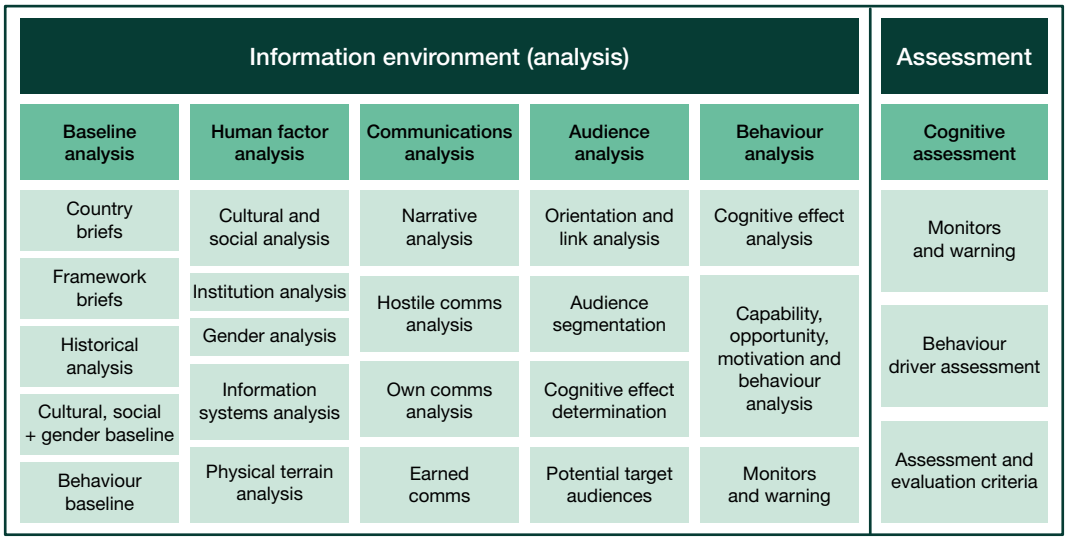


Figure 4.2 – Information environment assessment

4.10 **Baseline analysis.** The baseline analysis is the foundation of understanding for an operation. Within NATO, each joint force command is focused on specific threats and will allocate their resources to enable comprehensive baseline analysis for a given threat, region or geographic area. The baseline analysis should be published regularly and able to provide any organization the requisite background detail to make initial capability and force composition decisions and provide the foundational understanding to begin an operation. This analysis would be comprised of briefs outlining the historical, cultural and geographical analysis of the operating environment and some initial analysis into audiences from a cultural, social, gender and behavioural perspective.

NATO typically uses the 'PMESII' analytical framework to conduct human factor analysis, considering six elements: political, military, economic, social, infrastructure and information

4.11 **Human factors analysis.** An analysis of the human factors that affect the operating environment is known as human factors analysis (HFA). Several analytical frameworks are available to examine the human factors but the most common in NATO are the following six elements: political, military, economic, social, infrastructure and information (PMESII). Modification or other models are admitted such as PMESII + physical and time (PMESII-PT), geospatial + PMESII (GPMESII), PMESII + health (PMESIIH), or areas, structures, capabilities, organizations, people and events (ASCOPE), which may be better suited to describing a certain operating environment or support a planning process. The most common HFA tool is to compare PMESII and ASCOPE factors against each other using a matrix as shown in Figure 4.3. Within HFA, the following subcategories are analyzed.

PMESII / ASCOPE analysis	Political	Military/security	Economic	Social	Infrastructure	Information
Area	Boundaries, districts, political party areas, ethnic or adversary strongholds	Areas of operation, boundaries, districts	Agriculture, mineral, industry, economic centres, retail, offshore deposits	Religious boundaries, international governmental organizations and non-governmental organizations	Air, road, rail and river networks	Coverage for media types
Structures	Government centres, legislative, executive, and judicial (courts and prisons)	Military bases, police stations, militia, contractors	Industrial zones, technology parks, education facilities, economic centres, retail centres	Retail, sports and leisure facilities, religious buildings, meeting places	Routes, hospitals, water and power plants, education facilities, sanitation, irrigation	Communication infrastructure locations
Capability	Constitution and governance, opposition, effectiveness and corruption	Combat power, missions, intent, aims, constraints, freedoms	Industrial, agriculture, finance, markets, black market, corruption	Literacy and education levels, access to basic services, languages	Effectiveness of basic services (waste, water, power, food, health)	Literacy, data coverage, censorship, languages, outreach
Organization	Political parties, government	Police, military, security contractors	Companies, business forums, centres of learning	Ethnic groups, religions, charitable, youth, crime	Ministries, construction and maintenance facilities management, non-governmental organizations	TV, radio, Internet providers, print media, digital media, telephone coverage
People	Political leaders, diplomatic leadership	Leadership (military, police, adversary group)	Business leaders, economic governance, criminal leaders	Ethnic group leaders, religious leaders, patronage leaders, criminal leaders, influencers	Foreign investors, leadership, contractors, non-governmental organizations	Influencers, media reporters, journalists, public relations
Events	Elections, rallies, campaigns	Wars, operations, parades, anniversaries	Market days, opening hours, harvest seasons, business holidays	Religious events, key anniversaries, seasons, national holidays and events	Projects (ongoing and planned), investments, proposed closures	National censorship, campaigns, advertising, propaganda

Figure 4.3 – PMESII/ASCOPE orientation analysis

a. **Cultural and social analysis.** The cultural analysis provides an understanding of how people interpret and orient themselves to the operating environment by examining ideology and psychology. It includes the general and pervasive ideas of society, language and historically rooted concepts of collective identity, as well as the fundamental existence and moral beliefs provided by religion.

b. **Institution analysis.** Institution analysis seeks to understand the landscape of the institutions of audiences that live within the operating environment. Institutions embody ideas such as practices and conventions that form the landscape of social life. This includes political institutions, law and judicial machinery, associations and dissident groups operating outside of institutional conventions.

c. **Gender analysis.** A gender analysis develops the baseline understanding of the operating environment and the dynamics of a conflict. It may be conducted by addressing the goals, strengths, weaknesses and interdependencies of the main actors in the PMESII domains. When analyzing these factors from a gender perspective, the role, position and situation of men, women, boys, girls and others should be considered in relation to each operational domain. This not only looks at the human composition, but also the disaggregated gendered factors such as literacy rates, access to resources, educational background and other demographics that could influence or shape perceptions of the population. Refer to Allied Command Operations' (ACO's) *Gender Functional Planning Guide* for how to use the Gender Analysis Tool.

d. **Information systems analysis.** Information systems analysis involves mapping the information environment to determine how audiences get information, how that information propagates within an audience, and how it impacts perception and behaviour. Specific focus will be on communication infrastructure and the media as the primary means to share information.

e. **Physical terrain analysis.** In conjunction with the JIPOE, the physical terrain is analyzed to determine its impact on how audiences communicate. This analysis will examine the impact of terrain, urbanization, vegetation, lines of communication, climate and weather on the audiences' behaviour.

4.12 **Communications analysis.** Through the military public affairs (Mil PA) staff's input to the IEA, actionable insights are identified that can be embedded in the next cycle of its own communications activity to enable continuous improvement. These insights draw from assessment of narratives, NATO's own communications, those communications that are earned and hostile information activities (including those generated by potential adversaries), the overlaps between them and relating these insights to broader activity within the information environment. The methodology includes the assessment of its own communications objectives and cognitive effects, and is based on audience analysis.

a. **Narrative analysis.** An analysis of narratives of all of those in at least the actor category of our audience segmentation provides the foundation for communications analysis. Determining which organizations could influence our objectives and understanding their narratives provides an excellent tool to build our information activities planning upon. Narrative analysis is explained in detail within Allied Joint Publication (AJP)-10, *Allied Joint Doctrine for Strategic Communications*.

b. **Own communications.** An assessment of the effectiveness of NATO's communications is required to help in the assessment and refinement of strategic communications (StratCom). This assessment of own communications seeks to identify and assess the audiences targeted and reached, communications strategies and campaigns, themes, topics and the communication channels and means used to communicate.

c. **Earned communications.** Earned communications is anything that is said by third parties or international media outlets about a topic or organization during an observed time period that has not been generated by NATO or an affiliated party and over which NATO does not have any control. It could be positive, neutral or negative. It encompasses an understanding of the channels by which these communications are promulgated and discussed. Earned communications develops an understanding of the issues that relate to NATO in the information environment but are not necessarily driven by NATO messaging and therefore impact how NATO is perceived by NATO's key audiences/stakeholders.

d. **Hostile communications.** An assessment of the capability of adversary communications is required to develop an understanding

of hostile communications against NATO, including how potential or existing adversaries communicate against key or the most vulnerable audiences/stakeholders. This both contributes to the indications and early warnings process and helps NATO mitigate and manage hostile messaging in the information environment and to improve counter efforts.

4.13 **Audiences.** To understand and effect changes in an audience's attitudes and behaviours, it requires an understanding of audiences to identify those who can influence the end state and their current activities, perceptions and behaviours. Audiences need to be segmented to enable more focused understanding and subsequent targeting of capabilities to achieve the desired behavioural changes. An audience is defined as: 'an individual, group or entity whose interpretation of events and subsequent behaviour may affect the attainment of the end state.' Audiences are segmented into three main categories depending on how they can affect our end state, as illustrated in Figure 4.4.

Audience
An individual, group or entity whose interpretation of events and subsequent behaviour may affect the attainment of the end state.

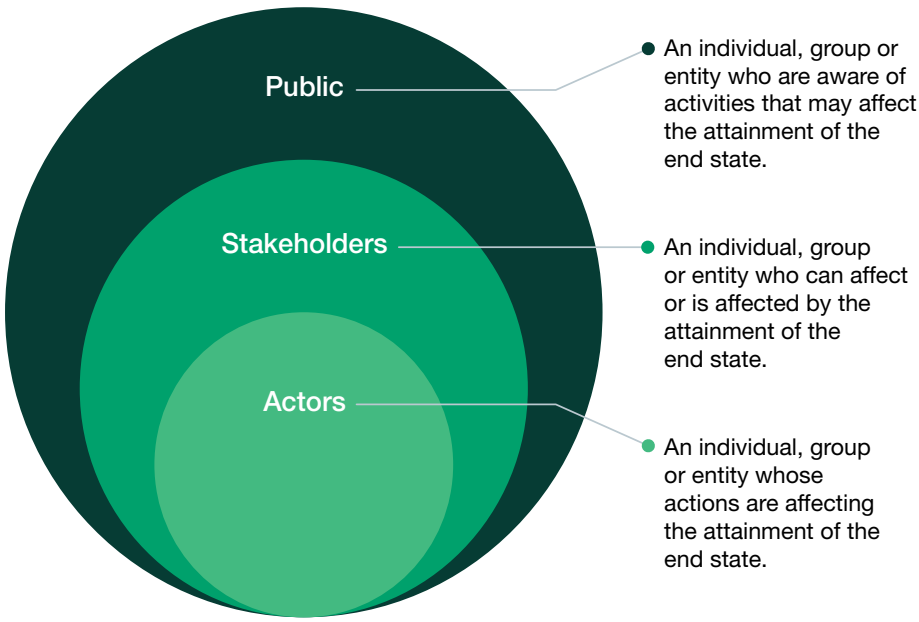


Figure 4.4 – Audience groupings

4.14 Audience analysis is the understanding and segmentation of audiences in support of the achievement of objectives. Audience analysis within the IEA is a four-stage process, as described below.

a. **Orientation.** Audiences are grouped into the three categories of audience – public, stakeholder and actor – and further segmented using one, or a combination, of the analytical frameworks outlined in paragraph 4.11. This orientation allows for further focused segmentation to be conducted. Using the people row from the PMESII/ASCOPE analysis, as shown in Figure 4.3, will provide a start point for audiences to be analyzed in detail.

b. **Link analysis.** Link analysis breaks down audience groupings into subcategories and determines the relationships between groupings; it can be used to identify centres of gravity or target groupings for activities. A simplified example of a link analysis looking at an operational network is illustrated in Figure 4.5.

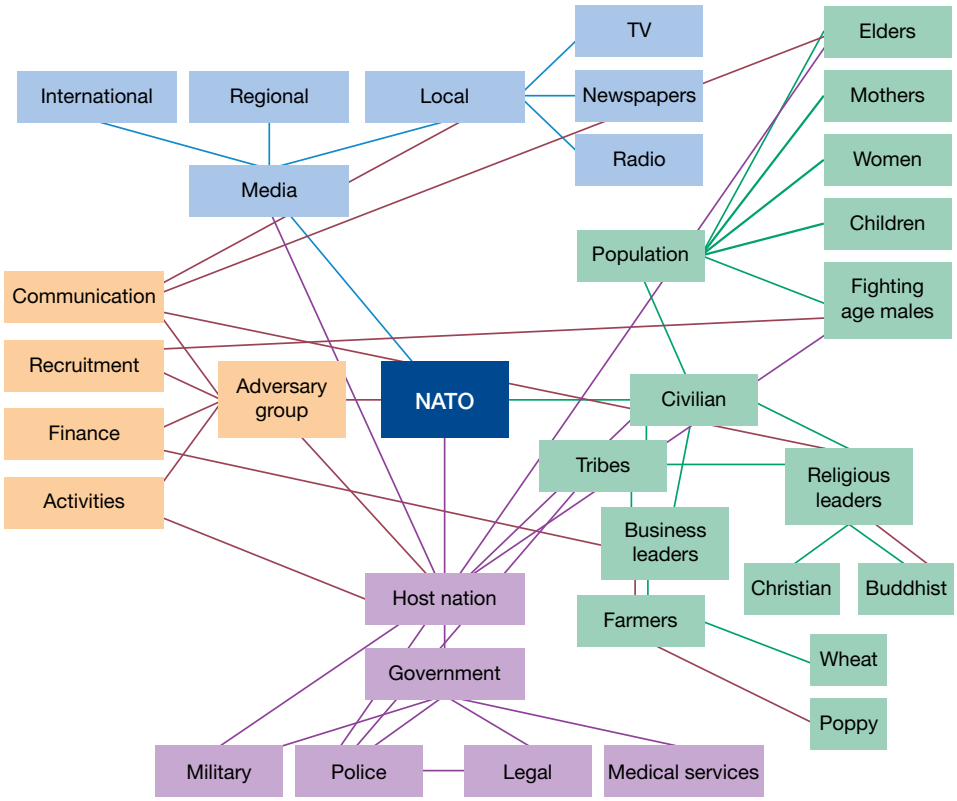


Figure 4.5 – Example link analysis

c. **Audience segmentation.** Audience groupings from the orientation phase can be further segmented by placing them on a shade shift diagram, which is a visual representation of how audiences relate to each other and their ability to affect our end state. These audience groupings can then be assessed to determine where they would best be on the shade shift to enable the achievement of objectives. Understanding where audiences' groupings are segmented and why helps with determining effects to change or influence behaviour that will result in a shift of audience groupings to support the achievement of objectives. The shade shift can be manipulated in a myriad of ways using different axes depending on the most appropriate way to display the information. An example of a simplistic audience segmentation using shade shift is illustrated in Figure 4.6.

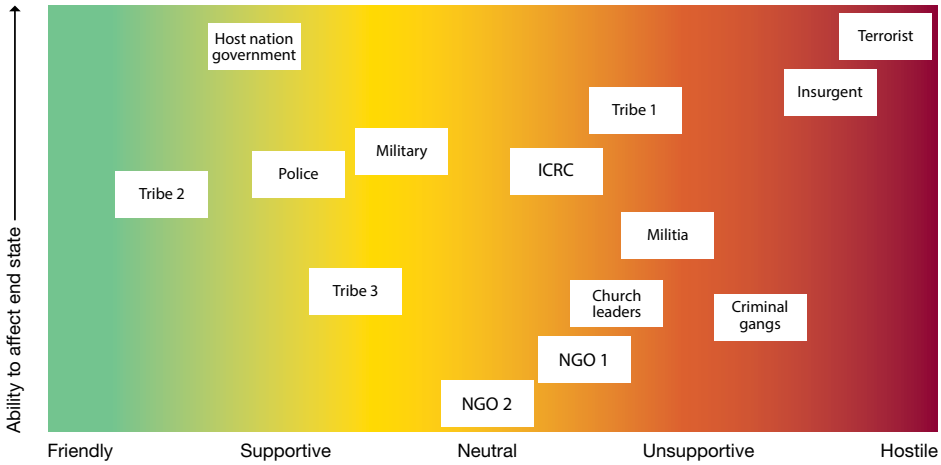


Figure 4.6 – Example audience segmentation

Audience analysis – UK fundamentals

UK 4.1. As described in Joint Tactics, Techniques and Procedures (JTTP) 3.81, *Integrated Action: An operational level guide to the audience-centric approach for commanders and staff*, Defence has defined three conceptual layers of audience analysis to support integrated action: baseline audience analysis (BAA), mission audience analysis (MAA) and target audience analysis (TAA). These layers allow for the range of insight required across the levels of operations and the difference in breadth and depth of analysis to be achieved.

UK 4.2. No one layer is exclusively aligned to support planning at the specific strategic, operational or tactical levels; it is expected that planners at different levels might have different needs for how frequently they use each layer. The layers are mutually beneficial: insights from one layer can be used to inform the assessment of other layers. The audience analysis layers can inform the assessment of operations, particularly the monitoring and evaluation activities, from the outset.

UK 4.3. **Baseline audience analysis.** BAA is defined as: the foundational level of audience analysis to support planning and inform mission and target audience analysis.[5] This is the underpinning analysis of audiences that can be used for higher-level planning (strategic or operational), further analysis and to help identify high-level metrics to use in assessment.

UK 4.4. **Mission audience analysis.** MAA is defined as: the focused understanding of target audiences in support of a mission or task to create the desired planning effect.[6] MAA provides the depth and scope of analysis required to support operational-level planning. While it is abstracted from the strategic (baseline) level analysis, it will be more specific and detailed, covering audience segments in line with the operational-level objectives. It also provides the prerequisite insight for developing TAA.

UK 4.5. **Target audience analysis.** TAA is defined as: the focused examination of targeted audiences to create desired effects.[7] This layer supports specific cognitive targeting activities and it will provide detailed information about the intended audience. When used to support the targeting cycle, the TAA will comply with a strict assurance standard. Conceptually, MAA and TAA are the most similar forms of audience analysis as they identify opportunities for creating effects. In contrast, BAA would not identify specific opportunities but inform the audience prioritisation.

5 Joint Doctrine Publication (JDP) 0-01.1, *UK Terminology Supplement to NATOTerm*.
6 JDP 0-01.1, *UK Terminology Supplement to NATOTerm*.
7 NATOTerm.

4.15 **Cognitive effect determination.** Cognitive effect determination examines the combination of the segmentation products to determine potential audiences whose behaviour could be influenced to achieve objectives. The behavioural outcomes can be added to the shade shift and will form the basis of depicting potential cognitive effects, as illustrated in Figure 4.7, to be considered by the commander. These potential cognitive effects are collated into a matrix of potential target audiences for a commander to approve and prioritize. Behaviour analysis can be supported by the psychological operations (PsyOps) staff who may provide general support to the IEA team for the behaviour analysis, which, when effects are approved, will allow for more specialized PsyOps audience analysis. PsyOps focus will initially be on information gathering using primary and secondary research data, which is then analyzed to support segmentation of audiences.

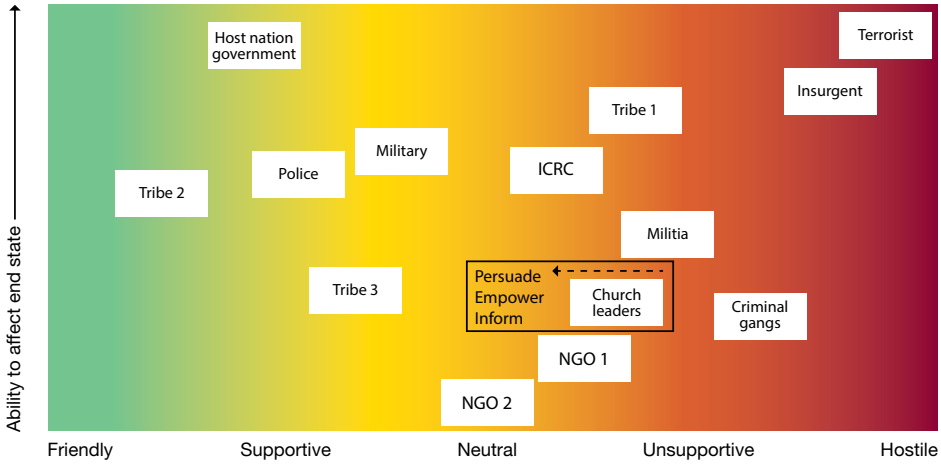


Figure 4.7 – Example potential cognitive effects

Comprehensive understanding of the operating environment

4.16 The CUOE is primarily the fusion of the IEA, the JIPOE, additional understanding and assessment from other directorates and capabilities (including external organizations), and the commander's mission analysis to enable the behaviour-centric approach. This fusion provides a commander and partners with a shared understanding of the situation to enable the determination of desired outcomes, objectives, effects and actions. The CUOE is continually updated as the situation changes, understanding deepens and assessment of activities is reported, which leads to the refinement of plans and future activities. An illustration of the CUOE is shown in Figure 4.8.

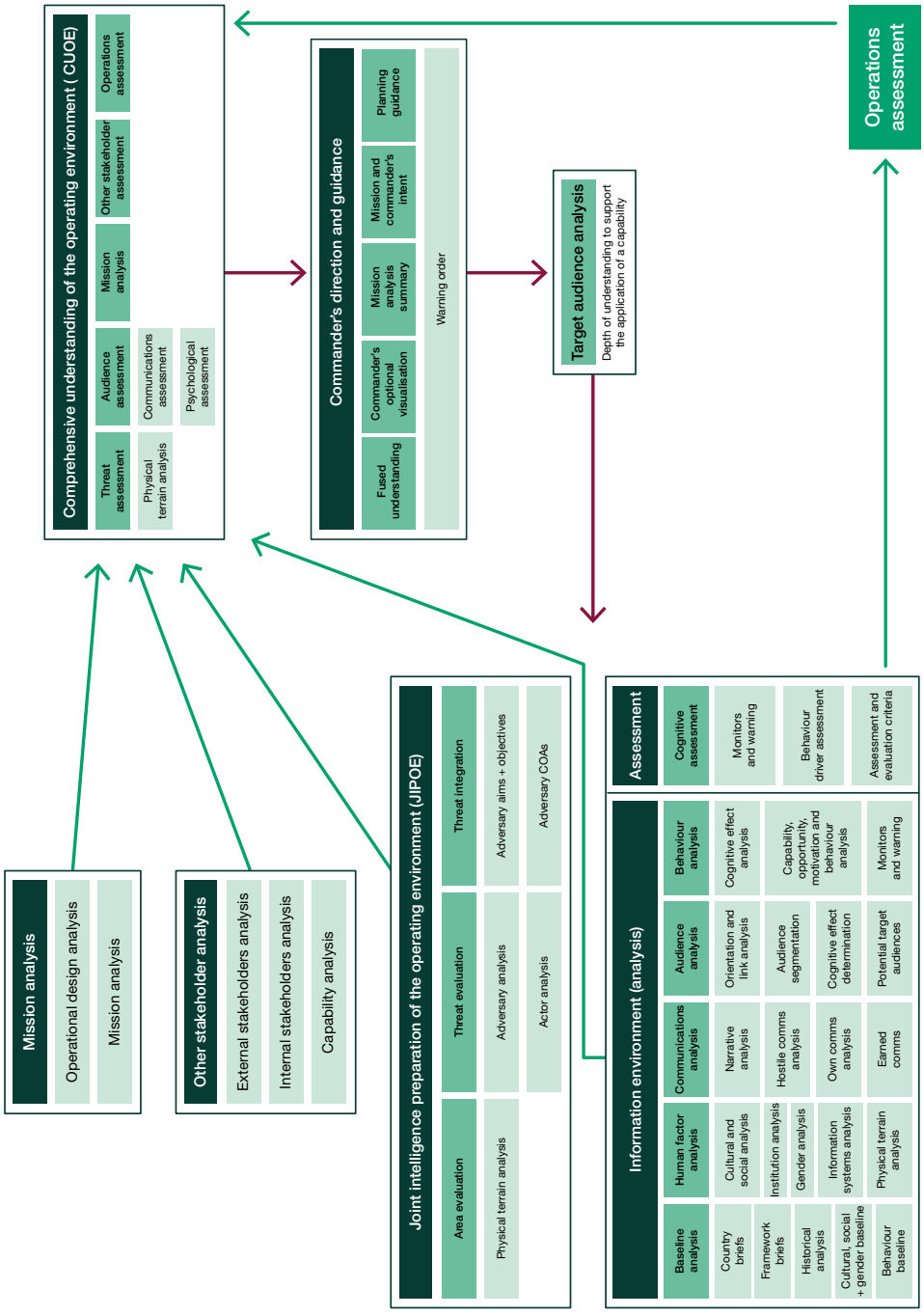


Figure 4.8 – Comprehensive understanding of the operating environment

The information environment assessment summarises the baseline, human factors, audience, communications and psychological analyses against a matrix of potential audiences

4.17 **Brief to comprehensive understanding of the operating environment.** Along with JIPOE and the commander's mission analysis, the IEA initial analysis will be presented to the commander at the CUOE. The IEA brief will be comprised of a summary of deductions from the baseline analysis, HFA, audience analysis, communications analysis and psychological analysis, presented as assessments along with the shade shift and the matrix of potential audiences to be targeted. The commander will provide direction and guidance for planning based on what is presented at the CUOE. Assessments and products from the IEA will feed almost every part of the operations planning process (OPP), which is discussed in detail in Section 2 of Chapter 4.

4.18 **Potential audiences.** A matrix will be presented to the commander to confirm priorities and to approve audiences. This matrix will recommend effects that will then be subject to detailed planning supported by target audience analysis (TAA) to enable the application of capabilities to create the effects. Figure 4.9 shows an example matrix.

Serial	Potential audience	Current situation	Audience segmentation	Recommended effect	Monitoring & evaluation	Recommended activity	Approved for TAA
Example	Blueland Mothers	Blueland is a patriarchal society but culturally children are expected to care for and provide financial assistance to their parents and family elders. Mothers wield significant influence and culturally status is derived from overtly demonstrating the ability to provide for your mother. Education and employment opportunities are limited to rural areas within Blueland, which is a substantial community. The Blueland Liberation Army (BLA) has a high proportion of child soldiers (under the age of 16).	UNSUPPORTIVE MEDIUM IMPACT Blueland mothers are supportive to the BLA as one of the few opportunities for income but are apprehensive and concerned over the dangers faced by their offspring in operative with the BLA.	Cognitive -ENCOURAGE -CONVINCE	- Increased employment opportunities - Increased presence of fighting aged males in local employment	Information Activity - ENGAGE and COMMUNICATE to build trust, highlight dangers of fighting and suggest alternative opportunities - ENCOURAGE and SUPPORT local employment initiatives	Yes
1							
2							

Figure 4.9 – Potential audiences

4.19 **Target audience analysis.** TAA is focused understanding that uses a combination of the JIPOE and IEA understanding processes. Once audiences and effects have been approved, planning will be conducted to create effects as activities or information activities. TAA will provide sufficient understanding to support the application of capabilities being planned for use in activities. Understanding can be achieved in all areas of the IEA, as well as from JIPOE, but further behaviour analysis should be conducted to support the planning of activities.

Integrated audience analysis

UK 4.6. Joint Doctrine Publication (JDP) 0-01, *UK Defence Doctrine* outlines numerous benefits of collaborating at both interdepartmental and international levels, including: sharing resources to increase the scope and depth of understanding; closer alignment of objectives; faster analysis and reaction times; and fewer frictions in how force assets are deployed and cooperate.

UK 4.7. There are limits on how much integration and sharing can be achieved due to sensitivities around data sources and the opportunity to align organisations. Collaborating on audience analysis is another way Defence can integrate with partners; sharing information and analysis will increase understanding across all parties, and so also assist integration.

UK 4.8. **Partners across government.** Within the UK government, multiple departments have an interest in their relevant audiences, generating an understanding for planning and assessment purposes. Interactions with other government departments are often managed by liaison officers who can help navigate requests and identify the best teams to engage with.

UK 4.9. **Partner nations.** As with all intelligence functions, the sharing of information can have an impact on the extent of integration the UK can achieve with allies and partners. There will be some data the UK can freely share and some that is for UK Eyes only. Equally, allies and partners may have specific data sets they can share and others they choose not to. When collaborating on audience analysis, analysts will consider where data has come from and identify potential caveats to consider (for example, the implicit influence of a nation's culture, which can affect analytical interpretations).

UK 4.10. **Industry engagement.** Many organisations in the commercial sector offer data collection, data analysis and audience analysis services. Supported by artificial intelligence applications and powerful data handling facilities, such services, if correctly used, can provide data analytics rapidly and on wide data sets, helping to accelerate Defence audience analysis.

4.20 **Behaviour analysis.** Behaviour analysis seeks to identify the behavioural vulnerabilities and opportunities of an approved target audience to support the planning of activities. It is comprised of the following processes.

a. **Cognitive effect analysis.** Cognitive effect analysis translates an operational objective into a cognitive effect using the approved target audiences to analyze a target audience, which then determines the levers for behavioural change using the social, technological, environmental, military, political, legal, economic and security (STEMPLES) brainstorming factors. Within the categories, the brainstorming identifies targetable factors which are refined to create supporting cognitive effects (SCE). These objectives can be graded and prioritized against a bespoke question set created using the criteria of criticality, accessibility, recoverability, vulnerability, effect and recognisability (CARVER) to enable comparative assessment between SCE and to understand the risks to be mitigated when planning to create these SCE. The CARVER analysis matrix[8] has been modified to enable comparative assessment of SCE. An example CARVER analysis matrix is shown at Figure 4.10.

8 The CARVER analysis matrix was developed by the United States Army special forces during the Vietnam War as a system to identify and rank targets so that resources could be efficiently used.

CARVER ANALYSIS	Question	Explanation	Score 1=Low, 5=High
Criticality	How vital is this to achieving the cognitive effect?	A supporting cognitive effect (SCE) is critical when assessed that it has a highly significant impact towards the cognitive effect.	
Accessibility	How easily can the target be reached?	An SCE is accessible when assessed that it is realistic through reasonable activity.	
Recoverability	How difficult is it to recover from this?	An SCE suggests less recoverability when assessed that it is difficult to recover from or be reversed.	
Vulnerability	How difficult is it to withstand this?	An SCE is a vulnerability when assessed that it cannot be mitigated or withstood.	
Effect	How likely is this to support the operational objectives?	An SCE has a high effect when assessed that it has a significant impact towards operational objectives.	
Recognisability	How easy is it to identify this?	An SCE is recognisable when assessed that we can identify and observe it.	
		Total	

Figure 4.10 – CARVER analysis example matrix

b. **Capability, opportunity, motivation and behaviour model analysis.** Capability, opportunity, motivation and behaviour (COM-B) is a behavioural science framework developed by University College London's Centre for Behaviour Change that is scientifically proven to be effective and used for a multitude of purposes by various organizations and agencies. COM-B provides a theoretical framework that is broken down into multiple levels, allowing for specific constructs to be identified within the target audience as an opportunity for attitude or behaviour change through information activities. The model examines the three factors that are required for any behaviour to occur, which are capability, opportunity and motivation. Capability can be psychological (knowledge) or physical (skills); opportunity can be social (societal influences) or physical (environmental resources); motivation can be automatic (emotion) or reflective (beliefs, intentions), as illustrated in Figure 4.11. The SCE, which is derived from the objective analysis, should be examined further in the COM-B model to determine the capability, motivation and opportunity for audience behaviour, which will then shape the construct of activities to counter or reinforce the behaviour.

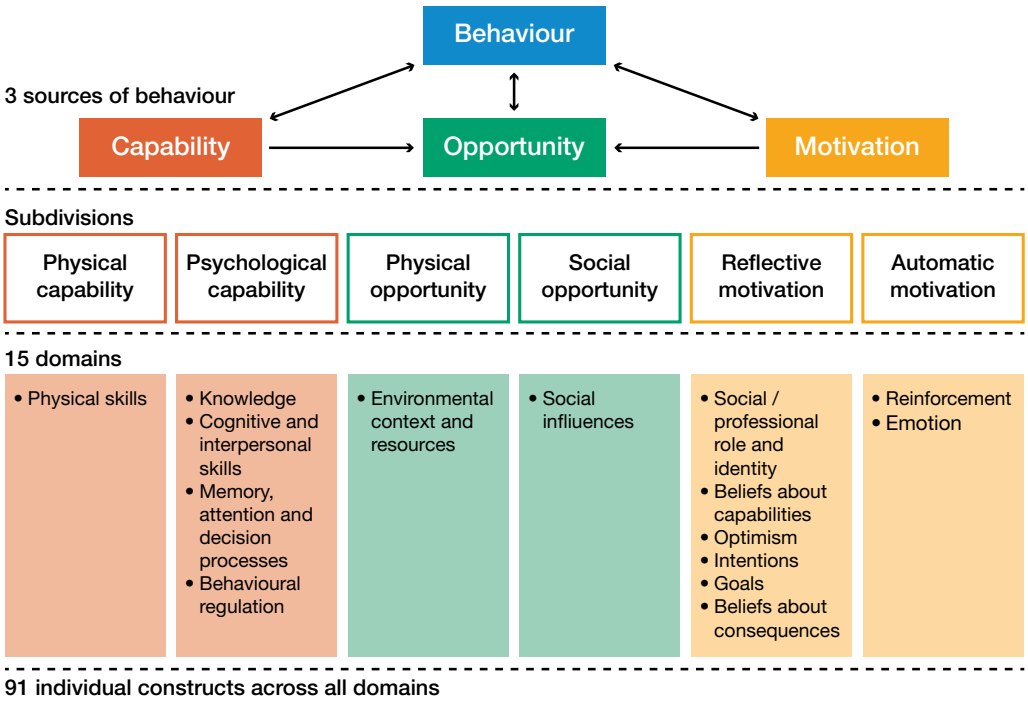


Figure 4.11 – Capability, opportunity, motivation and behaviour model

c. **Monitoring and warnings.** At this stage, a draft information decision support matrix is generated to track what an audience is saying and doing to determine the cognitive impact of military activity and then recommend further activity to reinforce or redirect behavioural change. The ability to monitor audience behaviour through triggers and warnings to confirm behaviour indicators across the multitude of information propagation means is critical and requires a detailed, planned intelligence collection plan coordinated with J2 Collection Operations Management. This stage forms the basis of the assessment planning, which is covered in detail in Section 4 of this chapter.

4.21 **Psychological operations support to target audience analysis.** The target audience is most often shaped by information derived from trustworthy sources, commonly referred to as key communicators. PsyOps provides an essential role in the shaping of these key communicators to identify behaviour drivers of audiences that could be targeted to achieve the commander's objectives. PsyOps capabilities are likely to be requested to support Info Ops in conducting the IEA to better understand behavioural dynamics of an audience.

Section 2 – Plan

4.22 **Operations planning process.** The OPP is articulated in AJP-5, *Allied Joint Doctrine for the Planning of Operations*. Info Ops staff must have a comprehensive understanding of the planning process so that they are able to contribute to it at every stage. In addition to the OPP many NATO organizations use Supreme Allied Commander Europe's (SACEUR's) ACO's *Comprehensive Operations Planning Directive* (COPD) as the primary planning process. Figure 4.12 depicts both NATO planning processes, their common outputs and the Info Ops inputs to them, which will be explained further in this section.

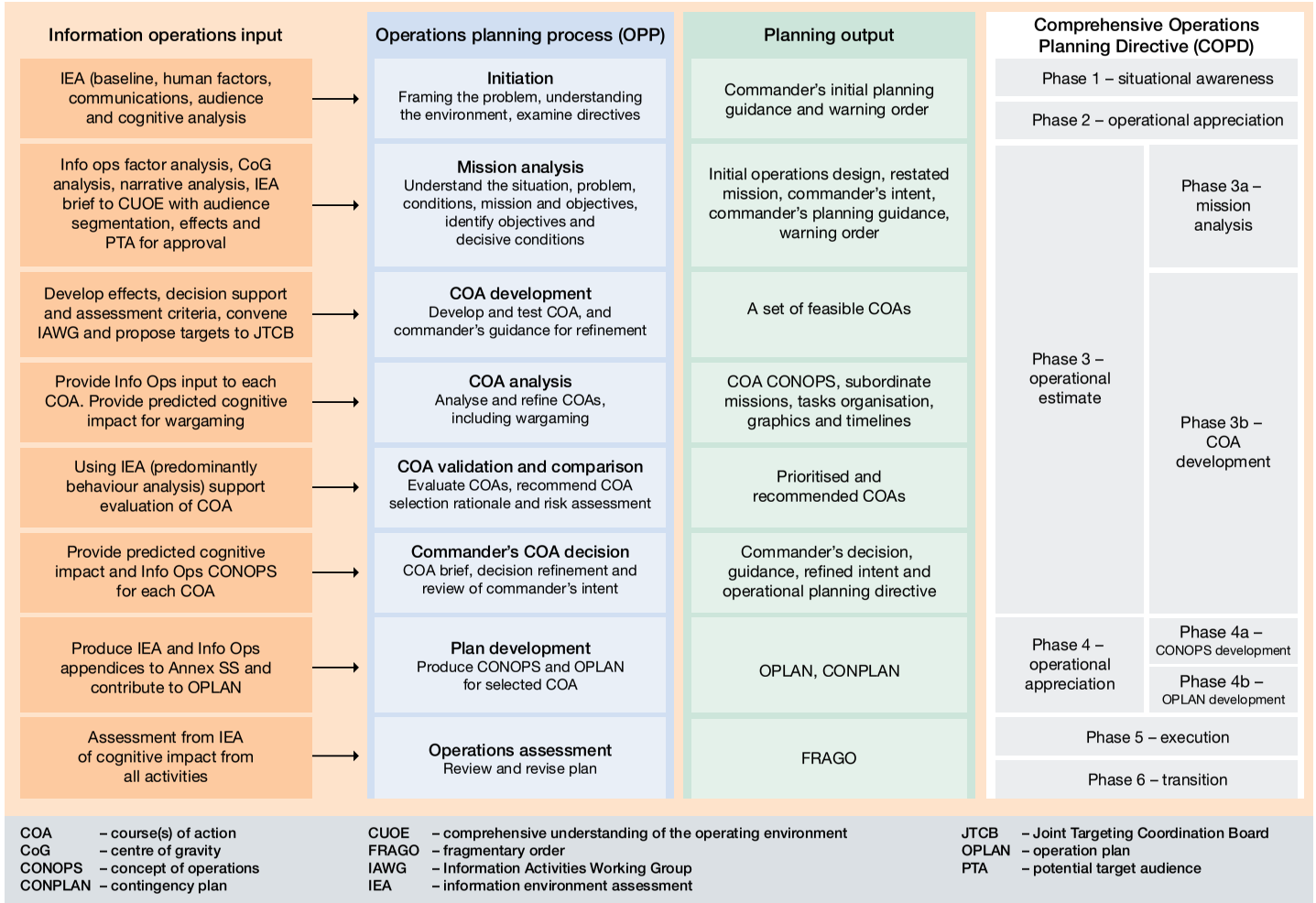


Figure 4.12 – Information operations support to the planning process

4.23 **Initiation.** Initiation is the start of the planning process that begins when directed by a higher authority through a warning order or on receipt of a higher commander's directive. The initiation planning activity is focused on framing the problem posed by understanding the operating environment, examining the political initiating directive and the higher commander's directive. The primary output of the planning process is the commander's initial planning guidance and warning order. Liaison and reconnaissance may be authorized to be conducted at this stage and Info Ops should seek to get a representative on any reconnaissance to increase understanding. Within this planning activity the Info Ops staff will contribute as follows:

- provide understanding of the narratives, audiences and the information environment through the IEA (as described in Section 1 of this chapter);
- gauge the initial scope of capabilities required for information activities and submit them to J3 for inclusion in the warning order;
- identify the information required for mission analysis and course of action (COA) development;
- identify Info Ops planning support requirements (including staff augmentation, support products and services);
- support the narrative development by constituting an ad hoc working group and identifying information requirements; and
- propose and assist in developing priority intelligence requirements (PIRs) and requests for information (RFIs), mindful of the long lead time often required to satisfy Info Ops requirements.[9]

4.24 **Mission analysis.** The purpose of mission analysis is to analyze the strategic context to precisely establish what the mission involves and where it fits into the bigger picture. It includes: analyzing the strategic intent, the outcomes sought and related strategic objectives; identifying the role of the joint force, key objectives and conditions to reach; and identifying freedoms, limitations (constraints and restraints) and assumptions that will apply, and possible changes of the situation following initiation. The main outputs of this

9 This follows the understood process of PIR and RFI development from the commander's critical information requirement (CCIR) and is conducted collaboratively with the intelligence and other staffs.

activity are the initial operations design and the planning guidance to the staff and to subordinate commands, both containing the initial commander's intent. The mission analysis comprises the following planning activities.

a. Refinement of JIPOE and IEA is continual, and understanding will deepen over time. However, a baseline understanding is required to conduct the mission analysis that will be enhanced when the CUOE fuses the mission analysis, JIPOE, IEA and additional understanding and assessment from other directorates and capabilities (including external organizations).

b. A strategic context review will examine superior authority directives to determine their role in supporting the commander's intent as well as NATO's objectives. This analysis will identify and examine other stakeholders and their objectives that will require supporting and will contribute to attaining the end state.

c. Factor analysis will examine specific aspects, facts or conditions in the operating environment to determine their impact on operational success to enable a commander to identify areas for clarification, constraints, assumptions and specified and implied tasks. This analysis is normally presented in a table by factor with a deduction and conclusion being articulated.

d. Analysis of the higher commander's intent and the given mission and tasks will enable the commander to understand, visualize, describe and direct the operation. At this stage the commander will begin to determine the effects they wish to create using the effect dimensions in the targeting framework that were described in Chapter 1. Info Ops staff should advise the commander on effects verbs and what they mean from an Info Ops perspective using the list at Annex A. The criteria for success should be identified, which will begin the assessment process and is covered in detail within Section 4 of this chapter.

e. The CUOE, which is presented during the mission analysis planning activity, will enable factor analysis and centre of gravity identification and analysis. This analysis technique is explained in detail in AJP-5, *Allied Joint Doctrine for the Planning of Operations* and will explore an actor in detail to identify their critical capabilities, requirements and vulnerabilities, which then enable the planning process for COA development and selection.

f. The Info Ops staff will contribute to all aspects of the commander's mission analysis to determine specified and implied tasks, and freedoms and constraints that will focus future planning activities. Some specific areas to be examined and determined by Info Ops staff, supported by a legal advisor and other functional area experts, during the mission analysis planning activity are as follows.

- Political, legal and rules of engagement implications regarding international law, custom and practice, host nation agreements and/or arrangements.

- Social and cultural attitudes that will limit or increase information activity options will feed into narrative understanding and lead to development of rules of behaviour (for example, Alliance or coalition sensitivities or ethnic, cultural and religious issues, and constraints imposed on the activities of the force to deny information to an adversary).

- Proposed information requirements and commander's critical information requirements (CCIRs).

- An initial Info Ops risk assessment including reviewing operations security (OPSEC) considerations and potential essential elements of friendly information (EEFI).

- The IEA initial analysis including an initial narrative landscape will be presented to the commander through the CUOE and comprises a summary of deductions from the background analysis, HFA, communications analysis, audience analysis and cognitive analysis presented as assessments along with the shade shift and potential target audiences.

4.25 **Commander's planning guidance.** Following on from the mission analysis, the commander will deliver their planning guidance to the headquarters staff and to subordinate commanders. The format and detail within this brief will vary depending on the situation and time available but the following key areas will be covered:

- a summary of the JIPOE and IEA assessments from the CUOE;
- commander's visualization of the operation;
- a summary of the mission analysis;

- mission, narrative and commander's intent;
- planning guidance for COA development; and
- warning order to subordinate commanders.

4.26 **Course of action development.** This planning activity takes the outputs from mission analysis, such as initial estimates, missions, tasks and planning guidance from the commander, to develop and subsequently test several potential COAs. Info Ops staff refine the Info Ops contribution to the staff estimate, as well as:

- refining desired and undesired effects in the information environment that support or degrade the joint force commander's objectives and decisive conditions;
- developing measures of effectiveness (MOEs) and their indicators;
- developing information activities tasks and related capabilities for recommending to J3/J35/J5 to include in the plan;
- recommending and synchronizing which information activities may be used to accomplish those recommended actions for each COA;
- supporting the development of micro narratives if required;
- synchronizing information activities within each COA;
- continuing to develop the Info Ops element of the staff estimate, inputs for the COA brief and inputs for target sets; and
- establishing the Information Activities Working Group (IAWG) and working group and, in coordination with the Joint Effects Branch, identify potential target sets ready for submission to the Joint Targeting Coordination Board (JTCB). The IAWG is explained in more detail in Section 3 of this chapter.

4.27 **Course of action analysis.** During this planning activity the potential COAs are refined and analyzed to develop a series of options that are derived from a logical cross functional process. This part of OPP will deliver a preliminary concept of operations (CONOPS), including missions and tasks, task organization and draft timelines. These are analyzed against several criteria, including troops to task and logistic feasibility. This process could

involve the use of wargaming where Info Ops staff should provide a prediction of the likely cognitive effect of all activities (including the narrative) being wargamed. Info Ops will:

- analyze each COA from a functional Info Ops perspective focusing on narratives;
- identify decision points for employing information activities;
- recommend adjustments for information activities tasking as appropriate;
- provide Info Ops input into synchronization matrices or other decision making tools;
- identify the Info Ops contribution to any branch or sequel plans;
- identify any high pay-off targets in the information environment; and
- submit and recommend CCIR for Info Ops.

4.28 **Courses of action validation and comparison.** This planning activity validates and compares the COAs to enable a commander to select the most appropriate criteria or direct further refinement. Evaluated criteria, wargaming results and general assessment enable the staff to generate a list of evaluated COAs, recommend a COA and give their reasoning behind the recommendation. Info Ops staff will:

- compare each COA based on missions and tasks, taking into account the different narratives;
- compare each COA in relation to the Info Ops requirements against available information activities;
- prioritize COAs from an Info Ops perspective; and
- revise the Info Ops input to the staff estimate.

4.29 **Course of action decision.** The commander will select the most appropriate COA or direct further refinement. During the decision brief Info Ops staff must provide the commander with a recommendation of how

information activities can best contribute to mission success in each of the COAs briefed. These recommendations must be clear and concise and related to own and opposing narratives. They must be easily understood at all levels of command and enable translation of the COA into the CONOPS and operation plan (OPLAN). Once a COA is selected, the planning team will refine the COA, leading to a refined intent, which includes:

- an agreed purpose;
- a main effort; and
- how the entire operation or major operation will achieve the operational-level objectives and contribute to achieving the military strategic objectives.

4.30 **Plan development.** The purpose of this planning activity is to produce a coherent CONOPS and an OPLAN. The CONOPS clearly and concisely expresses what the commander intends to accomplish and how it will be done with the available resources. SACEUR's ACO's COPD provides guidance on operational staff work. The narrative and the StratCom CONOPS is provided in the main body of the OPLAN and Annex SS is allocated to allow StratCom direction and guidance to be articulated in detail, including tasks for capabilities. Within Annex SS there are four appendices, which are as follows.

a. **Appendix 1 – Information Environment Assessment.** This appendix provides further detail on the audience analysis and deductions from the IEA. The suggested structure of this appendix is at Annex B of this publication.

b. **Appendix 2 – Information Operations.** This appendix provides specific detail on the integration of information activities, the engagement plan and the assessment plan. The structure and guidance for this appendix is at Annex B of this publication.

c. **Appendix 3 – Military Public Affairs.** This appendix provides the Mil PA plan and its structure will be covered in AJP-10.X, *Allied Joint Doctrine for Military Public Affairs*.

d. **Appendix 4 – Psychological Operations.** This appendix provides the PsyOps plan and its structure is covered in AJP-3.10.1, *Allied Joint Doctrine for Psychological Operations*.

The information environment assessment seeks to identify and measure the cognitive impact of activities against the audience baseline

4.31 **Operations assessment.** Operations assessment is described by NATO as the process of determining the results and progress of operations towards mission accomplishment, and the subsequent development and provision of conclusions and recommendations that support decision-making and improve the effectiveness of operations. Operations assessment is a continuous, collaborative and cross-functional process led by dedicated operations assessment staff. Info Ops will support the operations assessment through the IEA, which will seek to identify and measure the cognitive impact of activities against the audience baseline. This assessment is fed into operational assessment process as described in AJP-3, *Allied Joint Doctrine for the Conduct of Operations*. Throughout the planning process, the Info Ops staff will continue to conduct assessment focused on the information environment and contribute to the refinement or adjustment of the OPLAN.

Section 3 – Integrate

4.32 Integration is at the heart of Info Ops as every action will have a resultant cognitive effect. Therefore, Info Ops staff must ensure they are fully integrated across the headquarters and attend all the battle rhythm forums, as described in Chapter 3.

4.33 **Information Activities Working Group.** The IAWG is the forum for the coordination of information activities within an operational-level headquarters. This working group is chaired by Director Communications Division (Dir ComDiv) or Chief Info Ops. It meets as a subset and to prepare either the IACB, if held, or more likely the Strategic Communications Coordination Board (SCCB).

a. **Role and responsibilities.** The IAWG ensures that information activities are coherent and synchronized with the cognitive line of effort and other activities in the engagement space. The IAWG will approve the input from Info Ops staff to the planning process and will coordinate target nominations related to information and information systems to facilitate subsequent harmonization at the JTCB[10] and provide advice on possible effects in the information environment created by other military activities. The responsibilities of the IAWG are:

- presenting the analysis of the information environment through the IEA;
- developing plans for information activities in line with the commander's direction and guidance;
- assessing the predicted cognitive impact of all planned activities and determining if additional information activities could be conducted to support or mitigate effects;
- identifying the resources and requirements, staff actions and coordination to support the delivery of information activities;
- developing and monitoring assessment criteria to contribute to operations assessment;
- manage and approve the engagement plan, information activities synchronization matrix and assessment plan;
- reviewing and approving the Info Ops inputs to the planning process and operational staff work;
- developing target nominations for submission to the JTCB;

10 More detail on the JTCB is contained in AJP-3.9, *Allied Joint Doctrine for Joint Targeting*.

- coordinating with external stakeholders and consulting with other staff directorates as required; and

- providing StratCom guidance and direction to the headquarters.

b. **Participation.** Composition of the IAWG will be detailed in the Info Ops Appendix of the OPLAN (Appendix 2 to Annex SS), the IAWG Chair may direct participation as required. Attendance should include a representative from all staff directorates, principal advisors, representation from capabilities being considered for information activities and an Info Ops representative from subordinate headquarters. In some cases, external non-military organizations could be invited depending on the type of operation being conducted. As a battle rhythm event, efforts should be made to deconflict the IAWG from other events to enable appropriate participation. Representatives on the IAWG must have the authority to speak for, and make decisions on behalf of, their staff directorate.

4.34 **Joint targeting.** Joint targeting is an integration function that requires participation from the strategic and operational levels, all joint force staff directorates and component commands. It will also coordinate with various non-military audiences as part of NATO's comprehensive approach. Info Ops staff will develop target materials for information activities, which will be validated, approved and prioritized through the joint targeting process for resource allocation and effects employment. The IACB and JTCB are closely aligned and fuse activities between them prior to submission to the Joint Coordination Board or delegated targeting approval authority. A suitably trained, experienced and qualified targeting officer should be employed within the J10-Strategic Communications directorate (J10-StratCom) develop target packs and guide them through the process. Target development by Info Ops staff should be done in close coordination with NATO's Centralized Targeting Capacity to avoid duplication of effort and ensure that target development efforts across NATO are mutually supporting and prioritized. Further information on the targeting process can be found in AJP-3.9, *Allied Joint Doctrine for Joint Targeting*.

4.35 **Collateral damage considerations.** As part of the joint targeting process a commander will decide if any expected collateral damage resulting from targeting would be excessive or not, in relation to the military advantage offered by the engagement of each target and must take all feasible precautions to avoid it. The collateral damage methodology is explained in

AJP-3.9, *Allied Joint Doctrine for Joint Targeting* but it is not designed to be used for information activities. In addition to the predicted cognitive impact, Info Ops staff will predict the virtual and physical impact of information activities as collateral damage to be expressed at the JTCB before approval can be given.

4.36 **Joint effects.** Supreme Headquarters Allied Powers Europe's (SHAPE's) Joint Effects Branch manages, integrates and synchronizes targeting effects within the engagement space. This process integrates all targets developed at the operational level within a joint prioritized target list (JPTL). The target nominated and developed by Info Ops staff will be integrated through the appropriate working groups and target coordination boards.

4.37 **Execution.** The integration aspect of Info Ops execution requires dedicated Info Ops staff to be integrated alongside the capability liaison officers in the operations centre within a headquarters. This ensures that plans are executed as intended, that guidance on mission execution can be provided, and assessment of activities can be fed into the IEA for analysis.

Section 4 – Assess

4.38 **Assessment.** Assessment seeks to analyze and report on the performance and effectiveness of information activities to provide feedback to decision-makers so that information activities can be modified where necessary to achieve the desired results. Because there is always a delay between cause and effect of information activities, assessment is not immediate. Access to audiences being affected is not always possible but Info Ops staff should identify indicators and warnings for information activities to predict and observe behavioural changes over time.

4.39 **Criteria.** Assessment criteria should use the specific, measurable, achievable, realistic and time-bound (SMART) objectives approach and be designed from the outset. Assessment is best derived from a combination of criteria using both quantitative (usually measures of observable behaviour) and qualitative (usually indicators of attitudinal change) data, including disaggregated data (such as gender and age), to better represent and enable more comprehensive analysis of the data. Given the complexity of assessing information activities, additional criteria have been designed to determine the cumulative effect of an activity over time. Figure 4.13 shows these different

assessment criteria, which are combined to enable the IEA staff to contribute to the operations assessment on the cognitive effect of activities.

a. **Measure of activity.** This is a criterion to record what happened. It is a simple metric that determines the volume of activity. For example, if an information activity included distribution of leaflets, then measure of activity (MOA) could be: how many leaflets were produced; how many were distributed; and where and when were they distributed? This data provides an activity baseline which will be assessed by other criteria, thereby enabling decisions about more effective quantities, which will contribute to the planning of subsequent activities.

b. **Measure of performance.** This is a criterion to evaluate the accomplishment of own force actions. The measure of performance (MOP) enables the measurement of progress, intending to answer the question: are the actions being executed as planned and is a criterion used to assess task accomplishment? For example, 'we produced and disseminated 500/500 leaflets aimed at an approved audience'.

c. **Measure of effectiveness.** This is a criterion used to assess changes in system behaviour, capability or operating environment that is tied to measuring the attainment of an end state, achieving an objective or creating an effect. MOE can be used to assess the realization of specified effects. It considers what effects, both intended and unintended, have been created through the performance and activities of the force against audiences. MOE is used to monitor progress, highlight negative consequences and to support current and future planning. The key question that MOE endeavours to answer is whether the action achieved its stated purpose with the planned activities and the allotted capabilities.

d. **Measure of success.** This is a high-level assessment of mission success against the prescribed objectives and end state. Measure of success (MOS) is primarily a subjective assessment but is supported by objective metrics. MOS will be used in a commander's reporting to a higher headquarters and will summarize activities and atmospherics, highlight risks and issues, and report progress on accomplishing the mission and end state.

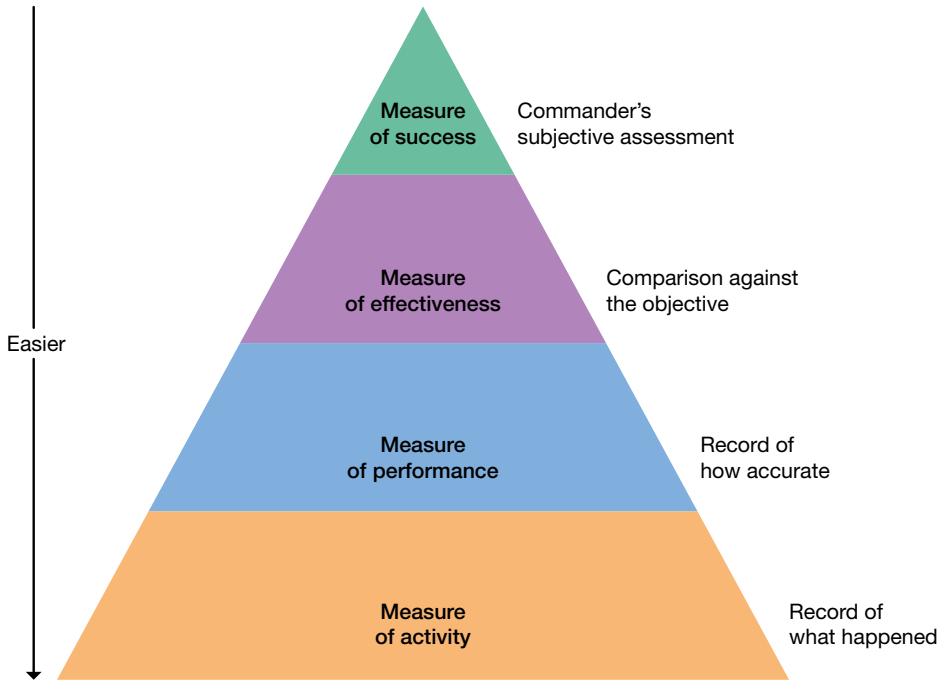


Figure 4.13 – Assessment

UK assessment frameworks and metrics

UK 4.11. The assessment framework for monitoring and evaluating the campaign is part of the Chief of the Defence Staff directive. It defines the assessment criteria to be applied at each level.

UK 4.12. At the campaign level, metrics should be thematic and reflect the multiple behaviours and attitudes that could be expected. This can be achieved through developing a theory of change and scrutinising how activity outputs contribute to outcomes and longer-term change in audiences. Metrics will be used to monitor audiences and to predict expected consequences. The theory of change will indicate how the outcome is planned as a result of the full sequence of activities and their consequences. The stages for developing the assessment framework are as follows.

- Use the military strategic objectives to define the observable behaviours that will be representative of the final outcome/ desired end state.

- Depending on the activity level, use a theory of change or develop it further to identify all associated metrics.
- Identify metrics for each outcome – consider the full range of available sources, as well as sources identified within the audience analysis and the broader understand function.
- Establish routes to access data for metrics – this could include setting requests for information and audience analysis tasking.

4.40 **Milestones.** Independent of the assessment criteria, Info Ops staff will develop a series of intermediate objectives, known as milestones, which are tangible and measurable. These milestones serve to provide a qualitive look at each step in a messaging programme to determine if the factors required are being met before moving to the next stage. For example, a new radio advertisement must be preceded by determining market reach and audience consumption. If those factors are not acceptable, precursor activities would include events and activities to improve broadcast coverage and actual listenership. Moving onward to the messaging series would only happen after the first milestone has been met.

4.41 **Process.** Assessment is a continual process that provides the commander with the data and analysis to support decision-making. The IEA focuses assessment on the audience to determine the behavioural changes as well as changes in narratives from the established baseline reported in the initial CUOE. This will feed into the operations assessment, which is normally led by the J5 directorate as detailed within AJP-3, *Allied Joint Doctrine for the Conduct of Operations*. Further detail can be found in the *NATO Operations Assessment Handbook*. The process for assessment is illustrated in Figure 4.14 and summarized below.

a. **Planning.** Assessment is integrated into all phases of the planning and execution processes. A well-crafted plan is useless unless its progress can be measured in a relevant way to allow a commander to understand if their actions are creating the effects required to achieve the objective.

b. **Activity.** All planned activities must stipulate the assessment criteria using SMART objectives to determine the desired outcome

of the activity. Monitoring and warning requirements need to be identified and resourced to enable collection of data to be analyzed for assessment.

c. **Data collection.** Data[11] can be processed by humans or by automated means. All activities conducted must include a comprehensive data collection plan gathering disaggregated data to assist with assessment, which can be augmented by numerous other data collection activities. The requirement and types of data to be collected must be determined in the planning process and be articulated in the operational staff work. Data collection can be immediate or longer term and will be achieved by a combination of methods such as: interviews, focus groups, surveys, digital surveys, post activity reports and media report analysis. Data is categorized into the following categories.

- **Quantitative** – a number that represents an amount or count.
- **Qualitative** – an observation that is a word, sentence, description or code. This data is collected using questionnaires, interviews or observations and usually appears in the narrative form.
- **Objective** – facts and the precise measurement of things.
- **Subjective** – resulting from an individual's opinion, experience or judgement.

d. **Analysis.** Collected data must be analyzed so that valid conclusions can be drawn about the metrics. Changes in these metrics must then be analyzed in aggregate to determine progress towards individual effects or directly towards objectives. Disaggregated data should be analyzed whenever possible because it can identify trends that might be symptoms of a deteriorating security situation, serve as early warning indicators and help build a knowledge base about evolving dynamics within local populations. The analysis of metrics should form the main body of evidence brought forward to the final assessment. Essential to analysis is a baseline against which to compare data deductions against. The IEA initial brief to the CUOE

11 Data is defined as: 'a reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.' (NATO Adopted)

should be regarded as the narrative and audience baseline against which assessment will track and measure behavioural change.

e. **Assessment.** In preparing the assessment, analyzed data is synthesized with other material, such as expert opinion, commentary and the data baseline. This assessment is presented to the commander and other stakeholders so they can gain appropriate understanding of the current situation and make recommendations for future action.

f. **Decision.** The commander will decide, based on the presentation of the assessment, what further direction and planning guidance is required. This direction and guidance will lead to a refinement of the operational staff work once it has been through the planning process. The commander will use the outcome of these assessments to shape reporting to higher headquarters and use as evidence for further engagements.

Figure 4.14 – Information environment assessment process

Key points

- There are four components of the Info Ops staff function: analyse, plan, integrate and assess.
- The IEA is the primary tool for understanding and assessment of audiences.
- The information environment is segmented into three dimensions: cognitive, physical and virtual.
- The cognitive dimension is the decisive dimension because it is where effects on individuals' thinking are created, thereby driving their behaviours and decisions. All actions in other dimensions ultimately affect the cognitive dimension.
- Assessment seeks to analyse and report on the performance and effectiveness of information activities so that plans can be modified where necessary to achieve the desired results.

Notes

Annex A

Effect, task and action verbs

A.1 Effect, task and action verbs are used to describe the desired effects of activities. Information operations (Info Ops) staff will advise the commander and planning staff of the planned or predicted resultant cognitive effect of all activities. The following list of verbs should be used, which are predominately sourced from the *Concise Oxford English Dictionary* (COED) but in some cases are elaborated to describe what the definition means from an Info Ops perspective.

advocate
A person who publicly supports or recommends a particular cause or policy. (COED)

advocate

(verb) Publicly recommend or support. (COED)

amplify
Make (a statement) more detailed. (COED)

assess
Evaluate or estimate the nature, value, or quality of. (COED)

assure
Tell someone something positively in order to dispel potential doubts. (COED)

broadcast
Transmit by radio or television. (COED)

channel
Direct towards a particular end. (COED)

coerce
Persuade (an unwilling person) to do something by using force or threats. (COED)

collect
Bring or gather together (COED)
From an Info Ops perspective, this refers to the collection of information.

communicate
Share or exchange information or ideas. (COED)

compel
Force or oblige to do something. (COED)

confuse
Make (someone) bewildered or perplexed. (COED)

contain
To restrict an entity's freedom of movement to within a specified area. (NATO Agreed)
From an Info Ops perspective, this refers to restraining the spread of information, a message, or an effect in a media source or audience, or on an information system.

convince
Cause to believe firmly in the truth of something. (COED)

co-opt
Divert to a role different from the usual or original one. (COED)
From an Info Ops perspective, this refers to convincing the target to agree to a specific action and/or agreement of your choosing.

corrupt
Made unreliable by errors or alterations. (COED)

deceive
To mislead an entity by manipulating its perceptions in order to induce it to react in a manner prejudicial to its interests. (NATO Agreed)
From an Info Ops perspective, this refers to the military activity of deception.

degrade
Cause to suffer a severe loss of dignity or respect; demean. (COED)
From an Info Ops perspective, this refers to adversary command and control or communications systems, and information collection efforts or means. It also refers to morale, worth or the effectiveness of adversary decisions and actions. Damage is done to the entity, which continues to operate but at a reduced effectiveness or efficiency.

deny
To prevent an entity from using specified people, space or infrastructure. (NATO Agreed)
From an Info Ops perspective, this means preventing someone from accessing and using critical information, systems and services.

demonstrate
To dissuade a hostile entity by a show of force, without seeking contact. (NATO Agreed)

destroy
To damage a target to such an extent that it is unable to fulfil its intended function without being reconstituted or entirely rebuilt. (NATO Agreed)
From an Info Ops perspective, this refers to physically damaging an enemy system, or entity, so badly that it cannot perform its function, create a psychological effect or reduce adversary command and control capability.

detect
Discover or identify the presence or existence of. (COED)
From an Info Ops perspective, this includes hostile information and disinformation, entities on social media or intrusions into information systems.

deter
Discourage (someone) from doing something by instilling fear of the consequences. (COED)

diminish
Make or become less. (COED)
From an Info Ops perspective, this includes the will, understanding or capability of an actor.

discourage
Cause (someone) to lose confidence or enthusiasm. (COED)

discredit
Harm the good reputation of. (COED)
From an Info Ops perspective, this includes the reputation, credibility and authority of an actor.

disrupt
Disturb or interrupt. (COED)
From an Info Ops perspective, this applies to using capabilities to interrupt information flow (denial of service attacks, electromagnetic warfare, destruction of broadcast facilities and command and control capability).

disseminate
Spread widely. (COED)

dissuade
Persuade someone not to take (a course of action). (COED)

distort
Give a misleading or false account or impression of. (COED)

distribute
Be spread over or throughout an area. (COED)

embolden
Give courage or confidence to. (COED)

empower
Give authority or power to; authorize. (COED)
From an Info Ops perspective, this means using information to promote confidence, authority, accountability and responsibility in an actor or group.

encourage
Give support, confidence or hope to. (COED)

establish
Achieve permanent acceptance or recognition for. (COED)

exploit
Make use of and derive benefit from (a resource). (COED)
From an Info Ops perspective, this means using information to take advantage of, or create, a favourable situation for tactical, operational or strategic purposes.

expose
Make (something) visible by uncovering it. (COED)
From an Info Ops perspective, this means revealing information that offers an advantage to the Alliance.

facilitate
Make easy or easier. (COED)

impose
1. Force to be accepted, done, or complied with.
2. Take advantage of someone. (COED)

indicate
1. Point out; show.
2. Suggest as a desirable or necessary course of action. (COED)

influence
The capacity to have an effect on the character or behaviour of someone or something, or the effect itself. (COED)
From an Info Ops perspective, influence is an outcome and refers to effects on the attitudes and behaviours of an audience. It may be achieved deliberately by communication and information activities, or as a resultant cognitive effect of all activities.

inform
Give information to. (COED)

isolate
Place apart or alone; cut off. (COED)

manipulate
Control or influence cleverly or unscrupulously. (COED)
From an Info Ops perspective, this means managing an actor to create friendly advantage, often through persuasion or deception.

mask
A disguise or pretence. (COED)
From an Info Ops perspective, this means protecting information from individuals or groups until an appropriate moment for its release. This applies particularly to operations security and deception.

misinform
Give false or inaccurate information to. (COED)

mislead
Cause to have a wrong impression about someone or something. (COED)

negate
Nullify; make ineffective. (COED)
From an Info Ops perspective, this means countering the effects of adversary information activities or the information itself. It is particularly applicable to counter hostile information, disinformation and operations security.

neutralize
To render a hostile entity or materiel temporarily incapable of interfering with friendly forces. (NATO Agreed)
From an Info Ops perspective, this means countering the source of information rather than the effect. For example, by denial of service, electromagnetic warfare or physical action.

persuade
Cause someone to do something through reasoning or argument. (COED)

prevent
Keep from happening or arising. (COED)
From an Info Ops perspective, this means persuading an actor not to undertake a course of action by convincing them that it will be unsuccessful. It is less reliant on physical force than coercion.

probe
Enquire into closely. (COED)
From an Info Ops perspective, this means to closely examine, evaluate and test a system or entity (human or technological) to gain an understanding of its general layout or perception.

promote
Further the progress of; support or encourage. (COED)
From an Info Ops perspective, this means to advocate or advance positive awareness of an actor, organization or courses of action.

protect
Keep safe from harm or injury. (COED)
From an Info Ops perspective, this means protecting the joint force commander's freedom to operate in the information environment.

publicize
Make widely known. (COED)

reassure
Allay the doubts and fears of. (COED)
From an Info Ops perspective, this means restoring confidence and dispelling fear through coordinated use of psychological operations, key leader engagement and presence, posture and profile measures.

reinforce
Strengthen or support; give added strength to. (COED)
From an Info Ops perspective, this means using information to maintain and increase support for specific ideas, actors, organizations or activities.

reveal
Disclose (previously unknown or secret information). (COED)

sever
Put an end to (a connection or relationship). (COED)

shape
Develop in a particular way. (COED)
From an Info Ops perspective, this means preparatory work focused on actors' behaviours to cause them to conform to a particular pattern, prior to subsequent activities conducted by NATO forces.

support
Assistance, encouragement, or approval. (COED)

undermine
Make less powerful or effective, especially in a gradual or insidious way. (COED)
From an Info Ops perspective, this refers to an actor's trust, credibility and loyalty by damaging reputation.

understand
Perceive the intended meaning of (words, a speaker or a language). (COED)

unmask
Expose the true character of. (COED)

usurp
Take (a position of power) illegally or by force. (COED)
From an Info Ops perspective, this means establishing a position of authority within the operating environment that means our ideas and arguments supplant those of our adversaries.

Annex B

Information operations operational staff work templates

B.1 Supreme Allied Commander Europe's (SACEUR's) Allied Command Operations' (ACO's) *Comprehensive Operations Planning Directive* (COPD) provides guidance on operational staff work. The narrative and the strategic communications (StratCom) concept of operations is provided in the main body of the operation plan (OPLAN) and Annex SS is allocated to allow StratCom direction and guidance to be articulated in detail, including tasks for capabilities. Within Annex SS there are four appendices, which are as follows.

a. Appendix 1 – Information Environment Assessment. This appendix provides further detail on the audience analysis and deductions from the information environment assessment (IEA).

b. Appendix 2 – Information Operations. This appendix provides specific detail on the integration of information activities, the engagement plan and the assessment plan.

c. Appendix 3 – Military Public Affairs. This appendix provides the military public affairs (Mil PA) plan and its structure will be covered in Allied Joint Publication (AJP)-10.X, *Allied Joint Doctrine for Military Public Affairs*.

d. Appendix 4 – Psychological Operations. This appendix provides the psychological operations plan and its structure is covered in AJP-3.10.1, *Allied Joint Doctrine for Psychological Operations*.

B.2 Information operations (Info Ops) staff are responsible for producing the supporting appendices for Annex SS using the suggested templates in this annex.

Appendix templates

B.3 Appendix 1 should seek to provide a summary of assessment from the IEA to support the OPLAN. Appendix 2 should seek to provide specific detail on the integration of information activities, the engagement plan and the assessment plan. Suggested layouts for these appendices are as follows.

APPENDIX 1 TO
ANNEX SS TO
OPLAN xxxx
TITLE xxxx
DATED dd mm yyyy

INFORMATION ENVIRONMENT ASSESSMENT

1. **Background.** An introduction to the IEA and the framework within which the analysis resides.

2. **Baseline analysis.** A summary of the baseline analysis using country and framework briefs, operational lessons, historical, cultural, social and gender analysis. This section may contain hyperlinks to open-source documents and is designed to signpost to research.

3. **Human factor analysis.** A summary of the key deductions of the human factors analysis which is often displayed using the PMESII/ASCOPE analysis tool as shown below.

	Political	Military	Economic	Social	Infrastructure	Information
Area						
Structures						
Capability						
Organization						
People						
Events						

4. **Communications analysis.** A summary of the narrative analysis of actors within the engagement space and the communications assessment focused on hostile, own and earned communications.

a. **Narratives and message analysis.** An analysis of narratives and recent messages of all of those in the actor category of audience segmentation provides the foundation for communications analysis. Determining which organizations could influence our objectives and understanding their narratives provides an excellent tool to build our information activities planning upon.

b. **Network analysis.** An analysis of how information is communicated in the engagement space to determine the tools and channels available. This

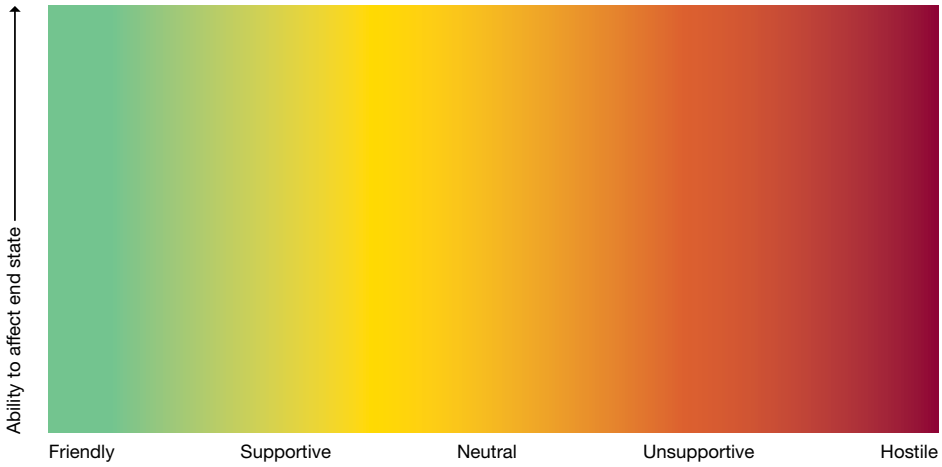
assessment could include radio, mobile phone and data coverage as well as the most used Internet and media outlets.

c. **Hostile communications.** An assessment of the capability of adversary communications, including how potential or existing adversaries communicate against key or the most vulnerable audiences/ stakeholders.

d. **Own communications.** An assessment of the effectiveness of NATO's communications to identify and assess the audiences targeted and reached, communications strategies and campaigns, themes, topics and the communication channels and means used to communicate.

e. **Earned communications.** An assessment of earned communications by third parties or international media outlets about a topic or organization that has not been generated by NATO or an affiliated party and over which NATO does not have any control. Earned communications develops an understanding of the issues that relate to NATO in the information environment but are not necessarily driven by NATO messaging and therefore impact how NATO is perceived by NATO's key audiences.

5. **Audience analysis.** Using a shade shift (suggested template below), outline the segmentation of audiences in the engagement space which will provide the audience baseline.



APPENDIX 2 TO
ANNEX SS TO
OPLAN xxxx
TITLE xxxx
DATED dd mm yyyy

INFORMATION OPERATIONS

References:

1. (xx)[12] SITUATION.

   a. **General.** See main text.

   b. **Specific.**

      (1) **Information environment.** Summary of mission-relevant aspects of the information environment, taken from the staff estimate, which is supported by the information environment assessment.

      (2) **Strategic communications framework.** Summary of mission-specific StratCom guidance on information activities (narrative, core message, StratCom/cognitive effects, themes and messages, focus topics).

      (3) **Own information activities.** Summary of the status of own narrative and information activities, taken from the staff estimate, which is supported by the IEA.

      (4) **Adversary narrative and information activities.** Summary of the status of adversary narrative and information activities, taken from the staff estimate, which is supported by the IEA.

      (5) **Other actors' narrative and information activities.** Summary of the status of other actors' information activities, taken from the staff estimate, which is supported by the IEA.

2. (xx) MISSION.

   a. **Strategic command.** Statement of the superior commander's intent towards the information environment, taken from the strategic OPLAN.

12 Abbreviated classification.

b. **Joint Force Command.** Statement of the commander's intent towards the information environment, taken from the OPLAN.

3. (xx) EXECUTION.

a. Concept of operations.

i. **Intent.** An articulation of what success looks like, stating the objectives and effects that will achieve the outcome and how they relate to each other using time and space to group them.

(a) **Effects.** List of effects that are to be created or contributed to by military means, derived from mission-specific strategic and political guidance on information activities and the strategic OPLAN. The list should also include any undesirable effects which are to be avoided.

ii. Scheme of manoeuvre.

(a) **Strategic communications objectives.** Outline the StratCom objectives from Annex SS which will be linked to tasks and effects.

(b) **Narrative.** Add organization, strategic and micro (if applicable).

iii. **Main effort.** The critical activity for success.

b. **Themes and messages.** Taken from mission-specific StratCom guidance on information activities and the strategic OPLAN, Annex SS (if available).

(1) **Primary contributors.** Cross-reference to appropriate functional annexes of capabilities conducting or contributing to information activities.

(2) **Engagement.** Guidance on developing the engagement plan including key leader, soldier and cultural considerations, expanded at Annex A if necessary. The engagement plan will outline in general terms the engagements (targets and likely engagers) required to support delivery of those effects assigned to information ops. It is unlikely to specify exactly when engagements will occur but may give a desired time period.

(3) **Information activity integration.** How information activities are synchronized with other joint functions in the operational synchronization matrix developed by J3. The Info Ops effects matrix provides the basis for this.

4. (xx) COORDINATING INSTRUCTIONS.

a. **Information Activities Working Group.** Guidance on the Information Activities Working Group (IAWG) composition and process in support of the Strategic Communications Coordination Board (SCCB), taken from the relevant standard operating procedures (SOP) (if available).

b. **Analysis support.** Guidance on intelligence/systems analysis support to Info Ops, as well as contributions by capabilities conducting or contributing to information activities, with cross-reference to appropriate functional annexes.

c. **Targeting.** Guidance concerning the coordination of target nominations in support of the Joint Targeting Coordination Board, taken from the relevant SOP (if available).

d. **Assessment.** Reference to effects listed in Paragraph 3.a: guidance on the coordinated/collective assessment of information activities. This will be articulated in a matrix if required at Annex B.

e. **Information operations reporting.** Guidance on contributions to reporting concerning narratives, information activities and effects in the information environment, with cross-reference to appropriate functional annexes.

f. **Operations security.** Guidance on measures required to ensure operations security (OPSEC).

g. **Command and control defence considerations.** Guidance on the aspects of command and control defence that require consideration.

Annexes:

A. Engagement plan
B. Assessment matrix

Notes

Lexicon

Additional UK terms and definitions are shown in highlighted text.

Part 1 – Acronyms and abbreviations

AAC	Audience Analysis Course
AAP	Allied administrative publication
ACO	Allied Command Operations
AJP	Allied joint publication
ASCOPE	areas, structures, capabilities, organizations, people and events
ASCP	Allied Strategic Communications Publication
BAA	baseline audience analysis
Bi-SC	of the two Strategic Commands
C2S	command and control system
CARVER	criticality, accessibility, recoverability, vulnerability, effect and recognisability
CCIR	commander's critical information requirement
CDMD	Counter Disinformation and Media Development
CDS	Chief of the Defence Staff
CEWG	Communications and Engagement Working Group
CIMIC	civil-military cooperation
CIS	communication and information systems
CMI	civil-military interaction
CMIWG	Civil-Military Interaction Working Group
COA	course of action
COED	Concise Oxford English Dictionary
COM-B	capability, opportunity, motivation and behaviour
COIN	counter-insurgency
CONOPS	concept of operations
COPD	Comprehensive Operations Planning Directive
COS	chief of staff
CPOE	comprehensive preparation of the operating environment

CUOE	comprehensive understanding of the operating environment
DCO	defensive cyberspace operation
DCDC	Development, Concepts and Doctrine Centre
DDA	Deterrence and Defence of the Euro-Atlantic Area
DDC	Defence Communicators Course
Defence StratCom	Defence strategic communication
DirCom	director of communications
Dir ComDiv	Director Communications Division
EDTs	emerging and disruptive technologies
EEFI	essential elements of friendly information
EME	electromagnetic environment
EMS	electromagnetic spectrum
GPMESII	geospatial + PMESII
HFA	human factors analysis
IACB	Information Activities Coordination Board
IAWG	Information Activities Working Group
IEA	information environment assessment
Info Ops	information operations
IOFC	Information Operations Foundation Course
J10-StratCom	J10-Strategic Communications directorate
JCB	Joint Coordination Board
JCMB	Joint Collection Management Board
JDP	joint doctrine publication
JFEWG	Joint Fires and Effects Working Group
JIAG	Joint Information Activities Group
JIOC	Joint Information Operations Course
JIPOE	joint intelligence preparation of the operating environment
JPTL	joint prioritized target list
JTCB	Joint Targeting Coordination Board
JTTP	joint tactics, techniques and procedures
JTWG	Joint Targeting Working Group
KLE	key leader engagement
LEGAD	legal advisor

MAA	mission audience analysis
MC	Military Committee
MCDC	Multinational Capability Development Campaign
Mil PA	military public affairs
MOA	measure of activity
MOD	Ministry of Defence
MOE	measure of effectiveness
MOP	measure of performance
MOS	measure of success
MPOC	Military Psychological Operations Course
MSO	military strategic objective
NATO	North Atlantic Treaty Organization
NCS	NATO Command Structure
NEO	non-combatant evacuation operation
NWCC	NATO Warfighting Capstone Concept
OCO	offensive cyberspace operation
OPLAN	operation plan
OPP	operations planning process
OPSEC	operations security
PIR	priority intelligence requirement
PMESII	political, military, economic, social, infrastructure and information
PMESIIH	PMESII + health
PMESII-PT	PMESII + physical and time
PPP	presence, posture and profile
PsyOps	psychological operations
RBIO	rules-based international order
RFI	request for information
SACEUR	Supreme Allied Commander Europe
SCCB	Strategic Communications Coordination Board
SCAEF	Strategic Communication Actions and Effects Framework
SCE	supporting cognitive effects
SCEPVA	Sovereign Cyber Effects Provided Voluntarily by Allies
SHAPE	Supreme Headquarters Allied Powers Europe
SIAWG	Strategic Information Activities Working Group

SMART	specific, measurable, attainable, relevant and time-bounded
SOP	standard operating procedures
SSR	security sector reform
STEMPLES	social, technological, environmental, military, political, legal, economic and security
StratCom	strategic communications
TAA	target audience analysis
TDWG	Target Development Working Group
TVB	Target Validation Board
UK	United Kingdom

Part 2 – Terms and definitions

actor
An individual, group or entity whose actions are affecting the attainment of the end state. (NATO Agreed)

adversary
An individual, group or entity whose intentions or interests are opposed to those of friendly parties and against which legal coercive political, military or civilian actions may be envisaged and conducted. (NATO Agreed)

artificial intelligence
The branch of computer science devoted to developing data processing systems that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement.
(NATO Adopted, record 28750)

audience
An individual, group or entity whose interpretation of events and subsequent behaviour may affect the attainment of the end state.
Note: The audience may consist of publics, stakeholders and actors.
(NATO Agreed)

audience analysis
The understanding and segmentation of audiences in support of the achievement of objectives. (NATO Agreed)

audience-centric approach
The understanding, planning, execution and monitoring of activity to influence audiences' attitudes, beliefs or behaviours to achieve desired outcomes. (JDP 0-01.1)

baseline audience analysis
The foundational level of audience analysis to support planning and inform mission and target audience analysis. (JDP 0-01.1)

centre of gravity
The primary source of power that provides an actor its strength, freedom of action and/or will to fight. (NATO Agreed)

civil-military cooperation
A military joint function that integrates the understanding of the civil factors of the operating environment and that enables, facilitates and conducts civil-military interaction to support the accomplishment of missions and military strategic objectives in peacetime, crisis and conflict. (NATO Agreed)

civil-military interaction
Activities between NATO military bodies and non-military actors to foster mutual understanding that enhances effectiveness and efficiency in crisis management and conflict prevention and resolution. (NATO Agreed)

collateral damage
Inadvertent casualties, damage and/or destruction caused by military operations. (NATO Agreed)

communication activities
Information activities performed by military public affairs and psychological operations capabilities. (This description only applies to this publication.)

comprehensive approach
Combining all available political, military and civilian capabilities, in a concerted effort to attain the desired end state. (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)

cyber and electromagnetic domain
A domain comprising of capabilities which enable activities that maintain freedom of action by creating effects in and through cyberspace and the electromagnetic spectrum. (JDP 0-01.1)

cyberspace
The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data. (NATO Agreed)

cyberspace operation
Actions in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve military objectives. (NATO Agreed)

deception
Deliberate measures to mislead targeted decision-makers into behaving in a manner advantageous to the commander's intent. (NATO Agreed)

Defence strategic communication
Advancing national interests by using Defence as a means of communication to influence the attitudes, beliefs and behaviours of audiences. (JDP 0-01.1)

effect dimensions
An analytical construct that translates actions in the engagement space into the physical, virtual and cognitive consequences that these actions may have. (NATO Agreed)

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

enemy
An individual or group, entity or state actors whose actions are hostile and against which the legal use of armed force is authorized. (NATO Agreed)

end state
The political-strategic statement of conditions that defines an acceptable concluding situation to be attained at the end of a strategic engagement. (NATO Agreed)

engagement space / battlespace
The part of the operating environment where actions and activities are planned and conducted. (NATO Agreed)

environment
The surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans, and their interrelations. (NATO Agreed)

fires
The use of weapon systems to create a specific lethal or non-lethal effect on a target.
Note: Fires include the use of systems employing electromagnetic energy. (NATO Agreed)

gender
The social attributes associated with being male and female, learned through socialisation, that determine a person's position and value in a given context, including in the relationship between women and men and girls and boys, as well as in the relations between women and those between men.
Note: Gender issues do not equate to an exclusive focus on women. (NATO Agreed)

gender mainstreaming
A strategy used to achieve gender equality by assessing the implications for women and men of any planned action, in all areas and at all levels, in order to assure that the concerns and experiences of both sexes are taken into account. (NATO Agreed)

gender perspective
The ability to detect if and when men, women, boys and girls are being affected differently by a situation due to their gender.
Note: Gender perspective takes into consideration how a particular situation impacts the needs of men, women, boys and girls, and if and how activities affect them differently. (NATO Agreed)

host nation
A country that, by agreement:
a. receives forces and materiel of NATO member states or other countries operating on/from or transiting through its territory;
b. allows materiel and/or NATO and other organizations to be located on its territory; and/or
c. provides support for these purposes. (NATO Agreed)

information
Unprocessed data of every description which may be used in the production of intelligence. (NATO Agreed)

information activities
Activities performed by any capability or means, focused on creating cognitive effects. (NATO Agreed)

information environment
An 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. (NATO Agreed)

information operations
A staff function to analyze, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and audiences in support of mission objectives. (NATO Agreed)

information system
An assembly of equipment, methods and procedures and, if necessary, personnel, organized to accomplish information processing functions. (NATO Agreed)

joint effects function
A staff function to integrate, coordinate, synchronize and prioritize actions and activities to create effects in the engagement space. (NATO Agreed)

measure of effectiveness
A criterion used to assess changes in system behaviour, capability, or operating environment, tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. (NATO Agreed)

measure of performance
A criterion that is tied to measuring task accomplishment in order to assess friendly actions. (NATO Agreed)

media operations
The military information activity that offers accurate and timely information to nominated audiences through the media, in order to create the desired communications effect and build consent for UK national objectives, while maintaining operations security and personal security. (JDP 0-01.1)

military public affairs
The strategic communications capability responsible for promoting military aims and objectives by communicating accurate and truthful information to internal and external audiences in a timely manner. (NATO Agreed)

mission audience analysis
The focused understanding of target audiences in support of a mission or task to create the desired planning effect. (JDP 0-01.1)

narrative
A spoken or written account of events and information arranged in a logical sequence to influence the behaviour of a target audience. (NATO Agreed)

offensive cyber operations
Activities that project power to achieve military objectives in or through cyberspace. (JDP 0-01.1)

operational domain
A specified sphere of capabilities and activities that can be applied within an engagement space.
Note: there are five operational domains: maritime, land, air, space and cyberspace, each conditioned by the characteristics of its operating environment.(NATO Agreed)
UK note: The UK recognises the five operational domains to be: maritime, land, air, space, and cyber and electromagnetic.

operating environment
A composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander. (NATO Agreed)

operations security
All measures taken to give a military operation or exercise appropriate security, using passive or active means, to deny an adversary knowledge of essential elements of friendly information or indicators thereof. (NATO Agreed)

propaganda
Information, especially of a biased or misleading nature, used to promote a political cause or point of view. (NATO Agreed)

psychological operation
Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviours, affecting the achievement of political and military objectives. (NATO Agreed)

public
An individual, group or entity who is aware of activities that may affect the attainment of the end state. (NATO Agreed)

stakeholder
An individual, group or entity who can affect or is affected by the attainment of the end state. (NATO Agreed)

strategic communications
In the NATO military context, the integration of communication capabilities and information staff function with other military activities, in order to understand and shape the information environment, in support of NATO strategic aims and objectives. (NATO Agreed)

target
An area, infrastructure, object, audience or organization against which activities can be directed to create desired effects. (NATO Agreed)

target audience analysis
The focused examination of targeted audiences to create desired effects. (NATO Agreed)

AJP-10.1(A)(1)

Designed by the Development, Concepts and Doctrine Centre

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

The material in this publication is certified as an FSC mixed resourced product, fully recyclable and biodegradable.