



C3 Classification Taxonomy

Baseline 1.0

Friday, 15 June 2012

Table of Contents

Table of Contents	2
1 Introduction	7
2 Background	8
3 C3 Classification Taxonomy	9
4 Operational Context	10
4.1 Missions and Operations	11
4.1.1 Policy and Guidance	11
4.1.1.1 Strategic Concept	11
4.1.1.2 Political Guidance	11
4.1.1.3 Military Guidance	12
4.1.1.4 Allied Publications	12
4.1.1.5 C3 Policies	12
4.1.2 Mission Types	12
4.1.2.1 Mission Type - Collective Defence (CD)	12
4.1.2.2 Mission Type - Consequence Management (CM)	12
4.1.2.3 Mission Type - Conflict Prevention (CP)	12
4.1.2.4 Mission Type - Counter Terrorism (Failed State) (CT(FS))	12
4.1.2.5 Mission Type - Counter Terrorism (State Sponsored Covert) (CT(SSC))	12
4.1.2.6 Mission Type - Support to Disaster Relief (DR)	13
4.1.2.7 Mission Type - Extraction Operation (EOP)	13
4.1.2.8 Mission Type - Enforcement of Sanctions and Embargoes (ESE)	13
4.1.2.9 Mission Type - Peace Enforcement (PE)	13
4.1.2.10 Mission Type - Peacekeeping (PK)	13
4.1.2.11 Mission Type - Support to Humanitarian Assistance (SHA)	13
4.1.2.12 Mission Type - Anti-Terrorism (AT)	14
4.1.2.13 Mission Type - Peacemaking (PM)	14
4.1.2.14 Mission Type - Peacebuilding (PB)	14
4.1.2.15 Mission Type - Support of Non-Combatant Evacuation Operations (NEO)	14
4.1.2.16 Mission Type - Military Aid/Support to Civil Authorities (SCA)	14
4.1.2.17 Mission Type - Permanent Tasks	14
4.1.3 Tasks	14
4.2 Operational Capabilities	15
4.2.1 Capability Hierarchy, Codes and Statements	15
4.2.1.1 Capability Hierarchy Framework (CHF)	15
4.2.1.2 Capability Codes (CCs)	16
4.2.1.3 Capability Statements (CSs)	16
4.2.2 Business Processes	16

4.2.2.1 IA Processes	16
4.2.2.2 SMC Processes	16
4.2.2.3 Governance Processes	16
4.2.2.4 Management Processes	16
4.2.2.5 Consultation Processes	16
4.2.2.6 Cooperation Processes	17
4.2.2.7 Mission Threads	17
4.2.2.8 Support Processes	17
4.2.3 Information Products	17
4.2.3.1 IA Information	17
4.2.3.2 SMC Information	17
4.2.3.3 Intent and Guidance	17
4.2.3.4 Rules and Measures	17
4.2.3.5 Plans	18
4.2.3.6 Tasking and Orders	18
4.2.3.7 Situational Awareness	18
4.2.3.8 Resource Status	18
4.2.3.9 Requests and Responses	18
5 CIS Capabilities	19
5.1 User-Facing Capabilities	20
5.1.1 User Applications	21
5.1.1.1 IA Applications	21
5.1.1.2 SMC Applications	21
5.1.1.3 Joint COI Applications	22
5.1.1.4 Air COI Applications	22
5.1.1.5 Land COI Applications	22
5.1.1.6 Maritime COI Applications	22
5.1.1.7 Space COI Applications	22
5.1.1.8 Special Operations COI Applications	22
5.1.1.9 JISR COI Applications	22
5.1.1.10 Logistics COI Applications	23
5.1.1.11 EW COI Applications	23
5.1.1.12 Environmental COI Applications	23
5.1.1.13 Missile Defence COI Applications	23
5.1.1.14 CIMIC COI Applications	23
5.1.1.15 CBRN COI Applications	23
5.1.1.16 ETEE COI Applications	24
5.1.1.17 CIS COI Applications	24
5.1.1.18 Modeling and Simulation COI Applications	24
5.1.1.19 Generic Applications	24
5.1.2 User Appliances	25

5.2 Technical Services	26
5.2.1 Community Of Interest (COI) Services	27
5.2.1.1 COI-Specific Services	27
5.2.1.1.1 COI-Specific IA Services	27
5.2.1.1.2 COI-Specific SMC Services	27
5.2.1.1.3 Joint COI Services	27
5.2.1.1.4 Air COI Services	28
5.2.1.1.5 Land COI Services	28
5.2.1.1.6 Maritime COI Services	28
5.2.1.1.7 Space COI Services	28
5.2.1.1.8 Special Operations COI Services	28
5.2.1.1.9 JISR COI Services	28
5.2.1.1.10 Logistics COI Services	28
5.2.1.1.11 EW COI Services	28
5.2.1.1.12 Environmental COI Services	29
5.2.1.1.13 Missile Defence COI Services	29
5.2.1.1.14 CIMIC COI Services	29
5.2.1.1.15 CBRN COI Services	29
5.2.1.1.16 ETEE COI Services	29
5.2.1.1.17 Modeling and Simulation COI Services	29
5.2.1.1.18 CIS COI Services	30
5.2.1.2 COI-Enabling Services	30
5.2.1.2.1 COI-Enabling IA Services	30
5.2.1.2.2 COI-Enabling SMC Services	30
5.2.1.2.3 Operational Planning Services	30
5.2.1.2.4 Tasking and Order Services	30
5.2.1.2.5 Situational Awareness Services	30
5.2.1.2.6 Business Support Services	30
5.2.1.2.7 Modeling and Simulation Services	30
5.2.2 Core Enterprise Services	31
5.2.2.1 Enterprise Support Services	31
5.2.2.1.1 Enterprise Support IA Services	31
5.2.2.1.2 Enterprise Support SMC Services	31
5.2.2.1.3 Unified Communication and Collaboration Services	32
5.2.2.1.4 Information Management Services	32
5.2.2.1.5 Geospatial Services	32
5.2.2.2 SOA Platform Services	32
5.2.2.2.1 SOA Platform IA Services	32
5.2.2.2.2 SOA Platform SMC Services	32
5.2.2.2.3 Message-oriented Middleware Services	33
5.2.2.2.4 Web Platform Services	33
5.2.2.2.5 Information Platform Services	33

5.2.2.2.6 Composition Services	33
5.2.2.2.7 Mediation Services	33
5.2.2.3 Infrastructure Services	34
5.2.2.3.1 Infrastructure IA Services	34
5.2.2.3.2 Infrastructure SMC Services	34
5.2.2.3.3 Infrastructure Processing Services	34
5.2.2.3.4 Infrastructure Storage Services	34
5.2.2.3.5 Infrastructure Networking Services	35
5.2.3 Communications Services	36
5.2.3.1 Communications Access Services	36
5.2.3.1.1 Communications Access IA Services	36
5.2.3.1.2 Communications Access SMC Services	36
5.2.3.1.3 Analogue Access Services	37
5.2.3.1.4 Digital (Link) Access Services	37
5.2.3.1.5 Message-based Access Services	37
5.2.3.1.6 Circuit-based Access Services	37
5.2.3.1.7 Frame-based Access Services	37
5.2.3.1.8 Packet-based Access Services	37
5.2.3.1.9 Multimedia Access Services	37
5.2.3.2 Transport Services	37
5.2.3.2.1 Transport IA Services	38
5.2.3.2.2 Transport SMC Services	38
5.2.3.2.3 Edge Transport Services	38
5.2.3.2.4 Core Network Services	38
5.2.3.2.5 Aggregation Services	38
5.2.3.2.6 Broadcast Services	39
5.2.3.2.7 Distribution Services	39
5.2.3.3 Transmission Services	39
5.2.3.3.1 Transmission IA Services	39
5.2.3.3.2 Transmission SMC Services	39
5.2.3.3.3 Wired Local Area Transmission Services	40
5.2.3.3.4 Wired Metropolitan Area Transmission Services	40
5.2.3.3.5 Wired Wide Area Transmission Services	40
5.2.3.3.6 Wireless LOS Static Transmission Services	40
5.2.3.3.7 Wireless LOS Mobile Transmission Services	40
5.2.3.3.8 Wireless BLOS Static Transmission Services	41
5.2.3.3.9 Wireless BLOS Mobile Transmission Services	41
5.2.4 Information Systems Equipment	42
5.2.5 Communications Equipment	43
6 Groupings	44
6.1 IA	44

6.2 SMC 44

1 Introduction

The C3 Classification Taxonomy provides a tool to synchronize all capability activities for Consultation, Command and Control (C3) in the NATO Alliance by connecting the Strategic Concept and Political Guidance through the NATO Defence Planning Process (NDPP) to traditional Communications and Information Systems (CIS) architecture and design constructs.

Throughout the years, many communities have developed and contributed components to the overall CIS capability of the Alliance but sadly, most groups did their work in splendid isolation. Today we are confronted with a patch-quilt of systems, applications, vocabularies and taxonomies and simple English words such as service or capability have become highly ambiguous. As a result of extreme stove-piping, NATO now faces a very complex fabric of capabilities that are not interoperable and attempts to solve these problems are often hampered by lack of mutual understanding caused by confusing vocabularies.

The purpose of this C3 Classification Taxonomy is to capture concepts from various communities and map them for item classification, integration and harmonization purposes. Recognizing dependencies and relationships, it links Political and Military Ambitions, Mission-to-Task Decomposition, Capability Hierarchy, Statements and Codes, Operational Processes, Information Products, Applications, Services and Equipment to Reference Documents, Standards, Implementation Programs and Fielded Baselines.

This approach is referred to as 'enterprise mapping', as the C3 Classification Taxonomy 'charts' the NATO C3 'landscape'.

2 Background

The complex challenges posed by the future security environment call for a systematic method for planning under uncertainty. Flexible and agile capabilities are required that can be quickly adapted to evolving NATO needs. A flexible and agile framework must seamlessly provide an enterprise environment where the Nations can accomplish future NATO missions and aims.

Addressing these challenges requires a Comprehensive Approach focused on the achievement of objectives/effects through a coordinated use of the Alliance's Political, Military, Economic and Civil instruments of power. It will often require the Alliance to operate as part of a wider Coalition. Consequently, achieving the required objective/effects will often necessitate the coordinated action of many disparate entities within and between organizations. These organizations may be military and non-military; NATO organizations or organizations from member nations; organizations from non-NATO nations, International Organizations (IO) such as the United Nations (UN) and Non-Governmental Organizations (NGO). It is therefore urgent to consider and include coordination with said organisations as NATO derives and defines future NATO Consultation, Command and Control (C3) requirements.

The complexity and uncertainty outlined above means that interoperability will often need to be achieved on an ad-hoc basis. The manner in which interoperability is achieved therefore needs to be flexible and adaptive. Such flexibility and adaptability is achieved by applying a service-oriented approach to the development of interoperability solutions at the organizational and system level. The key to deriving robust C3 capabilities and associated interoperability is to separate 'what needs to be delivered' (i.e., the capability requirements) from 'how it is delivered' (the solution/technology).

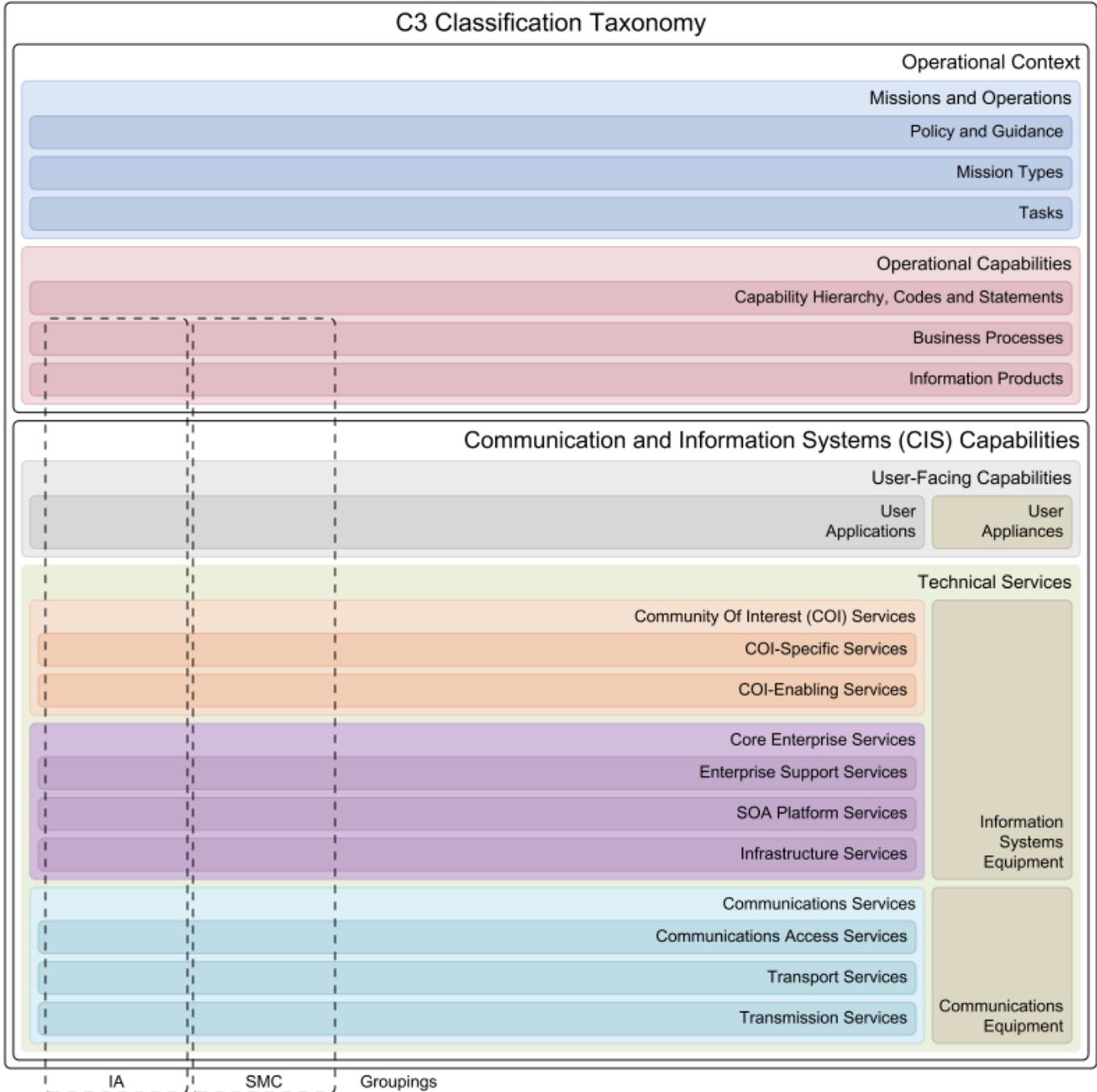
It is NATO's intent that the approach for deriving C3 requirements is through 'service provision'. This entails specifying the 'requester' for a task to be performed and a 'provider' who commits to performing the task. An example of a requester may be a Headquarter (HQ) and the provider may be a subordinate unit or another HQ. This illustrates that a request may be a tasking with an obligation to deliver or that a request can be negotiated and potentially denied. This is the essence of the service-oriented approach.

The service-oriented approach is a natural complement to capability based planning. It emphasizes to describe how the elements within a system/organization interrelate and interact to perform tasks and hence achieve required objectives and effects. Such interrelation and interaction is the core element of architectures. Thus, the generation of architectures is intrinsic to this service oriented approach. In implementing a Service Oriented Architecture (SOA) as one of the key enablers for NATO's Network Enabled Capability (NEC), there is a need to reflect multiple perspectives on relationships between processes, requirements, standards, architectures and implementations that will help program, capability and project managers gain a better understanding of the complete environment.

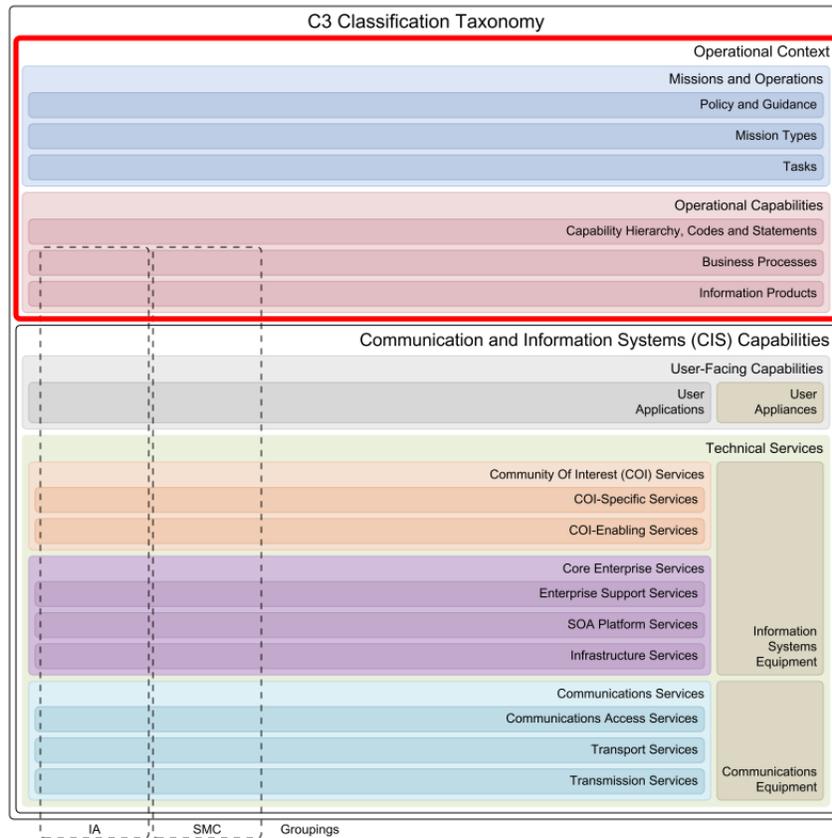
In a complex and federated enterprise like NATO there is a need for a generic structure or framework that can be used to align and synchronize various activities and projects that are on-going in parallel when the organisation's CIS infrastructure transforms towards a network-enabled capability. The C3 Classification Taxonomy provides that generic framework.

3 C3 Classification Taxonomy

For the purpose of this document, a 'taxonomy' is defined as a 'particular classification arranged in a hierarchical structure organised by supertype-subtype relationships. The picture below depicts the top levels of the C3 Classification Taxonomy connecting the top-level political ambitions all the way to 'the wire'. Subsequent chapters provide definitions for all depicted components as extracted from the Allied Command Transformation (ACT) Enterprise Mapping (EM) Wiki on the date shown at the bottom of the page. Lower levels in the taxonomy as well as linkage between the taxonomy items and Programs Of Work (POWs), Implementation programs (CPs, CURs), Standards and Fielded Capabilities can be found on the ACT EM Wiki at <https://tide.act.nato.int/em>.



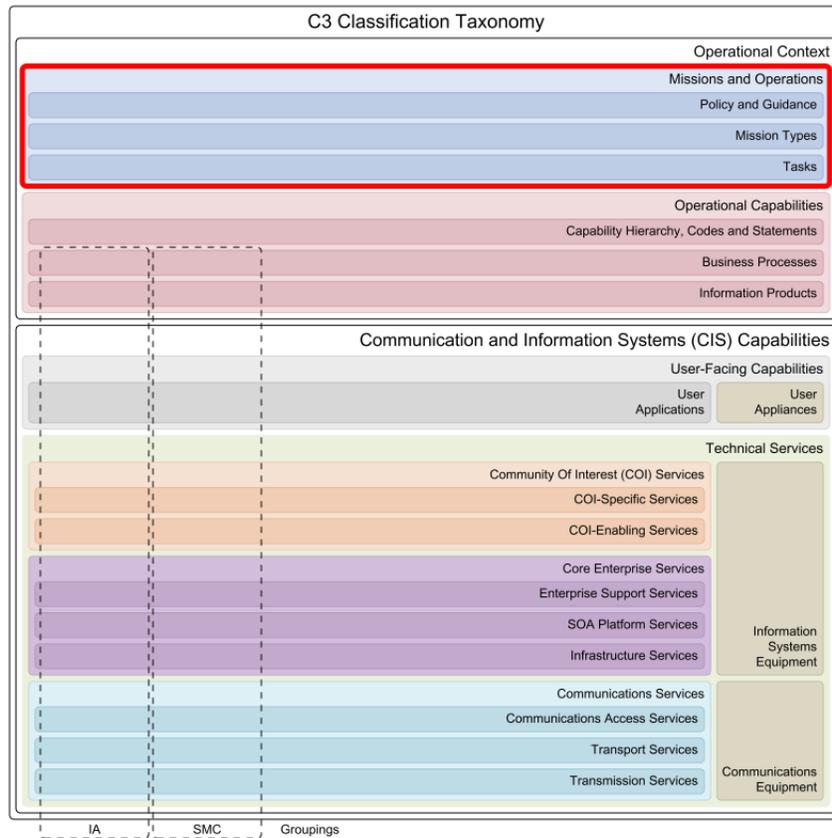
4 Operational Context



The Operational Context describes the environment in which CIS Capabilities are defined and used. By capturing NATO's overarching political guidance, stating the Level of Ambition (LoA), identifying mission types and key tasks, cataloging needed capabilities, addressing operational processes, and capturing relevant information products, a context and scope for CIS Capability creation and deployment is defined.

Information in this part of the C3 Classification Taxonomy is broader than the typical focus on C3 capabilities, and is primarily obtained from NATO's Defence Planners through the NATO Defence Planning Process (NDPP).

4.1 Missions and Operations



Missions and Operations capture NATO's Political and Military Level of Ambition (LoA) as derived from the Strategic Concept and Political Guidance. These ambitions are expressed as a series of possible mission types and related tasks, as well as references to relevant concepts, guidance, policies, and publications. Mission types and key tasks are derived from the Mission-to-Task Decomposition (MTD) expressed in the NATO Defence Planning Process (NDPP).

4.1.1 Policy and Guidance

Policy and Guidance express NATO's political and military Level of Ambition (LoA) based on a Strategic Concept that serves as the Alliance's roadmap. Derived Political Guidance reflects the political, military, economic, legal, civil and technological factors which could (and should) impact the development of required capabilities. Furthermore, this segment captures the policies and other reference documents that guide and support C3 capability development, implementation and sustainment.

4.1.1.1 Strategic Concept

The Strategic Concept is an official document that outlines NATO's enduring purpose and nature and its fundamental security tasks. It also identifies the central features of the new security environment, specifies the elements of the Alliance's approach to security and provides guidelines for the adaptation of its military forces. The concept that was adopted by NATO leaders at the 2010 Lisbon Summit, will serve as the Alliance's roadmap for the next ten years. It reconfirms the commitment to defend one another against attack as the bedrock of Euro-Atlantic security.

4.1.1.2 Political Guidance

"Political Guidance" provides direction for the continuing transformation of defence capabilities and forces, and the implementation of defence-related aspects of the Strategic Concept. The Political Guidance expresses the NATO Level of Ambition (LoA), and it provides the aims and objectives for the Alliance as starting point for the NATO Defence Planning Process (NDPP).

4.1.1.3 Military Guidance

Military Guidance translates the Strategic Concept into detailed instructions necessary for military implementation of the Alliance's Strategic Concept. It also provides supplementary guidance to the Political Guidance.

4.1.1.4 Allied Publications

Allied Publications (APs) are NATO standards established and approved by several or all NATO member states at tasking authority level.

4.1.1.5 C3 Policies

Consultation, Command & Control (C3) Policies are established by the C3 Board (C3B) in order to govern C3 capability management throughout a capability's life cycle.

4.1.2 Mission Types

Mission Types (MTs) are a strategic representation of operations as derived from NATO's Level of Ambition (LoA) and expressed as a set of Military Strategic Objectives (MSOs) and Operational Objectives (OO) required to achieve a specified end-state.

The circumstances in which a certain Mission Type may occur are described in so-called Generic Planning Situations (GPSs), that provide generalized descriptions of the affiliated political, military, socio-economic and geographic environment.

4.1.2.1 Mission Type - Collective Defence (CD)

Collective Defence (CD) results from the invocation of NATO's article 5 which states that an armed attack against one or more NATO Nations shall be considered an attack against all and consequently the Nations agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

4.1.2.2 Mission Type - Consequence Management (CM)

Consequence Management (CM) is the use of reactive measures to mitigate the destructive effects of terrorism. Regardless of the level of effort to defend against terrorist attacks, it is likely that terrorism will continue, and with it, the possibility of a Chemical, Biological, Radiological, and Nuclear (CBRN) event with associated mass casualties.

4.1.2.3 Mission Type - Conflict Prevention (CP)

Conflict Prevention (CP) involves activities that are normally conducted in accordance with the principles of Chapter VI of the UN Charter. Activities may include: diplomatic, economic, or information initiatives; actions designed to reform a country's security sector and make it more accountable to democratic control; or deployment of forces designed to prevent or contain disputes from escalating to armed conflict.

4.1.2.4 Mission Type - Counter Terrorism (Failed State) (CT(FS))

Counter-Terrorism (CT) is the use of offensive measures to reduce the vulnerability of forces, individuals and property to terrorism, to include Counter-Force activities and containment by military forces and civil agencies. CT operations are mainly joint operations. In case the CT operations are conducted in or against a failed state, these are referred to as "Counter Terrorism (Failed State)" (CT(FS)).

4.1.2.5 Mission Type - Counter Terrorism (State Sponsored Covert) (CT(SSC))

Counter-Terrorism is the use of offensive measures to reduce the vulnerability of forces, individuals and property to terrorism, to include Counter-Force activities and containment by military forces and civil agencies. CT operations are mainly joint operations. In case the CT operations are conducted in a manner covert to opposing regimes, these are referred to as "Counter Terrorism (State Sponsored Covert)" (CT(SSC)).

4.1.2.6 Mission Type - Support to Disaster Relief (DR)

Support to Disaster Relief (DR) provides support after a man-made or natural disaster. Emergency relief concerns sustaining the means to safeguard life and requires very rapid reaction particularly where extreme climates are encountered. Protecting human life is an inherent responsibility. Relief operations, in the narrow sense of the provision of aid, are principally the purview of humanitarian or aid agencies, whether United Nations (UN) or government, including host government (where one exists), Non-Governmental Organizations (NGOs), and the civil sector.

4.1.2.7 Mission Type - Extraction Operation (EOP)

Extraction Operation (EOPs) may be described as missions where a NATO-led force covers or assists in the withdrawal of a UN or other military mission from a crisis region. A force committed to an extraction operation should have similar capabilities to those required by a force operating in support of Non-Combatant Evacuation Operation (NEO) and should include the necessary assets for transporting the personnel to be extracted. An extraction operation is most likely to be conducted in an uncertain or hostile environment. In general, these conditions are similar to those pertaining in the previous instances of NEO. In a hostile environment, a loss of consent for the presence of a UN or other mission could occur or the HN government may not have effective control of the territory in question. Under these circumstances, planning must anticipate a potential need for a NATO extraction force. In the past, NATO has established extraction forces, on a temporary basis, to enhance the safety of international missions.

4.1.2.8 Mission Type - Enforcement of Sanctions and Embargoes (ESE)

Enforcement of Sanctions and Embargoes (ESE) is designed to force a nation to obey international law or to conform to a resolution or mandate. Sanctions generally concern the denial of supplies, diplomatic, economic, and other trading privileges, and the freedom of movement of those living in the sanctions area. Sanctions may be imposed against a specific party or in the context of Non-Article 5 Crisis Response Operation (NA5CRO), over a wide area embracing all parties. The military objective is to establish a barrier, allowing only non-sanctioned goods to enter or exit. Depending on geography, sanction enforcement normally involves some combination of air, land, and maritime forces. Examples are embargoes, maritime interdiction operations (MIOs), and the enforcement of no-fly zones (NFZs).

4.1.2.9 Mission Type - Peace Enforcement (PE)

Peace Enforcement (PE) involves operations that normally take place under the principles of Chapter VII of the UN Charter. The difference between PE and other Peace support operations (PSOs) is that the Chapter VII mandate allows more freedom of action for the commander concerning the use of force without losing legitimacy, with a wider set of options being open. Even in a PE, consent should be pursued through persuasion prior to using force, with coercion through force being an option at any time without altering the original mandate. These operations are coercive in nature and are conducted when the consent of all parties to the conflict has not been achieved or might be uncertain. They are designed to maintain or re-establish peace or enforce the terms specified in the mandate. In the conduct of PE, the link between political and military objectives must be extremely close. It is important to emphasize that the aim of the PE operation will not be the defeat or destruction of an adversary, but rather to compel, coerce, and persuade the parties to comply with a particular desired outcome and the established rules and regulations.

4.1.2.10 Mission Type - Peacekeeping (PK)

Peacekeeping (PK) involves operations that are generally undertaken in accordance with the principles of Chapter VI of the UN Charter in order to monitor and facilitate the implementation of a peace agreement. The loss of consent or the development of a non-compliant party may limit the freedom of action of the PK force and even threaten the continuation of the mission or cause it to evolve into a PE operation. Thus, the conduct of PK is driven by the requirement to build and retain perceived legitimacy.

4.1.2.11 Mission Type - Support to Humanitarian Assistance (SHA)

Support to Humanitarian Assistance (SHA) consists of activities and tasks to relieve or reduce human suffering. SHA may occur in response to earthquake, flood, famine, or manmade disasters such as chemical, biological, radiological, or nuclear contamination or pandemic outbreak. They may also be necessary as a consequence of war or the flight from political, religious, or ethnic persecution. HA is conducted to relieve or reduce the results of natural or man-made disasters or endemic conditions that might present a serious threat to life or that can result in great damage to or loss of property. HA is limited in scope and duration and is designed to supplement or complement the efforts of the Host Nation (HN) civil

authorities or agencies that may have the primary responsibility for providing that assistance. They normally supplement the activities of governmental authorities, Non-Governmental Organisations (NGOs), and Intergovernmental Organisations (IGOs).

4.1.2.12 Mission Type - Anti-Terrorism (AT)

Anti-Terrorism (AT) is the use of defensive measures to reduce the vulnerability of forces, individuals and property to terrorism, to include limited response and containment by military forces and civilian agencies. Nations have the primary responsibility for the defence of their populations and infrastructures with the Alliance providing support: this includes preventive measures as a foundation for basic security.

4.1.2.13 Mission Type - Peacemaking (PM)

Peacemaking (PM) involves the diplomatic-led activities aimed at establishing a cease-fire or a rapid peaceful settlement and is conducted after a conflict has started. Through comprehensive approaches the activities can include the provision of good offices, mediation, conciliation, and such actions as diplomatic pressure, isolation, sanctions, or other activities. Peacemaking is accomplished primarily by diplomatic means; however, military support to peacemaking can be made either indirectly, through the threat of intervention, or in the form of direct involvement of military assets.

4.1.2.14 Mission Type - Peacebuilding (PB)

Peacebuilding (PB) involves actions that support political, economic, military, and social measures through comprehensive approaches and that are aimed at strengthening political settlements of a conflict. Thus, for a society to regenerate and become self-sustaining, it must address the constituents of a functioning society that were discussed in Chapter I. Peacebuilding includes mechanisms to identify and support structures that will consolidate peace, foster a sense of confidence and well-being, and support economic reconstruction. Peacebuilding therefore requires the commitment of political, humanitarian and development resources to a long-term political process.

4.1.2.15 Mission Type - Support of Non-Combatant Evacuation Operations (NEO)

Support of Non-Combatant Evacuation Operations (NEOs) involves national diplomatic initiatives, with Alliance forces participating in a supporting role. NEOs may be described as operations conducted to relocate (to a place of safety) non-combatants threatened in a foreign country. Normally, Alliance forces would only support a NEO in the framework of a NATO-led operation and that support would not include the evacuation of nationals, which remains a national responsibility; however, nations could conduct NEOs for their nationals on a bi- or multi-national basis using NATO doctrine. Generally, a force committed to a NEO should have the capability to provide security, reception and control, movement, and emergency medical support for the civilians and unarmed military personnel to be evacuated.

4.1.2.16 Mission Type - Military Aid/Support to Civil Authorities (SCA)

Military Aid/Support to Civil Authorities (SCA) embraces all those military activities that provide temporary support, within means and capabilities, to civil communities or authorities, when permitted by law, and which are normally undertaken when unusual circumstances or an emergency overtakes the capabilities of the civil authorities. Categories of support include military assistance to civil authorities and support to humanitarian assistance operations.

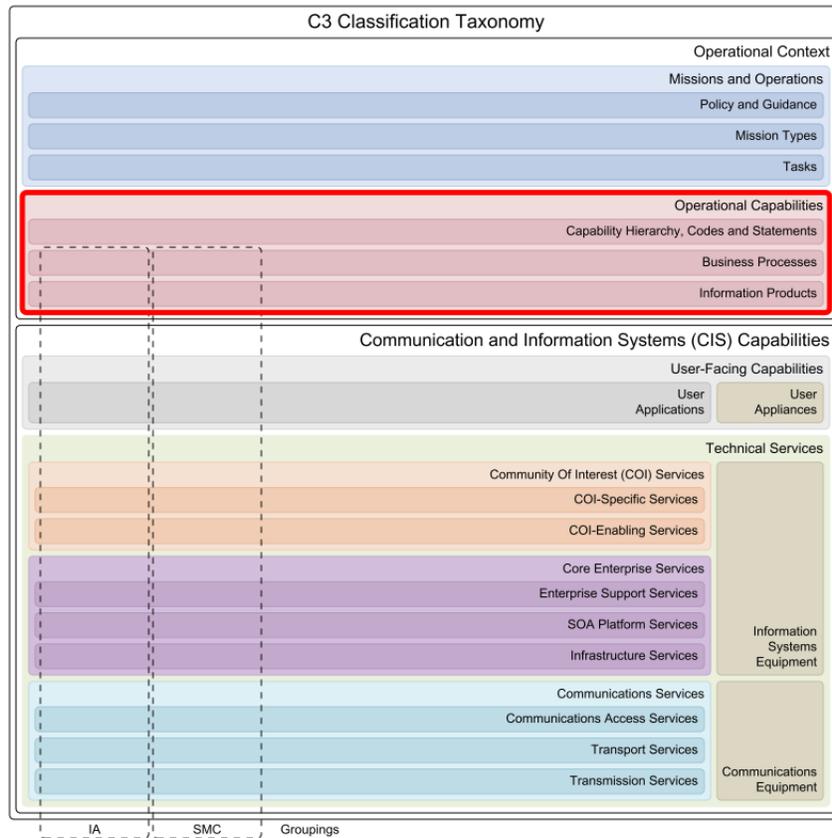
4.1.2.17 Mission Type - Permanent Tasks

Permanent Tasks capture routine activities performed on a permanent basis throughout NATO's static structure that are not captured by the official Mission Types.

4.1.3 Tasks

Tasks represent activities which need to be performed by the Alliance in order to achieve the stated objective for a given Mission Type (MT). Key Tasks (KTs) as the highest level in the task hierarchy are identified through Mission-to-Task Decomposition (MTD) which is part of the NATO Defence Planning Process (NDPP). Key Tasks are related to the achievement of an objective or desired effect within a specific Mission Task. Key Tasks are decomposed into Sub-Tasks (STs) and Sub-Sub-Tasks (SSTs).

4.2 Operational Capabilities



Operational Capabilities capture everything required by the Alliance to successfully complete Mission Types and achieve stated Levels of Ambition (LoAs). Operational Capabilities are captured in a Capability Hierarchy Framework (CHF) and are expressed as a set of Capability Codes (CCs) and Capability Statements (CSs) linked to established Business Processes. To support the implementation of C3 capabilities, Information Products that are identified during Business Process Analysis (BPA) are captured separately and linked to these Mission Types, Key Tasks and Capability Codes.

4.2.1 Capability Hierarchy, Codes and Statements

Capability Hierarchy, Codes and Statements express the capability needs resulting from the NATO Defence Planning Process (NDPP). On one hand, the Capability Hierarchy Framework (CHF) provides a structure to support the expression of Minimum Capability Requirements (MCRs) and Priority Shortfall Areas (PSA). On the other hand, in relation to this hierarchy, the Capability Codes (CCs) and Capability Statements (CSs) are used to specify capability requirements, and so form the basis for requirements apportionment and target setting.

4.2.1.1 Capability Hierarchy Framework (CHF)

The Capability Hierarchy Framework (CHF) incorporates the capabilities required to conduct all three of the military missions assigned in MC 0400/3, the Guidance for the Military Implementation of NATO's Strategic Concept:

- Collective Defence
- Crisis Management
- Cooperative Security

The overall objective of the Capability Hierarchy Framework is to provide a structure to support the expression of the "Minimum Capability Requirements" (MCR) and the Priority Shortfall Areas (PSA). It consists of a functional decomposition of capabilities at various levels of aggregation, and thus provides the framework within which capability requirements at alternative levels of granularity can be described and captured.

The Capability Hierarchy Framework integrates with and complements the Mission Analysis and Situation Analysis components of the "Capability Requirements Review" (CRR). The Minimum Capability Requirements (MCR) for the short/medium term are expressed in terms of the Bi-SC agreed Capability Codes (CCs) and Capability Statements (CSs). This MCR is derived primarily via mission analysis conducted through the "Mission to Task Decomposition" (MTD) developed for identified Mission Types (MTs).

The linkage of Capability Codes to the MTD by means of structured, consistent and validated Capability Assignment Logic is the primary mechanism for ensuring operationally valid requirements within the CRR process. The Capability Codes are, in turn, linked to the CHF in a manner that reflects the various functional capability contributions delivered by that Capability Code. This allows Capability Code shortfalls identified during Step 2 of the NATO Defence Planning Process (NDPP) to be translated into related functional capability shortfalls in the CHF.

4.2.1.2 Capability Codes (CCs)

Capability Codes (CCs) are unique alphanumeric descriptors for functional capability groups and are used as a common language to describe capabilities in the Defence and Operations Planning frameworks.

4.2.1.3 Capability Statements (CSs)

Capability Statements (CSs) capture capability requirements along the Doctrine, Organization, Training, Materiel, Leadership, Facilities, Personnel, and Interoperability (DOTMLPFI) lines of development and are part of the common language used to describe capabilities in the Defence and Operations Planning frameworks.

4.2.2 Business Processes

Business Processes are a collection of related, structured activities or tasks that produce a specific service or product (serve a particular goal) for a particular customer or customers. The C3 business process definitions connect activities, actors and information products, relevant to the NATO C3 environment.

4.2.2.1 IA Processes

Information Assurance (IA) Processes are a grouping of related, structured activities or tasks that are concerned with information security for a particular customer or set of customers.

4.2.2.2 SMC Processes

Service Management and Control (SMC) Processes are a grouping of related, structured activities or tasks that are concerned with service provisioning to a particular customer or set of customers.

4.2.2.3 Governance Processes

Governance Processes support the tasks of steering the Alliance toward specific objectives with the perspective of assuring the interests of the stakeholders. They include setting direction through prioritisation and decision-making, monitoring performance, compliance and progress against agreed direction and objectives. Governance processes concur in defining a framework to establish transparent accountability of individual decision and ensures the traceability of decisions to assigned responsibilities.

4.2.2.4 Management Processes

Management Processes support the tasks of planning, organizing, directing, resourcing and controlling the efforts of the Alliance towards specific objectives as set and ruled by the governance body.

4.2.2.5 Consultation Processes

Consultation Processes support the practice of regular exchange of information and opinions, communication of actions or decisions and discussion among the NATO Nations with the aim of reaching consensus on policies to be adopted or actions to be taken.

4.2.2.6 Cooperation Processes

Cooperation Processes support regular exchanges and dialogue at senior and working levels on political and operational issues as well as the development of a common Comprehensive Approach with key partners, most important UN and EU, on issues of common interest including in communication and information-sharing; capacity-building, training and exercises; lessons learned, planning and support for contingencies; and operational coordination and support in order to improve NATO's ability to deliver stabilization and reconstruction effects.

4.2.2.7 Mission Threads

Mission Threads are an operational description of end-to-end activities that accomplish the execution of a mission. Mission Types and Tasks provide the Operational Mission Area context for the development of complete end-to-end Mission Thread architectures that will also describe the Information Products, User Applications and Technical Services required to successfully execute a Mission Thread from end-to-end.

4.2.2.8 Support Processes

Support Processes underpin day-to-day operations of the Alliance, such as finance and administration, communication, manpower, security, logistics and other.

4.2.3 Information Products

Information Products are collections of information that represent the formal output of a business process and/or can be used as an input to other business processes. Information Products consists of several Information Elements and can be seen as any communications or representation of knowledge such as facts, data, or opinions in any medium or form.

4.2.3.1 IA Information

Information Assurance (IA) Information is a grouping of information products that are required to perform Information Assurance (IA).

4.2.3.2 SMC Information

Service Management and Control (SMC) Information is the set of information products needed to implement and enforce SMC policies at all levels.

4.2.3.3 Intent and Guidance

Intent & Guidance represents the intentions and key directions issued by a leader.

Intent provides the keystone doctrine for the planning, execution and support of Allied joint operations. The intent defines the end-state in relation to the factors of mission; adversary, operating environment, terrain, forces, time and preparation for future operations. As such, it addresses what results are expected from the operation, how these results might enable transition to future operations, and how, in broad terms, the Commander expects the force to achieve those results. Its focus is on the force as a whole. Additional information on how the force will achieve the desired results is provided only to clarify the Commander's intentions.

Guidance provides instructions and advice on the execution of plans, operations, and support activities of Allied joint operations.

4.2.3.4 Rules and Measures

Rules & Measures capture constraints issued by authorities and determine how compliance with those constraints is measured. Rules are authoritative statements of what to do or not to do in a specific situation, issued by an appropriate person or body. It clarifies, demarcates, or interprets a law or policy. Measures indicate the degree or grade of excellence expressed in terms of performance or effectiveness.

4.2.3.5 Plans

Plans are procedures, decided after consideration at the appropriate level of command, to execute a mission or task by military forces, their military organizations and units, in order to achieve objectives before or during a conflict. Military plans are generally produced in accordance with the military doctrine of the troops involved.

4.2.3.6 Tasking and Orders

Tasking & Orders represent the assigned of work to an individual or group of individuals by a leader. Tasking is the process of translating the allocation into orders, and passing these orders to the units involved. Orders are communications - written, oral, or by signal - which conveys instructions from a superior to a subordinate. Each order normally contains sufficient detailed instructions to enable the executing agency to accomplish the mission successfully.

4.2.3.7 Situational Awareness

Situational Awareness (SA) is the perception of environmental elements with respect to time and/or space, the comprehension of their meaning, and the projection of their status, affecting the safe, expedient and effective conduct of the mission. It involves being aware of what is happening in the vicinity to understand how information, events, and one's own actions will impact goals and objectives, both immediately and in the near future. Situation Awareness provides critical information to decision-makers in complex, dynamic areas such as military command and control.

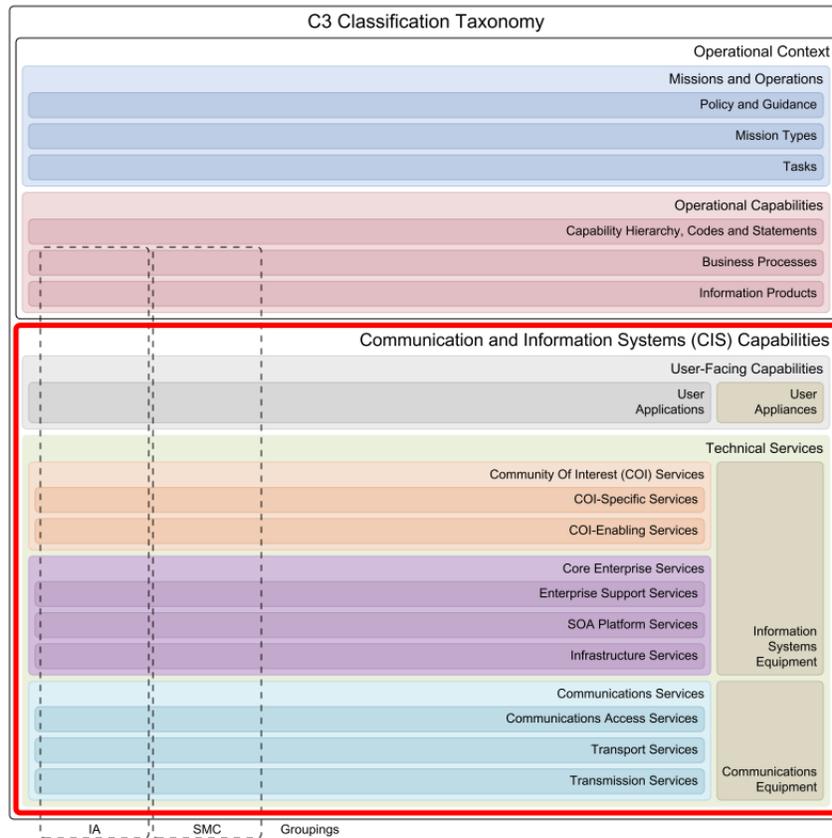
4.2.3.8 Resource Status

Resource Status indicates the current state or condition of resources. This then provides information about any entity available for use, such as ammunition, equipment, manpower, funding, etcetera.

4.2.3.9 Requests and Responses

Requests & Responses are information products used in business process transactions. Requests are acts of asking for someone or something while a response constitutes a reply or a reaction to a request. Responses are replies or answers to certain request, or reactions to specific stimuli.

5 CIS Capabilities

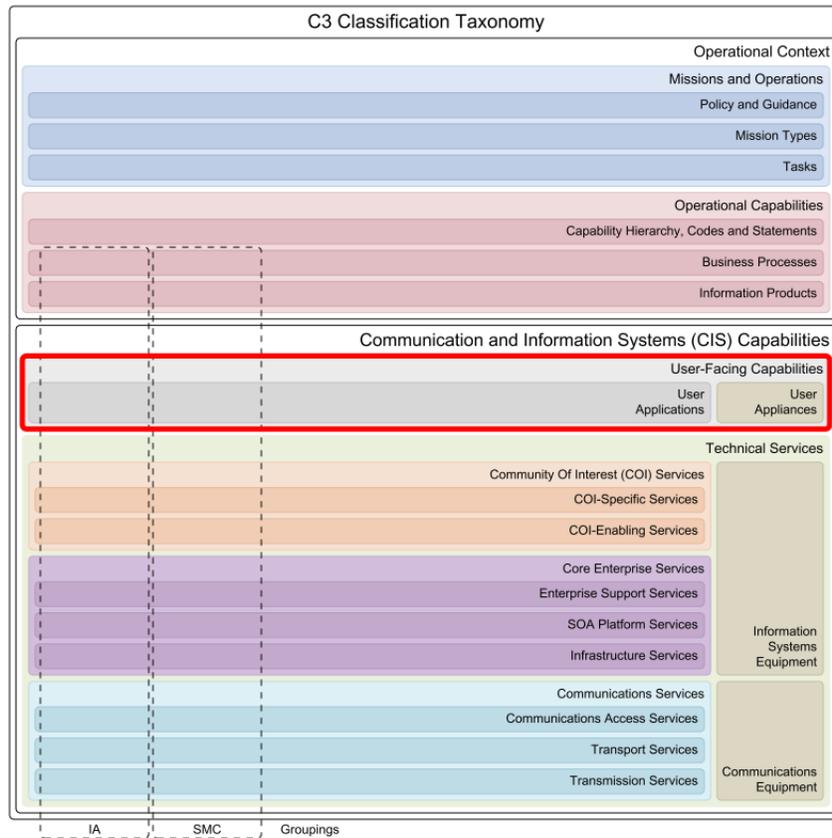


Communication and Information System (CIS) Capabilities describe the DOTMLPFI (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability) solutions to meet NATO's information and communication needs in support of Missions and Operations. CIS is a collective term for communication systems and information systems.

Communication Systems are systems or facilities for transferring data between persons and equipment. They usually consists of a collection of communication networks, transmission systems, relay stations, tributary stations and terminal equipment capable of interconnection and inter-operation so as to form an integrated whole. These individual components must serve a common purpose, be technically compatible, employ common procedures, respond to some form of control and generally operate in unison.

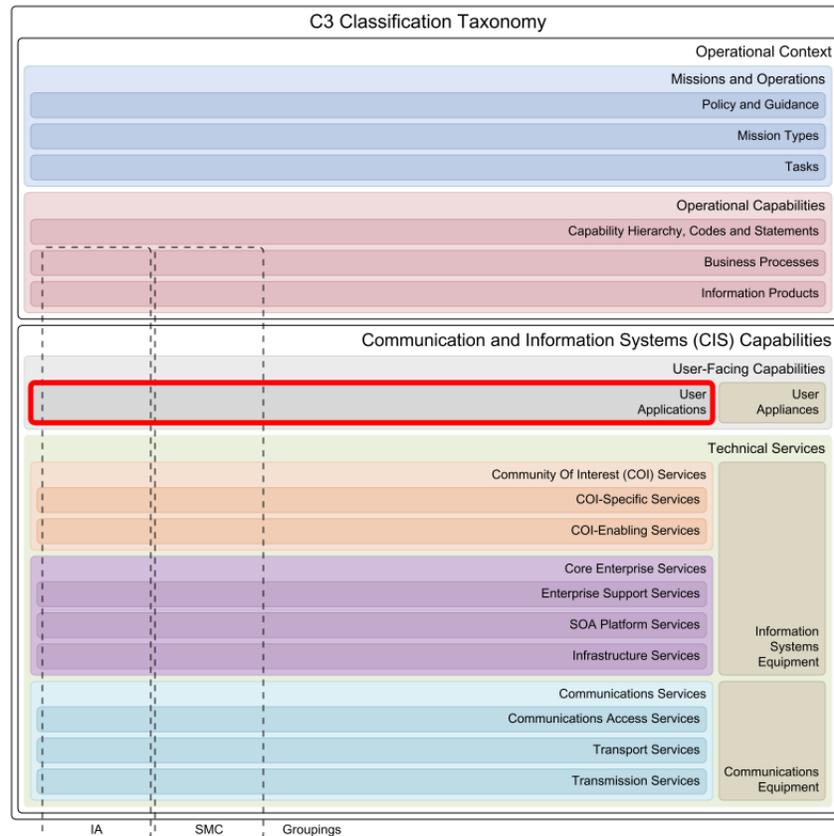
Information Systems are integrated sets of components for collecting, storing, and processing data for delivering information, knowledge, and digital products. Organizations and individuals rely on information systems to manage their operations, compete in the marketplace, supply services, and augment personal lives.

5.1 User-Facing Capabilities



User-Facing Capabilities express the requirements for the interaction between end users and all CIS Capabilities, in order to process Information Products in support of Business Processes. User-Facing Capabilities incorporate the User Appliances, as well as the User Applications that run on those appliances.

5.1.1 User Applications



User Applications - also known as application software, software applications, applications or "apps" - provide the computer software components designed to help an end user perform singular or multiple related tasks. Within the C3 Classification Taxonomy and based on TOGAF 9, the objective of this class is to "define the major kinds of application systems necessary to process the data and support the business". The goal is to define what kinds of User Applications are relevant to the enterprise, and what those applications need to do in order to manage data (process Information Products) and to present information to the human and computer actors in the enterprise (support Business Processes).

User Applications provide the logical interface between human and automated activities. Their description identifies information and functional requirements for the end user to perform specific tasks. The application's context within a Community Of Interest (COI) determines whether information and/or function is the primary discriminator used to build the NATO Network Enabled Capability (NNEC) compliant application hierarchy.

User Applications run on User Appliances. The applications and their capabilities are defined without reference to particular technologies. The applications are stable and relatively unchanging over time, whereas the technology used to implement them will change over time, based on technological developments and changing business needs.

5.1.1.1 IA Applications

Information Assurance (IA) Applications provide the user interfaces to implement, enforce and monitor IA policies. These applications are the overlap between User Applications and the Information Assurance domain, meaning that they exist in both the User Applications class and the IA grouping (i.e. the logical grouping of critical components that jointly implement the tenets of NATO's Information Assurance policies).

5.1.1.2 SMC Applications

Service Management and Control (SMC) Applications manage, control and monitor services in all layers of the network-enabled enterprise based on centralized and de-centralized business models, and provide the user interfaces to implement, enforce and monitor SMC policies. These applications are the overlap between User Applications and the Service Management and Control domain, meaning that they exist in both the User Applications class and the SMC

grouping (i.e the logical grouping of critical components that jointly provide the tools to manage and control a distributed and federated service-oriented enterprise).

5.1.1.3 Joint COI Applications

Joint Community of Interest (COI) Applications enable users to collect, process, present and distribute information that supports the major functions of joint operations. Joint Operations are the set of military activities that are conducted by joint forces and those service forces employed in specified command relationships with each other, which of themselves do not establish joint forces. In case these joint operations are carried out by military forces of two or more nations, these are known as Combined Joint Operations.

Examples of Joint COI Applications include targeting, collection management, and operational planning.

5.1.1.4 Air COI Applications

Air Community of Interest (COI) Applications enable users to collect, process, present and distribute information that supports the major functions of air operations. Air Operations are the set of military activities that are conducted by air forces to attain and maintain a desired degree of control of the air, influence events on land and along coastal areas, and, as required, support land, maritime and space operations.

5.1.1.5 Land COI Applications

Land Community of Interest (COI) Applications enable users to collect, process, present and distribute information that supports the major functions of land operations. Land Operations are the set of military activities that are conducted by land forces to attain and maintain a desired degree of control within the Area of Responsibility (AOR) on land, and, as required, support maritime, air and space operations.

Examples of Land COI Applications include manoeuvre, fire support, air defence, command and control, intelligence, mobility and survivability, and combat service support.

5.1.1.6 Maritime COI Applications

Maritime Community of Interest (COI) Applications enable users to collect, process, present and distribute information that supports the major functions of maritime operations. Maritime Operations are the set of military activities that are conducted by maritime air, surface, sub-surface and amphibious forces to attain and maintain a desired degree of control of the surface, sub-surface, and air above the sea, influence events ashore, and, as required, support land, air and space operations.

5.1.1.7 Space COI Applications

Space Community of Interest (COI) Applications" enable users to collect, process, present and distribute information that supports the major functions of space operations. Space Operations are the set of military activities that are conducted by dedicated forces to attain and maintain a desired degree of control of the upper atmosphere and space, influence events on earth, and, as required, support land, maritime and air operations.

5.1.1.8 Special Operations COI Applications

Special Operations Community of Interest (COI) Applications enable users to collect, process, present and distribute information that supports the major functions of special operations. Special Operations are the set of military activities that are conducted by specially designated, selected, organised, trained, and equipped forces using operational techniques and modes of employment not standard to conventional forces, that are planned and executed independently or in coordination with operations of conventional forces, and, as required, support land, maritime and air operations.

5.1.1.9 JISR COI Applications

Joint Intelligence, Reconnaissance and Surveillance (JISR or Joint ISR) Community of Interest (COI) Applications enable users to collect, process, present and distribute information for intelligence support to operations. Intelligence Support is the set of military activities that are undertaken to receive commander's direction, proactively collect information, analyse it, produce useful predictive intelligence and disseminate it in a timely manner to those who need to know.

5.1.1.10 Logistics COI Applications

Logistics Community of Interest (COI) Applications enable users to collect, process, present and distribute information that provides logistics support to operations. Logistics is the set of (military) activities that are undertaken for the planning and carrying out of the movement, sustainment, and maintenance of forces.

In its most comprehensive sense, logistics support comprises those aspects of military operations which deal with:

- design and development, acquisition, storage, transport, distribution, maintenance, evacuation and disposition of material,
- movement planning and transport of personnel and equipment,
- acquisition or construction, maintenance, operations and disposition of facilities,
- acquisition or furnishing of services, and
- medical and health service support.

5.1.1.11 EW COI Applications

Electronic Warfare (EW) Community of Interest (COI) Applications enable users to collect, process, present and distribute information that supports the major functions of Electronic Warfare operations. Electronic Warfare is the set of military activities that are conducted by designated forces to exploit the electromagnetic spectrum by interception and identification of emissions, by preventing hostile use of the spectrum, and by actions to ensure its effective use by friendly forces in support of operations.

Electronic Warfare COI Applications will be used to plan, coordinate, and monitor Electronic Support Measures (ESM), Electronic Countermeasures (ECM), and Electronic Protection Measures (EPM). These applications will be used by the Joint Electronic Warfare Centre staff and Electronic Warfare staff at joint and component command levels.

5.1.1.12 Environmental COI Applications

Environmental Community of Interest (COI) Applications enable users to collect, process, present and distribute information for environmental support to operations. Environmental Support is the set of (military) activities that are undertaken to systematically observe and report the military significant aspects of the meteorological, hydrographic, oceanographic, and geographic characteristics of the area of operations.

5.1.1.13 Missile Defence COI Applications

Missile Defence (MD) Community of Interest (COI) Applications enable users to collect, process, present and distribute information that supports the major functions of Missile Defence operations. Missile Defence is the set of military activities that are conducted by designated forces to protect the NATO populations, territory or forces against attacks by ballistic missiles, and to minimize the effects of these attacks.

5.1.1.14 CIMIC COI Applications

Civil-Military Co-operation (CIMIC) Community of Interest (COI) Applications enable users to collect, process, present and distribute information that supports the major functions of civil-military cooperation support to operations. CIMIC is the set of (military) activities that are undertaken to coordinate and cooperate, in support of the mission, between NATO commanders and civil actors, including the national population and local authorities, as well as international, national and non-governmental organisations and agencies.

5.1.1.15 CBRN COI Applications

Chemical, Biological, Radiological, and Nuclear (CBRN) Community of Interest (COI) Applications enable users to collect, process, present and distribute information that supports the major functions of CBRN Defence operations. CBRN Defence is the set of military activities that are conducted by forces to protect the NATO populations, territory or forces against attacks with CBRN weapons or agents, and to minimize the effects of these attacks.

CBRN COI Applications provide decisions makers with accurately display of the CBRN environment in order to execute a comprehensive threat and risk analysis, which include information on own forces' CBRN capabilities and information on hostile capabilities and threats, allowing the creation of CBRN estimates and the CBRN annex to the operational plan.

5.1.1.16 ETEE COI Applications

Education, Training, Exercises and Evaluation (ETEE) Community of Interest (COI) Applications enable users to collect, process, present and distribute information for ETEE support to operations. ETEE is the set of (military) activities that are conducted to attain and maintain the required standards for readiness and operational capabilities for NATO, national and multinational forces through education, individual and collective training, exercises and evaluation. In this context, ETEE COI Applications directly support the education, training, and exercise of Strategic Command staff and NATO command forces, and the conduct of independent operational assessments.

5.1.1.17 CIS COI Applications

Communication and Information Systems (CIS) Community of Interest (COI) Applications enable users to collect, process, present and distribute information for CIS support to operations. CIS Support is the set of military activities that are undertaken to install, configure, operate, manage and control military services and systems for communications and information processing and handling.

Historically, the first military communications had the form of sending/receiving simple signals, and the first distinctive tactics of military communications were called Signals, while units specializing in those tactics received the Signal Corps name. And still today, when the COI is involved in high-tech communications and information systems, the field of expertise is still referred to as Signals in some Nations.

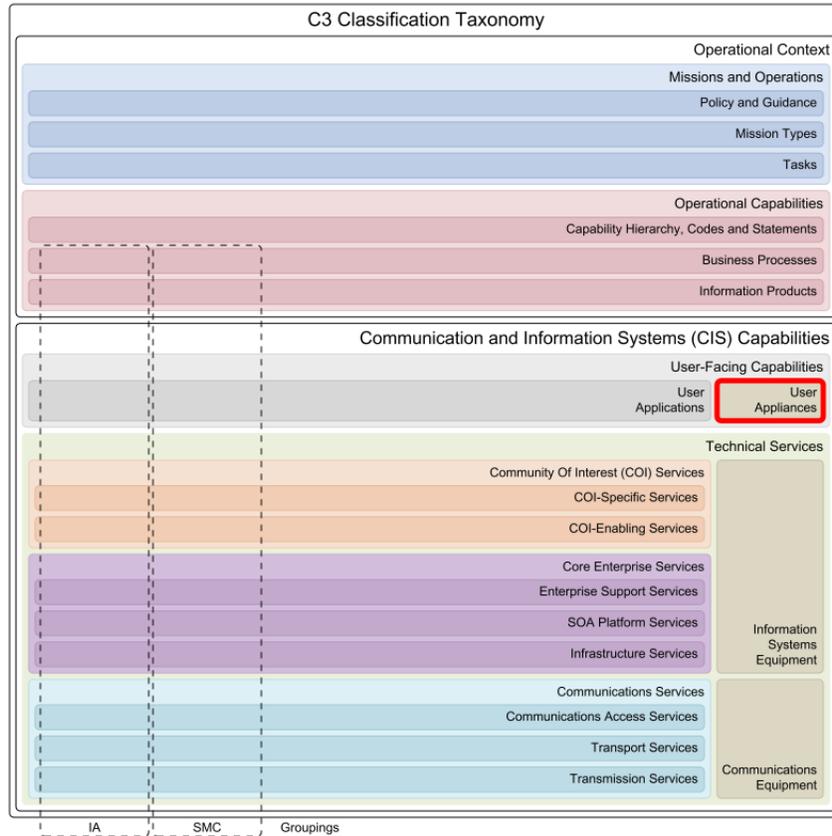
5.1.1.18 Modeling and Simulation COI Applications

Modeling and Simulation (M) Community of Interest (COI) Applications enable users to collect, process, present and distribute information for modeling and simulation support to operations. Modeling and Simulation are the set of (military) activities that are undertaken to use models, including emulators, prototypes, simulators, and stimulators, either statically or over time, to develop data as a basis for making operational or managerial decisions. It is important to recognize that assumptions, conceptualizations, and implementation constraints influence the practical results of simulations, while proper use of M techniques and procedures can still produce invaluable contributions to military decision making.

5.1.1.19 Generic Applications

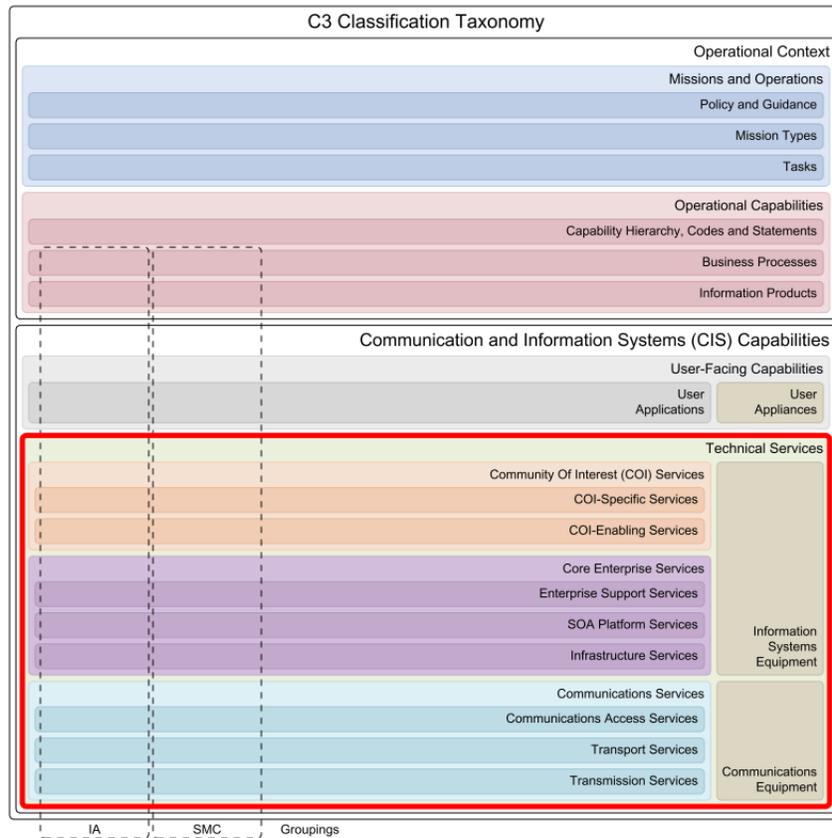
Generic Applications enable users to collect, process, present and distribute information for generic support to operations or routine administrative tasks.

5.1.2 User Appliances



User Appliances provide the physical interfaces between end users and a provided suite of User Applications. User Appliances are instruments, apparatuses and/or devices for a particular purpose or use. User Appliances support various environments, which will have implications for ergonomics, form factors, physical and electrical specifications, and more. Examples of User Appliances are telephones, computers, laptops, tablets and peripherals (I/O units) including: terminals, card readers, optical character readers, magnetic tape units, mass storage devices, card punches, printers, computer output to microform converters (COM), video display units, data entry devices, teletypes, teleprinters, plotters, scanners, or any device used as a terminal to a computer and control units for these devices.

5.2 Technical Services

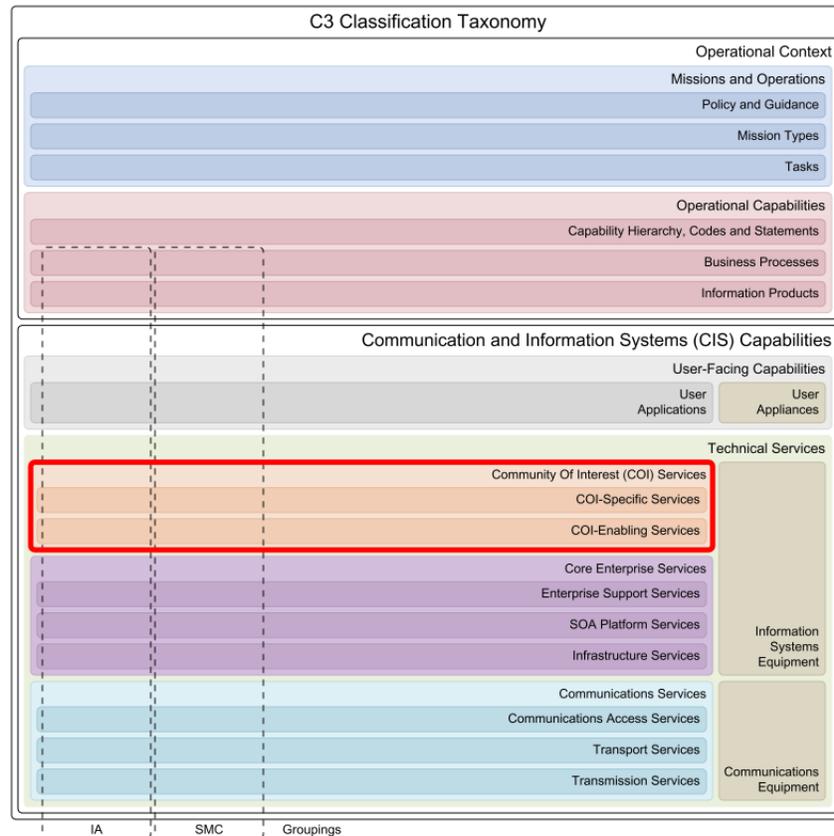


Technical Services express the requirements for a set of related software and hardware functionalities that can be reused for different purposes, together with the policies that should control their usage. These requirements are derived from the operational needs expressed by the collection of User-Facing Capabilities. Inherently, the Technical Services must support all NATO Mission Types.

Technical Services are implemented in a federated model that allows NATO and the Nations to jointly provide a robust and secure platform on top of which powerful User Applications can be run. Thus the Technical Services provide the foundation for the NATO Network Enabled Capability (NNEC). They must implement agreed and open standards, must exhibit plug-and-play properties, and must be transparent to operational users.

The complete collection of Technical Services is often referred to as the Technical Services Framework (TSF) or NNEC Services Framework (NSF).

5.2.1 Community Of Interest (COI) Services



Communities of Interest (COI) Services support one or many collaborative groups of users with shared goals, interests, missions or business processes. These services are primarily meant for COI Application or Service consumption.

5.2.1.1 COI-Specific Services

Community of Interest (COI)-Specific Services provide specific functionality as required by particular C3 user communities in support of NATO operations, exercises and routine activities. These COI-Specific Services were previously also referred to as "functional services" or "functional area services".

5.2.1.1.1 COI-Specific IA Services

Community of Interest (COI)-Specific Information Assurance (IA) Services provide the necessary means to implement and enforce IA policies at the COI-specific level. These services are the overlap between COI-Specific Services and the Information Assurance domain, meaning that they exist in both the COI-Specific Services class and the IA grouping.

5.2.1.1.2 COI-Specific SMC Services

Community of Interest (COI)-Specific Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the COI-specific level. These services are the overlap between COI-Specific Services and the Service Management and Control domain, meaning that they exist in both the COI-Specific Services class and the SMC grouping.

5.2.1.1.3 Joint COI Services

Joint Community of Interest (COI) Services" provide unique computing and information services in support of Joint Operations. Joint Operations are the set of military activities that are conducted by joint forces and those service forces employed in specified command relationships with each other, which of themselves do not establish joint forces. In case these joint operations are carried out by military forces of two or more nations, these are known as Combined Joint Operations.

5.2.1.1.4 Air COI Services

Air Community of Interest (COI) Services provide unique computing and information services in support of Air Operations. Air Operations are the set of military activities that are conducted by air forces to attain and maintain a desired degree of control of the air, influence events on land and along coastal areas, and, as required, support land, maritime and space operations.

5.2.1.1.5 Land COI Services

Land Community of Interest (COI) Services provide unique computing and information services in support of Land Operations. Land Operations are the set of military activities that are conducted by land forces to attain and maintain a desired degree of control within the Area of Responsibility (AOR) on land, and, as required, support maritime, air and space operations.

5.2.1.1.6 Maritime COI Services

Maritime Community of Interest (COI) Services provide unique computing and information services in support of Maritime Operations. Maritime Operations are the set of military activities that are conducted by maritime air, surface, sub-surface and amphibious forces to attain and maintain a desired degree of control of the surface, sub-surface, and air above the sea, influence events ashore, and, as required, support land, air and space operations.

5.2.1.1.7 Space COI Services

Space Community of Interest (COI) Services provide unique computing and information services in support of Space Operations. Space Operations are the set of military activities that are conducted by dedicated forces to attain and maintain a desired degree of control of the upper atmosphere and space, influence events on earth, and, as required, support land, maritime and air operations.

5.2.1.1.8 Special Operations COI Services

Special Operations Community of Interest (COI) Services provide unique computing and information services in support of Special Operations. Special Operations are the set of military activities that are conducted by specially designated, selected, organised, trained, and equipped forces using operational techniques and modes of employment not standard to conventional forces, that are planned and executed independently or in coordination with operations of conventional forces, and, as required, support land, maritime and air operations.

5.2.1.1.9 JISR COI Services

Joint Intelligence, Surveillance and Reconnaissance (JISR or Joint ISR) Community of Interest (COI) Services provide unique computing and information services for intelligence support to operations. Intelligence Support is the set of military activities that are undertaken to receive commander's direction, proactively collect information, analyse it, produce useful predictive intelligence and disseminate it in a timely manner to those who need to know.

5.2.1.1.10 Logistics COI Services

Logistics Community of Interest (COI) Services" provide unique computing and information services for logistics support to operations. Logistics is the set of (military) activities that are undertaken for the planning and carrying out of the movement, sustainment, and maintenance of forces.

5.2.1.1.11 EW COI Services

Electronic Warfare (EW) Community of Interest (COI) Services provide unique computing and information services in support of Electronic Warfare operations, e.g. tools for EW threat assessment, response planning, and coordination of force deployment, operational reporting, and cueing to other functional services. Electronic Warfare is the set of military activities that are conducted by designated forces to exploit the electromagnetic spectrum by interception and identification of emissions, by preventing hostile use of the spectrum, and by actions to ensure its effective use by friendly forces in support of operations.

5.2.1.1.12 Environmental COI Services

Environmental Community of Interest (COI) Services provide unique computing and information services for environmental support to operations. Environmental Support is the set of (military) activities that are undertaken to systematically observe and report the military significant aspects of the meteorological, hydrographic, oceanographic, and geographic characteristics of the area of operations.

At present, environmental information can only be managed and exploited using isolated stove-piped processes and systems with limited interoperability between environmental information systems and other services. In addition, management of different types of environmental information is not standardised. This lack of synergy in the provision and exploitation of environmental information can lead to inappropriate decisions, incorrect tasking or utilisation of assets that may contribute to mission failure. One of the main information products provided by the Environmental COI Services is the "Recognised Environmental Picture" (REP).

5.2.1.1.13 Missile Defence COI Services

Missile Defence (MD) Community of Interest (COI) Services provide unique computing and information services in support of Missile Defence operations. Missile Defence is the set of military activities that are conducted by designated forces to protect the NATO populations, territory or forces against attacks by ballistic missiles, and to minimize the effects of these attacks.

5.2.1.1.14 CIMIC COI Services

Civil-Military Co-operation (CIMIC) Community of Interest (COI) Services provide unique computing and information services in support of civil-military cooperation support to operations. CIMIC is the set of (military) activities that are undertaken to coordinate and cooperate, in support of the mission, between NATO commanders and civil actors, including the national population and local authorities, as well as international, national and non-governmental organisations and agencies.

5.2.1.1.15 CBRN COI Services

Chemical, Biological, Radiological, and Nuclear (CBRN) Community of Interest (COI) Services provide unique computing and information services in support of CBRN Defence operations. CBRN Defence is the set of military activities that are conducted by forces to protect the NATO populations, territory or forces against attacks with CBRN weapons or agents, and to minimize the effects of these attacks.

5.2.1.1.16 ETEE COI Services

Education, Training, Exercises and Evaluation (ETEE) Community of Interest (COI) Services provide unique computing and information services for ETEE support to operations. ETEE is the set of (military) activities that are conducted to attain and maintain the required standards for readiness and operational capabilities for NATO, national and multinational forces through education, individual and collective training, exercises and evaluation. In this context, ETEE COI Applications directly support the education, training, and exercise of Strategic Command staff and NATO command forces, and the conduct of independent operational assessments.

5.2.1.1.17 Modeling and Simulation COI Services

Modeling and Simulation (M) Community of Interest (COI) Services provide unique computing and information services for modeling and simulation support to operations. Modeling and Simulation are the set of (military) activities that are undertaken to use models, including emulators, prototypes, simulators, and stimulators, either statically or over time, to develop data as a basis for making operational or managerial decisions.

Modeling and Simulation COI Services organize and utilize specific applications, which are distributed but logically connected by a network and open standards, to enable increased interoperability and to conserve resources. They are unique from other information technology (IT) services in that they expose assumptions and constraints to support composability of models.

5.2.1.1.18 CIS COI Services

Communication and Information Systems (CIS) Community of Interest (COI) Services provide unique computing and information services in support for CIS support to operations. CIS Support is the set of military activities that are undertaken to install, configure, operate, manage and control military services and systems for communications and information processing and handling.

5.2.1.2 COI-Enabling Services

Community of Interest (COI)-Enabling Services provide COI-dependant functionality required by more than one communities of interest. They are similar to Enterprise Support Services in that they provide building blocks for domain-specific service development. The distinction between the two is that Enterprise Support Services provide generic COI-independent capabilities for the entire enterprise (e.g. collaboration and information management services) and COI-Enabling Services provide those COI-dependant services that are typically shared by a larger group of COIs (e.g. operational planning and situational awareness capabilities).

5.2.1.2.1 COI-Enabling IA Services

Community of Interest (COI)-Enabling Information Assurance (IA) Services provide the necessary means to implement and enforce IA policies at the COI-enabling level. These services are the overlap between COI-Enabling Services and the Information Assurance domain, meaning that they exist in both the COI-Enabling Services class and the IA grouping.

5.2.1.2.2 COI-Enabling SMC Services

Community of Interest (COI)-Enabling Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the COI-enabling level. These services are the overlap between COI-Enabling Services and the Service Management and Control domain, meaning that they exist in both the COI-Enabling Services class and the SMC grouping.

5.2.1.2.3 Operational Planning Services

Operational Planning Services provide operational plans and procedures, decided after consideration at the appropriate level of command, to execute a mission or task by military forces, their military organizations and units, in order to achieve objectives before or during a conflict. Operational Planning begins with the end state in mind, providing a unifying purpose around which actions and resources are focused.

5.2.1.2.4 Tasking and Order Services

Tasking and Order Services develop and manage operational orders, tasking and associated functionality (e.g. resource availability, rules of engagement, etc).

5.2.1.2.5 Situational Awareness Services

Situational Awareness (SA) Services provide the situational knowledge required by a military commander to plan operations and exercise command and control. This is the result of the processing and presentation of information comprehending the operational environment - the status and dispositions of friendly, adversary, and non-aligned actors, as well as the impacts of physical, cultural, social, political, and economic factors on military operations.

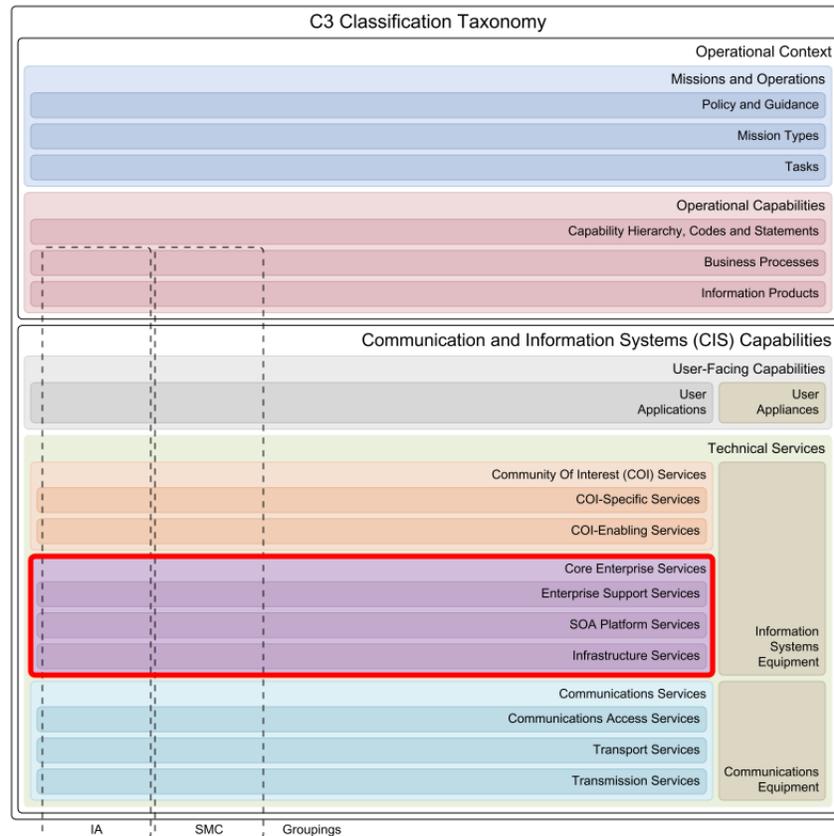
5.2.1.2.6 Business Support Services

Business Support Services provide shared services to those COI-specific applications and services that are primarily responsible for support, logistics, human resources, financial management and other Enterprise Resource Planning functions.

5.2.1.2.7 Modeling and Simulation Services

Modeling and Simulation (M) Services enable the integration of M services in other communities of interest, and to exploit the output of M activities in other COI Services (e.g. the provision of simulation results to improve statistical appreciation of Situational Awareness).

5.2.2 Core Enterprise Services



Core Enterprise Services (CES) provide generic, domain independent, technical functionality that enables or facilitates the operation and use of Information Technology (IT) resources, independent of issues concerning communications, Information Assurance (IA), and Service Management and Control (SMC).

In this case the IT resources refer to: data; networked IT-equipment (i.e. hardware, such as servers, workstations, printers, routers and switches, including cables; and IT environment equipment, such as power units and server room cooling equipment; as well as software (bespoke or common and generic, embedded or not).

5.2.2.1 Enterprise Support Services

Enterprise Support Services are a set of Community Of Interest (COI) independent services that must be available to all enterprise members. Enterprise Support Services facilitate other service and data providers on the enterprise network by providing and managing underlying capabilities to facilitate collaboration and information management for end-users. Enterprise Support Services are enablers used by other services and users across the whole network-enabled enterprise, acting as “building blocks” for developing more sophisticated COI services and applications.

5.2.2.1.1 Enterprise Support IA Services

Enterprise Support Information Assurance (IA) Services provide a foundation to implement uniform, consistent, interoperable and effective web service security. They also provide the necessary means to implement and enforce IA policies at the enterprise support level. These services are the overlap between Enterprise Support Services and the Information Assurance domain, meaning that they exist in both the Enterprise Support Services class and the IA grouping.

5.2.2.1.2 Enterprise Support SMC Services

Enterprise Support Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the enterprise support level. These services are the overlap between Enterprise Support Services and the Service Management and Control domain, meaning that they exist in both the Enterprise Support Services class and the SMC grouping.

5.2.2.1.3 Unified Communication and Collaboration Services

Unified Communication and Collaboration Services provide users with a range of interoperable collaboration capabilities, based on commercial standards that are secure and fulfil NATO and Coalition operational requirements. They will enable real-time situational updates to time-critical planning activities between coalition partners, communities of interest (e.g. the Intel community or the Logistics community), and NATO and National agencies. Levels of collaboration include awareness, shared information, coordination and joint product development.

5.2.2.1.4 Information Management Services

Information Management Services provide technical services "...to direct and support the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organisation", para-phrased from the is referring to::NATO Information Management Policy (NIMP). These services support organisations, groups, individuals and other technical services with capabilities to organise, store and retrieve information (in any format, structured or unstructured) through services and managed processes, governed by policies, directives, standards, profiles and guidelines.

5.2.2.1.5 Geospatial Services

Geospatial Services deliver network-based access to quality raster, vector and terrain data, available in varying degrees of format and complexity. Geospatial Services form a distinct class of information services through their unique requirements for collecting, converting, storing, retrieving, processing, analysing, creating, and displaying geographic data. The generic nature of Geospatial Services - "organizing information by location" - is interdisciplinary and not specific to any Community of Interest (COI) or application. Nevertheless highly specialized services are also required, based on specialised needs such as enabling unique processes such as transformation of geographic coordinates, querying catalogues.

Geospatial location and time are integral to nearly all aspects of the military environment. Geography is a foundational property for modeling and representing the battlespace in a coherent, intuitive way. Geographic phenomena fall into two broad categories: discrete and continuous. Discrete phenomena are recognizable objects that have relatively well-defined boundaries or spatial extent (e.g. buildings, streams, and measurement stations). Continuous phenomena vary over space and have no specific extent (e.g. temperature, soil composition, and elevation). A value or description of a continuous phenomenon is only meaningful at a particular position in space (and possibly time). Temperature, for example, takes on specific values only at defined locations, whether measured or interpolated from other locations. These concepts are not mutually exclusive. In fact, many components of the landscape may be viewed alternatively as discrete or continuous.

Historically, geographic information has been treated in terms of two fundamentally different types: vector data and raster data. Vector data typically deal with discrete phenomena, each of which is conceived of as a feature. Raster data deal with real world phenomena that vary continuously over space.

5.2.2.2 SOA Platform Services

Service Oriented Architecture (SOA) Platform Services provide a foundation to implement web-based services in a loosely coupled environment, where flexible and agile service orchestration is a requirement. They offer generic building blocks for SOA implementation (e.g. discovery, message busses, orchestration, information abstraction and access, etc.) and can be used as a capability integration platform in a heterogeneous service-provisioning ecosystem.

5.2.2.2.1 SOA Platform IA Services

Service Oriented Architecture (SOA) Platform Information Assurance (IA) Services provide a foundation to implement uniform, consistent, interoperable and effective web service security. They also provide the necessary means to implement and enforce IA policies at the SOA platform level. These services are the overlap between SOA Platform Services and the Information Assurance domain, meaning that they exist in both the SOA Platform Services class and the IA grouping.

5.2.2.2.2 SOA Platform SMC Services

Service Oriented Architecture (SOA) Platform Service Management and Control (SMC) Services provide a suite of capabilities needed to ensure that SOA services are up and running, accessible and available to users, protected and secure, and that they are operating and performing within agreed upon parameters. They also provide the necessary means to implement and enforce SMC policies at the SOA platform level. These services are the overlap between SOA Platform

Services and the Service Management and Control domain, meaning that they exist in both the SOA Platform Services class and the SMC grouping.

5.2.2.2.3 Message-oriented Middleware Services

Message-Oriented Middleware Services provide functionality to support the exchange of messages (data structures) between data producer and consumer services, independent of the message format (XML, binary, etc.) and content.

Message-Oriented Middleware Services support the one-to-one and one-to-many message exchange topologies. They support the following synchronous, asynchronous, and long running modes of delivery. They support routing, addressing, and caching. And they support the message exchange patterns for request/response, publish/subscribe, for solicit response (polling for response), and for fire and forget.

5.2.2.2.4 Web Platform Services

Web Platform Services provide a suite of functionalities that can be used to support the deployment of SOA services onto a common web-based application platform.

5.2.2.2.5 Information Platform Services

Information Platform Services provide capabilities required to manage the enterprise information sphere. They include generic services that deal with information transformation, provision and maintenance including quality assurance.

5.2.2.2.6 Composition Services

Composition Services will access and fuse data and behavior on demand, and return a single result to the consumer. Composition Services can, from queues and/or in batch, provide a set of data transforms and routings to transactions that can serve machine-to-machine business processes.

A service composition is a coordinated aggregate of services. The consistent application of service-orientation design principles leads to the creation of services with functional contexts that are agnostic to any one business process. These agnostic services are therefore capable of participating in multiple service compositions. Services are expected to be capable of participating as effective composition members, regardless of whether they need to be immediately enlisted in a composition.

There are two aspects of composition: composition synthesis is concerned with synthesizing a specification of how to coordinate the component services to fulfil the client request; and orchestration, is concerned with how to actually achieve the coordination among services, by executing the specification produced by the composition synthesis and by suitably supervising and monitoring that execution.

5.2.2.2.7 Mediation Services

A mediator is an entity that acts as an intermediate broker between communication parties which are incompatible in terms of their message formats, communication protocols, policies, or communication paradigm. Data mediation comprises automated capabilities for conversion, fusion and re-arrangement of data in order to overcome the discrepancies between incompatible participants.

Mediation Services provide a middle layer between incompatible producers of information and consumers of information. Mediation services process the data of the information producer and transform it into a representation which is understandable for the consumer. In doing so Mediation Services bridge the gap between both parties, enabling interaction between them which has not been possible beforehand.

Data mediation involves three fundamental aspects of communication:

- the data format which defines how information is represented,
- the communication protocol which defines how pieces of data are exchanged between communication entities, and
- message exchange policies which define constraints and non-functional restrictions on the way messages are exchanged.

The act of transforming the data requires not only a syntactic (i.e. regarding the data format and structure) but in particular a semantic understanding of the data on both the data consumer and data producer side. For example, a simple mediation service that converts geographic data from a polar coordinate based format to Cartesian coordinate based format has to have – beside information of the syntactic formats – a semantic understanding (semantic model) of both coordinate

systems. The semantic models explain how a consumer should interpret a producer's information, i.e. what the producer's model means in terms of the consumer's model.

For correct transformation these semantic models must always exist, but can either be explicitly or implicitly used in the transformation process. Explicitly means that semantic models are present during the runtime of a mediation service as parameters, in the same way as the source data, i.e. as machine readable representations. Implicitly means that the semantic models are incorporated in the implementation of a mediator service during its design time, but are not represented at runtime as parameters when calling the mediator service. Typically, an implicit semantic model is one which needs to be agreed out-of-band by the developer of a transformation and is then hard-coded into the transformation process. Following this distinction between explicit and implicit semantics, the class of Mediation Services can be further divided into mediation services which make explicit or implicit use of the corresponding semantic models.

Mediation Services characterize a set or class of services. The functions which are described below are common to all members of the set of Mediation Services, i.e. any child service in the taxonomy should fulfill the functional requirements as stated in this article for the class of Mediation Services. A specialization/refinement of the functions is done in each specific sub-class of Mediation Services, e.g. Data Format Transform Services, respectively. The same applies to the non-functional requirements which apply to the entire set of Mediation Services, too.

5.2.2.3 Infrastructure Services

Infrastructure Services provide software resources required to host services in a distributed and federated environment. They include computing, storage and high-level networking capabilities that can be used as the foundation for data centre or cloud computing implementations.

Infrastructure Services in this taxonomy are aligned with "Infrastructure as a Service" (IaaS) concepts that are used and promoted by the Information Technology (IT) industry today as part of their Cloud Computing developments.

5.2.2.3.1 Infrastructure IA Services

Infrastructure Information Assurance (IA) Services provide the necessary means to implement and enforce information assurance policies at the infrastructure level. These services are the overlap between Infrastructure Services and the Information Assurance domain, meaning that they exist in both the Infrastructure Services class and the IA grouping.

5.2.2.3.2 Infrastructure SMC Services

Infrastructure Service Management and Control Services defines how Infrastructure Services are consumed by other services and users. ITILv3 principles are used to define the functions and processes. Infra SMC services manages the communication with other Level 1 SMC Services and exchanges information products between them and Business Processes. These services are the overlap between Infrastructure Services and the Service Management and Control domain, meaning that they exist in both the Infrastructure Services class and the SMC grouping.

Controlling involves translation and distribution of overall requirements to specific parameters.

Management involves:

- Receiving requirements from other Level1 SMC Services
- Receiving action orders from Business Processes
- Exchanging Information Products between SMC services and Business processes.

5.2.2.3.3 Infrastructure Processing Services

Infrastructure Processing Services provide shared access to physical and/or virtual computing resources in a data centre or cloud computing environment. They primarily provide Operating System (OS) capabilities to time-share computing resources (e.g. CPU, memory and input/output busses) between various tasks, threads or programs based on stated policies and algorithms.

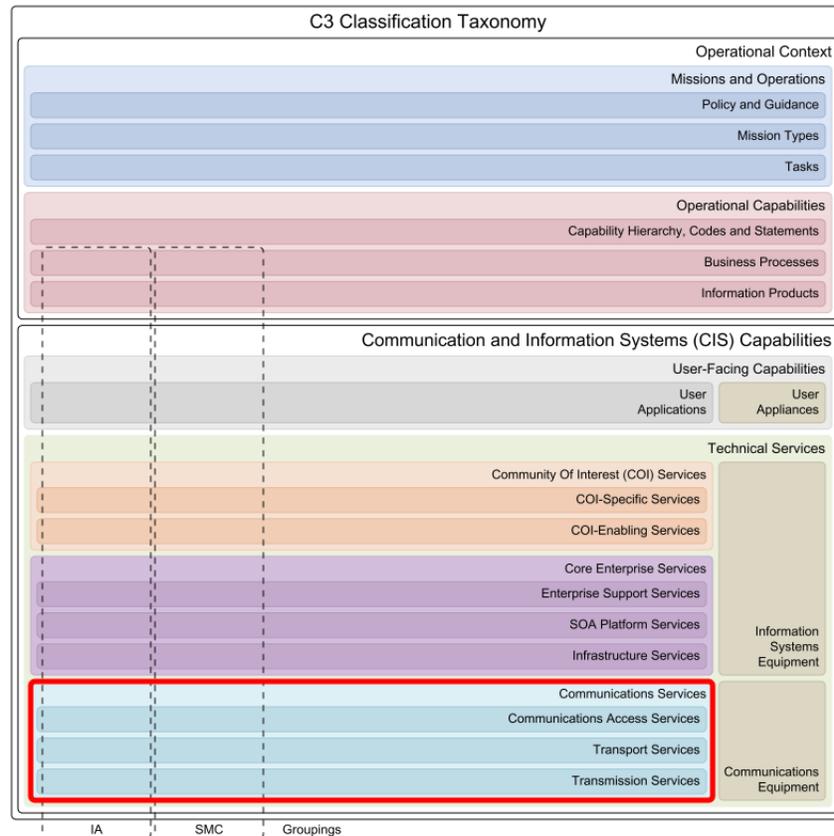
5.2.2.3.4 Infrastructure Storage Services

Infrastructure Storage Services provide access to shared physical and/or virtual storage components for data and information persistence. They offer data/information retention at different levels of complexity, ranging from simple block level access to sophisticated big data object storage with metadata or relational databases.

5.2.2.3.5 Infrastructure Networking Services

Infrastructure Networking Services provide access to high-level protocols and methods that fall into the realm of process-to-process communications across an Internet Protocol (IP) network. They are akin to components in the Open Systems Interconnection's (OSI) application layer but are limited to those services required for the infrastructure layer in that taxonomy. OSI application layer protocols such as those for e-mail and directory services are covered by other Core Enterprise Services.

5.2.3 Communications Services



Communications Services interconnect systems and mechanisms for the opaque transfer of selected data between or among access points, in accordance with agreed quality parameters and without change in the form or content of the data as sent and received.

5.2.3.1 Communications Access Services

Communications Access Services provide end-to-end connectivity of communications or computing devices. Communications Access Services can be interfaced directly to Transmission Services (e.g. in the case of personal communications systems) or to Transport Services, which in turn interact with Transmission Services for the actual physical transport.

Communications Access Services correspond to customer-facing communications services. As such, they can also be referred to as Subscriber Services, or Customer-Edge (CE) Services.

The Communications Access Services nomenclature is based on the type of end-to-end access service supported between the communications/computing devices.

5.2.3.1.1 Communications Access IA Services

Communications Access Information Assurance (IA) Services provide a foundation to implement and enforce IA policies at the communications access level. These services are the overlap between Communications Access Services and the Information Assurance domain, meaning that they exist in both the Communications Access Services class and the IA grouping.

5.2.3.1.2 Communications Access SMC Services

Communications Access Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the communications access level. These services are the overlap between Communications Access Services and the Service Management and Control domain, meaning that they exist in both the Communications Access Services class and the SMC grouping.

The Communications Access SMC Services are loosely based on the Information Technology Infrastructure Library (ITIL) Service Strategy. Examples of ITIL lifecycle process that can be employed are Strategy, Design, Transition, Operations, and Improvement.

5.2.3.1.3 Analogue Access Services

Analogue Access Services support the delivery or exchange of analogue signals over an analogue interface port, using encoding and/or compression to the Transport Services or directly, without manipulation, to the Transmission Services (e.g. wireless radio).

5.2.3.1.4 Digital (Link) Access Services

Digital (Link based) Access Services provide the delivery or exchange of digital signals (synchronous or asynchronous) over a digital interface port to the Transport Services or directly to the Transmission Service (e.g. modem port of a handheld SATCOM terminal).

5.2.3.1.5 Message-based Access Services

Message-based Access Services support the delivery or exchange of formatted messages either free text or tactical data link, through user appliances that are directly connected to a Transmission Service (e.g. the keypad of a VHF radio).

5.2.3.1.6 Circuit-based Access Services

Circuit-based Access Services support the delivery or exchange of raw user data, via fractional access to digital lines or circuits (e.g. ISDN BRI, fractional E1), directly to the end-user appliance (e.g. an ISDN phone) through terminal adapters, channel service units / data service units (CSU/DSU), multiplexers, etc., which in turn interface to Transport Services - after aggregation with other Communications Access Services - or directly to Transmission Services (e.g. ISDN port of an Inmarsat SATCOM terminal).

5.2.3.1.7 Frame-based Access Services

Frame-based Access Services support the transparent delivery or exchange of user data, end-to-end, formatted and encapsulated into frames (e.g. Ethernet frames, PPP frames). The frames are delivered by the user end-point, adapted transported by the relevant Transport Service or Transmission Service, and dispatched to the Communications Access Service at the other end-point(s), transparently (i.e. frame contents are not altered, and frame headers are not looked-up for switching purposes). In other words, user end-points are agnostic to the service class and type selected by the Service Provider, provided the delivery of frames end-to-end is seamless and does not interfere with protocols at the same layer.

5.2.3.1.8 Packet-based Access Services

Packet-based Access Services support the delivery or exchange of data (or digitised voice, video) encapsulated in IP packets.

5.2.3.1.9 Multimedia Access Services

Multimedia Access Services provide the interface with User-Facing Capabilities, as well as the adaptation (e.g. encoding and compression) of the media (e.g. voice, video, text) and the protocols employed for multimedia communication sessions (e.g. video-teleconferencing), for delivery and exchange over packet-based, frame-based, circuit-based, or digital (link)-based Communications Access Services.

5.2.3.2 Transport Services

Transport Services provide resource-facing services, providing metro and wide-area connectivity to the Communications Access Services that operate at the edges of the network. In that role, Transport Services interact with the Transmission Services using them as the physical layer fabric supporting the transfer of data over a variety of transmission bearers as and where needed.

The Transport Services nomenclature is based on the type of end-to-end transport service supported over and/or within the "Core Network" (e.g. WAN, PCN). Possible types include point-point, point-to-multipoint, multipoint-to-multipoint, routing/switching, multiplexing, etc.

5.2.3.2.1 Transport IA Services

Transport Information Assurance (IA) Services provide a foundation to implement and enforce IA policies at the communications transport level. These services are the overlap between Transport Services and the Information Assurance domain, meaning that they exist in both the Transport Services class and the IA grouping.

5.2.3.2.2 Transport SMC Services

Transport Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the communications transport level. These services are the overlap between Transport Services and the Service Management and Control domain, meaning that they exist in both the Transport Services class and the SMC grouping.

The Transport SMC Services are loosely based on the Information Technology Infrastructure Library (ITIL) Service Strategy. Examples of ITIL lifecycle process that can be employed are Strategy, Design, Transition, Operations, and Improvement.

5.2.3.2.3 Edge Transport Services

Edge Transport Services provide the delivery or exchange of traffic flows over different Transmission Services. The traffic flows are formatted and delivered by the Communications Access Services at the edges of the network. This "edge" in Edge Transport is the Wide Area Network (WAN) edge (i.e. the provider edge). In Protected Core Networking (PCN) terms, the edge can be considered as the entry point into the Protected Core.

The Edge Transport Services category can be broken down into service classes that closely follow the OSI stack. The main difference between Communication Access Services and Edge Transport Services is that the latter are resource-facing, and are streamlined for the efficient transfer of larger volumes of traffic resulting from the aggregation of multiple Communications Access Services.

Edge Transport Services can implement encryption for link security and traffic flow confidentiality protection (LINKSEC).

5.2.3.2.4 Core Network Services

Core Network Services enable the processes related to connecting IP based Transport Services together, Frame Transport Services together and TDM Transport Services together, either point to point, point to multipoint or multipoint to multipoint over metro and wide area networks. They involve the interaction of different transmission bearers of the same or different types at different nodes. These routing or switching nodes can be on the terrestrial communications segment, a terrestrial wireless segment or even the SATCOM space segment (e.g. carrier, frame or packet switching occurring on a regenerative transponder onboard the satellite payload).

Communications Equipment deployed for these Core Network Services (e.g. routers, switches, radio relays, SATCOM transponders, etc) may operate at different points across the core of the network. The Core Network Services support standalone routing or switching elements (i.e. without attached Communications Access Services) and only connect to Transmission Services (one or more services, when routing/switching across different bearers is involved), or connect with Communications Access Services to IP-, Frame- and TDM-based Transport Services. Nonetheless Core Network Services are not concerned with emulated Communications Access Services or IP-, Frame- and TDM-based Transport Services, by virtue of the single-hop end-to-end nature of the tunnelling mechanisms supporting the virtualisation of protocols over higher-layer protocols.

Core Network Services are closely associated with WAN routing/switching topologies (point-to-multipoint, mesh of point-to-point links or multipoint-to-multipoint). The topology is defined when the Core Network Service is specified and will form part of the Service Level Specification (SLS).

5.2.3.2.5 Aggregation Services

Aggregation Services provide the aggregation of traffic over parallel converging transmission paths, and involves Packet, Frame and Circuit Transport Services, where each of the services uses the same Transmission Service to converge into a given network node (often referred to as concentrator). They are only concerned with a selective "fan-out" and do not involve broadcast.

Aggregation Services apply within and at the edge of the core. Aggregation Services within the core provide the aggregation of transport flows from multiple edge-points that connect to the aggregation node (e.g. concentrator) over

transmission lines not involving switching or routing. Aggregation Services at the edge provide the aggregation of access flows from multiple end-nodes that connect to the aggregation node over transmission lines.

Like Communications Access Services, Edge Transport Services and Core Network Services, Aggregation Services can be closely mapped to the OSI stack lower layers.

5.2.3.2.6 Broadcast Services

Broadcast Services provide the broadcast of traffic over parallel diverging transmission paths, and involves Packet, Frame and Circuit Transport Services, where each of the services uses the same Transmission Service to diverge out of a given network node (often referred to as concentrator).

Broadcast Services apply within and at the edge of the core. Broadcast Services within the core involves the broadcast of transport flows towards multiple edge-points that connect to the broadcast node either directly over transmission lines or through Core Network Services. Broadcast Services at the edge involves the broadcast of traffic flows towards multiple end-nodes that connect to the broadcast node over transmission lines.

5.2.3.2.7 Distribution Services

Distribution Services provide the distribution of transport flows between the Distribution Nodes (DN) and to or from multiple end-nodes that connect to the DN over transmission lines.

Distribution Services are formed through a combination both the "within the core" and "at the edge" infrastructure types associated with Aggregation Services and Broadcast Services, to form a logical "ring".

5.2.3.3 Transmission Services

Transmission Services cover the physical layer (also referred to as media layer or air-interface in wireless/satellite (SATCOM) communications) supporting Transport Services, as well as Communications Access Services. Support for the latter is relevant to personal communications systems, in which the User Appliances directly connect to the transmission element without any transport elements in between.

Transmission Services are confined to the assets dealing with the adaptation to the transmission media (i.e. line drivers, adapters, transceivers, transmitters, and radiating elements (e.g. antennas). In some cases this adaption will include the modem, but in other cases the modem will be associated with Transport Services when implementing the first stage of the media-adaptation process (e.g. coding, modulation). The second stage, involving frequency conversion, amplification, radiation, bent-pipe transponder relay, etc., will be covered under Transmission Services proper.

The Transmission Services nomenclature is based on the service categories wired or wireless (including SATCOM) and coverage (i.e. local, metro, wide, and LOS, BLOS). Additionally in the case of wireless the terms static or mobile are employed. Categorising the transmission services in this manner is considered to be intuitive, "military service" agnostic, combines both wireless-radio and SATCOM under the single term "wireless" thus resulting in fewer service categories and excludes cross referencing.

5.2.3.3.1 Transmission IA Services

Transmission Information Assurance (IA) Services provide a foundation to implement and enforce IA policies at the communications transmission level. These services are the overlap between Transmission Services and the Information Assurance domain, meaning that they exist in both the Transmission Services class and the IA grouping.

5.2.3.3.2 Transmission SMC Services

Transmission Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the communications transmission level. These services are the overlap between Transmission Services and the Information Assurance domain, meaning that they exist in both the Transmission Services class and the SMC grouping.

The Transmission SMC Services are loosely based on the Information Technology Infrastructure Library (ITIL) Service Strategy. Examples of ITIL lifecycle process that can be employed are Strategy, Design, Transition, Operations, and Improvement.

5.2.3.3.3 Wired Local Area Transmission Services

Wired Local Area Transmission Services support physical transfer of data (e.g. digital bit stream), point-to-point or point-to-multipoint, using wired transmission medium amongst two or more static nodes over relatively short distances. Examples of transmission media are copper wires (two-wire, four-wire, twisted pair, coaxial, etc.) and optical fibre.

Examples of Wired Local Area Transmission Services, associated with the supporting technology employed, are telephony, local loop circuit to access leased lines, Local Area Network (LAN), and video distribution. Within this context a LAN is considered to interconnect network nodes over a relatively short distance, generally within a single location (i.e. building, office). It is also possible for a LAN to span a group of closely co-located locations.

5.2.3.3.4 Wired Metropolitan Area Transmission Services

Wired Metropolitan Area Transmission Services support physical transfer of data (e.g. digital bit stream), point-to-point or point-to-multipoint, using medium to high capacity wired transmission medium over distances spanning tens of kilometres (e.g. 5 to 50 km). Examples of transmission media are copper leased lines and optical fibre.

The capabilities of these services are defined by the characteristics of the transmission media, which enables wavelength-based multiplexing and switching, seamless transport of ATM, Ethernet, etc.

Examples of Wired Metropolitan Area Transmission Services, associated with the supporting technology employed, are Dense Wavelength Division Multiplexing (DWDM), Synchronous Optical Networking (SONET), Synchronous Digital Hierarchy (SDH), Distributed-Queue Dual-Bus (DQDB), and Plesiochronous Digital Hierarchy (PDH).

5.2.3.3.5 Wired Wide Area Transmission Services

Wired Wide Area Transmission Services support physical transfer of data (e.g. digital bit stream), point-to-point or point-to-multipoint, using high capacity wired transmission medium over long distances. Examples of transmission media are copper leased lines and optical fibre.

The capabilities of these services are defined by the characteristics of the transmission media, which enables wavelength-based multiplexing and switching, seamless transport of ATM, Ethernet, etc.

Examples of Wired Wide Area Transmission Services, associated with the supporting technology employed, are Dense Wavelength Division Multiplexing (DWDM), Synchronous Optical Networking (SONET), Synchronous Digital Hierarchy (SDH), and Plesiochronous Digital Hierarchy (PDH).

5.2.3.3.6 Wireless LOS Static Transmission Services

Wireless Line of Sight (LOS) Static Transmission Services support the wireless transfer of data amongst two or more static nodes within Line of Sight (LOS) of each other, employing modulated Radio Frequency (RF) carriers in different frequency bands. Selection of frequency bands is based on coverage, capacity, propagation, transceiver attributes, and frequency coordination constraints.

In the context of these services, a distinction is made between transmission over an optical/visual LOS path (i.e. free of any form of visual obstruction), and a virtual LOS path (i.e. a straight line through visually obstructing material) - also referred to as Non- or Near- LOS (NLOS).

Examples of Wireless Line of Sight (LOS) Static Transmission Services with optical/visual LOS are Direct Line of Sight (DLOS) radio and Ultra High Frequency (UHF) radio-relay. Services with virtual LOS are often employed in the context of Wireless Local Area Network (WLAN) and Wireless Metropolitan Area Network (WMAN), or with other types of LOS wireless communication such as Combat Net Radio (CNR), cellular, etc.

5.2.3.3.7 Wireless LOS Mobile Transmission Services

Wireless Line of Sight (LOS) Mobile Transmission Services support the wireless data of amongst two or more nodes, where one or more of the nodes are operating on the move, within Line of Sight (LOS) of each other, employing modulated Radio Frequency (RF) carriers in different frequency bands. Selection of frequency bands is based on coverage, capacity, propagation, transceiver attributes, and frequency coordination constraints.

In the context of these services, a distinction is made between transmission over an optical/visual LOS path (i.e. free of any form of visual obstruction), and a virtual LOS path (i.e. a straight line through visually obstructing material) - also referred to as Non- or Near- LOS (NLOS).

5.2.3.3.8 Wireless BLOS Static Transmission Services

Wireless Beyond Line of Sight (BLOS) Static Transmission Services support wireless transfer of data amongst two or more static nodes Beyond Line of Sight (BLOS) of each other, employing modulated Radio Frequency (RF) carriers in different frequency bands. Selection of frequency bands is based on coverage, capacity, propagation, transceiver attributes, and frequency coordination constraints.

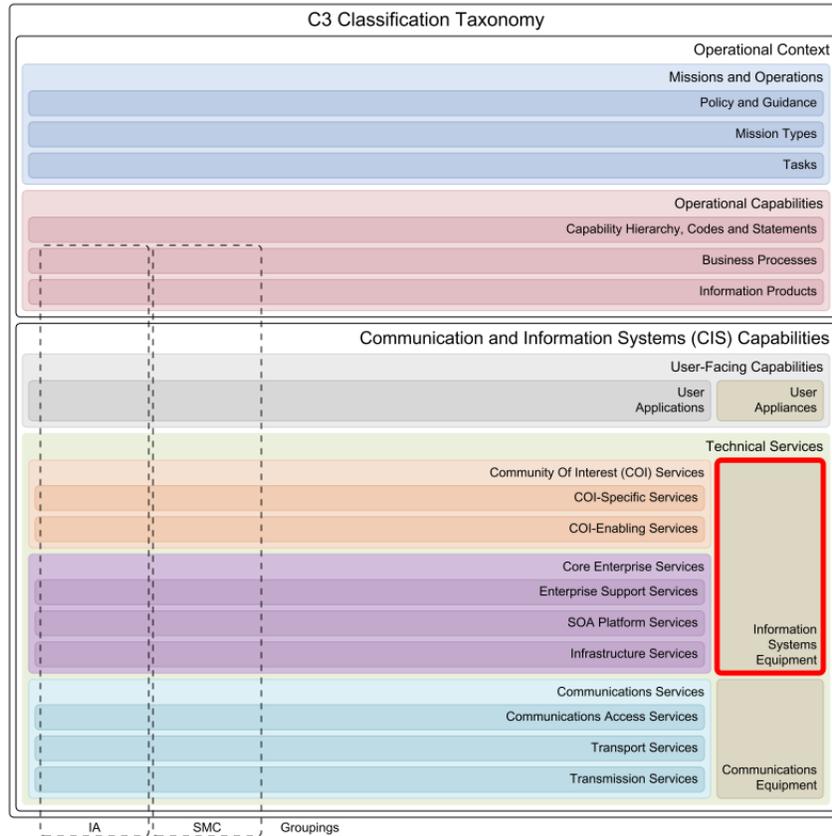
In the context of these services, the wireless transmission path between the static nodes can be established passively (i.e. wireless signal is refracted back to earth by different atmospheric layers) or actively (i.e. wireless signal is transmitted back to earth via a transponder). In the case when a transponder (e.g. satellite) is employed, the transponder can perform frequency translation, filtering (including limiting), channel amplification, combining/splitting over one or multiple antennas/coverage beams, as well as relaying over one or more channels.

5.2.3.3.9 Wireless BLOS Mobile Transmission Services

Wireless Beyond Line of Sight (BLOS) Mobile Transmission Services support wireless transfer of data amongst two or more nodes, where one or more of the nodes are operating on the move, Beyond Line of Sight (BLOS) of each other, employing modulated Radio Frequency (RF) carriers in different frequency bands. Selection of frequency bands is based on coverage, capacity, propagation, transceiver attributes, and frequency coordination constraints.

In the context of these services, the wireless transmission path between the mobile nodes can be established passively (i.e. wireless signal is refracted back to earth by different atmospheric layers) or actively (i.e. wireless signal is transmitted back to earth via a transponder). Example transponders can be a satellite (i.e. satellite communications on-the-move) or a Medium/High Altitude Long Endurance (HALE) relay such as an Unmanned Aerial Vehicles (UAV) carrying a Communications Relay Package (CRP).

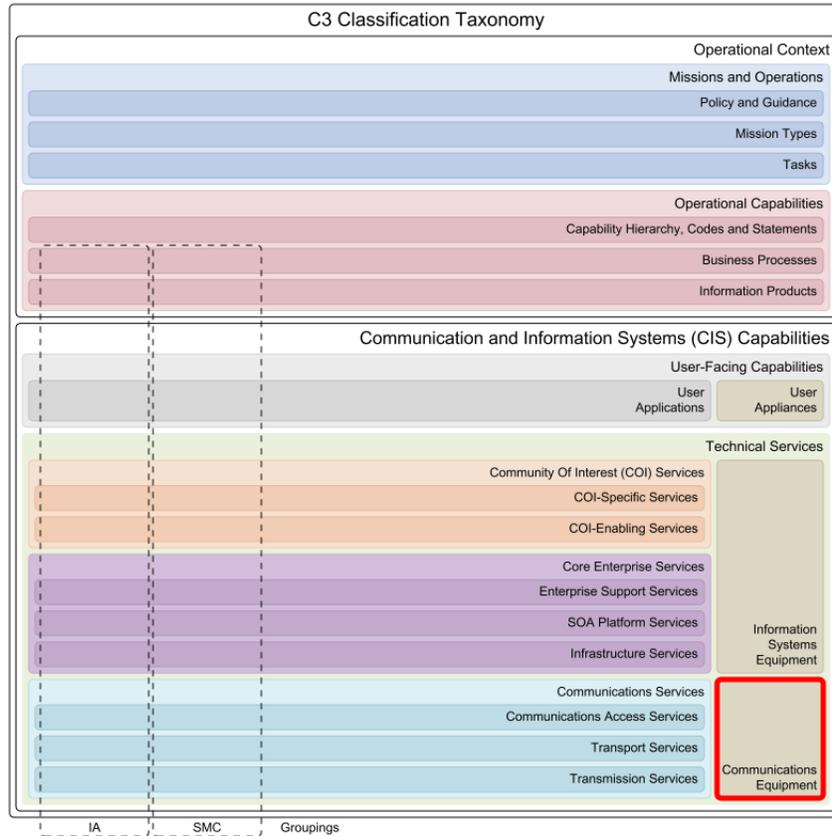
5.2.4 Information Systems Equipment



Information Systems (IS) Equipment includes those devices involved in hosting software for the provision of Community Of Interest (COI) Services and Core Enterprise Services, and the handling of operational data of the enterprise.

Examples of Information Systems (IS) Equipment include databases, file servers, application servers, middleware, back-up solutions and various others. Typical IS equipment are servers and central processing units (mainframes) and all related features and peripheral units, including processor storage, console devices, channel devices, etc.

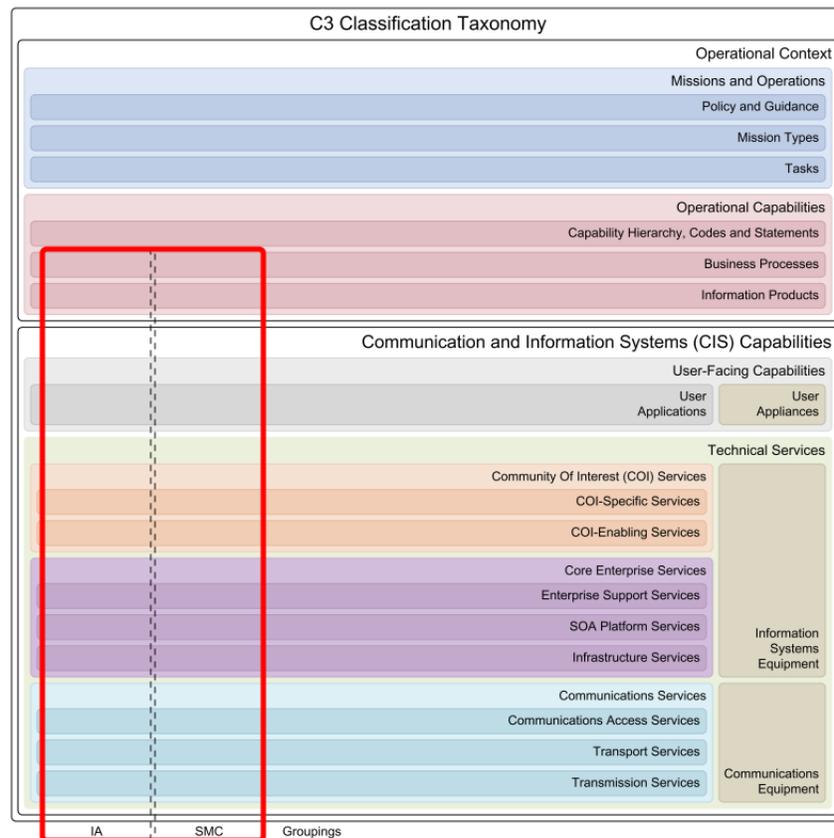
5.2.5 Communications Equipment



Communications Equipment includes those devices, hardware and software elements used for transfer of data that make up the networking and physical communications links for the enabling of Communications Services.

Examples of Communications Equipment include modems, data sets, multiplexers, concentrators, routers, switches, local area networks, private branch exchanges, network control equipment, microwave or satellite communications systems and the physical transmission media.

6 Groupings



Groupings are a mechanism to bundle components from various classes of the C3 Classification Taxonomy into a collection with a particular common characteristic. Two significant examples are the Information Assurance (IA) grouping and the Service Management and Control (SMC) grouping. Both require components from several classes of the taxonomy (horizontal relation), and also need to ensure coherence within the grouping (vertical relation).

6.1 IA

Information Assurance (IA) provides a collection of measures to protect information processed, stored or transmitted in communication, information or other electronic systems in respect to confidentiality, integrity, availability, non-repudiation and authentication.

The Information Assurance grouping overlaps with most classes (horizontal layers) of the C3 Classification Taxonomy, and should therefore not be seen as a class itself but rather as a logical grouping of critical components that jointly implement the tenets of NATO's Information Assurance policies.

6.2 SMC

Service Management and Control (SMC) provides a collection of capabilities to coherently manage components in a federated service-enabled information technology infrastructure. SMC tools enable service providers to provide the desired quality of service as specified by the customer.

The Service Management and Control grouping overlaps with most classes (horizontal layers) of the C3 Classification Taxonomy, and should therefore not be seen as a class by itself but rather as a logical grouping of critical components that jointly provide the tools to manage and control a distributed and federated service-oriented enterprise.