NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

14 March 2016

DOCUMENT
AC/322-D(2016)0017

CONSULTATION, COMMAND AND CONTROL BOARD (C3B)

C3 Taxonomy Baseline 2.0

Note by the Secretary

References: (a) 6300 TSC FCX 0010/TT-151521, C3 Taxonomy Baseline 2.0, 19 November 2015
(b) AC/322-N(2016)0021 & AS1, Architecture Capability Team – Advice on C3 Taxonomy Baseline 2.0, 1 February 2016

1. The Allied Command Transformation (ACT), with Reference (a), requested the C3 Board to review the C3 Taxonomy Baseline 2.0 as new version, superseding AC/322-N(2012)0092.

2. As a result of the advice of the Architecture Capability Team at Reference (b), the C3 Board endorsed the C3 Taxonomy Baseline 2.0. This document is deliberately issued without markings to facilitate the widest possible dissemination.

3. This updated C3 Taxonomy supersedes any previous versions and should be considered for all updated and future NATO capabilities.

(Signed) M. ROTERMUND

Enclosure 1: C3 Taxonomy Baseline 2.0

1 Enclosure

Action Officer: Lori MacRae, Ext. 5071
Original: English

19 NOV 15

C3 Taxonomy Perspective, Baseline 2.0

Table of Contents

1 Introduction

The C3 Taxonomy is a model that represents the concepts and their relationships involved in all the life cycle activities for NATO's Consultation, Command and Control (C3) capabilities. The C3 Taxonomy provides a tool and common language to synchronize these activities and improve connecting NATO's Strategic Concept and Political Guidance through levels of ambition expressed in 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 NATO's CIS capabilities but did so in relative isolation. Today, we are confronted with a patchwork quilt of systems, applications, services, standards, vocabularies and taxonomies. Even simple English words, such as service or capability, have become highly ambiguous. As a result of this stove-piping, NATO now faces a very complex CIS fabric that is not interoperable and attempts to solve this problem is often hampered by lack of mutual understanding.

The purpose of this C3 Taxonomy is to capture concepts from various communities and record them for item classification, integration and harmonization purposes. Recognizing their dependencies and relationships, the taxonomy plots and associates political and military ambitions, Mission-to-Task Decomposition, Capability Hierarchy, Statements and Codes, Business Processes, Information Products, User Applications, Technical Services and Equipment definitions and requirements to Reference Documents, Standards, Patterns, Increments and other concepts.

In an analogy to geographical surveying, this approach is referred to as "enterprise mapping", since the C3 Taxonomy charts NATO's complex C3 landscape. As with geographic elements on maps, the assignment of colors, fonts and positions of taxonomy elements in the poster, and the assignment of text, numbering and indentation in the report have particular meaning. The mapping of the taxonomy elements is rich in semantic relations that provide the orientation between the concepts. The environment of the concepts is arranged in separate "layers" (vs. grid) and the granularity (vs. scale) in the "levels" of detail.

The data for the C3 Taxonomy is registered, processed and maintained on the Enterprise Mapping (EM) Wiki, a protected internet-facing website run by Allied Command Transformation (ACT). This website contains far more information than is made available through the C3 Taxonomy poster and this document; information about lower levels in the taxonomy and the linkage between the here mentioned taxonomy items and other concepts are available for registered uSers on the EM Wiki via https://tide.act.nato.int/em.

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 while keeping the federated nature of the organization in mind.

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 objectives and 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 organizations as NATO derives and defines requirements for Consultation, Command and Control (C3).

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).

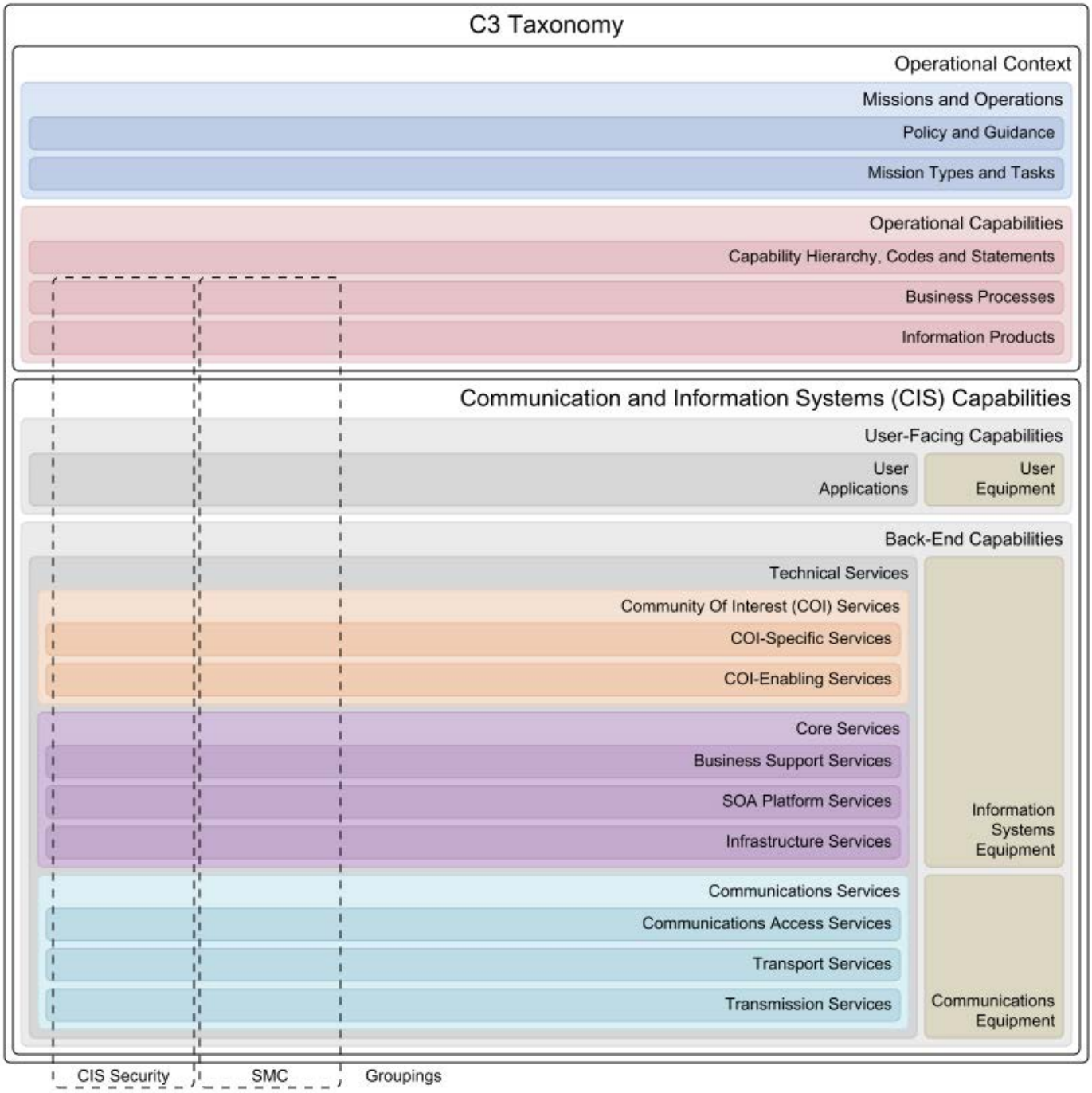
It is NATO's intent that the approach for deriving C3 requirements is through "service provision". This entails specifying the "requester" for a task to be performed and a "provider" who commits to performing the task. An example of a requester may be a headquarter and the provider may be a subordinate unit or another headquarter. 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 (NNEC), 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.

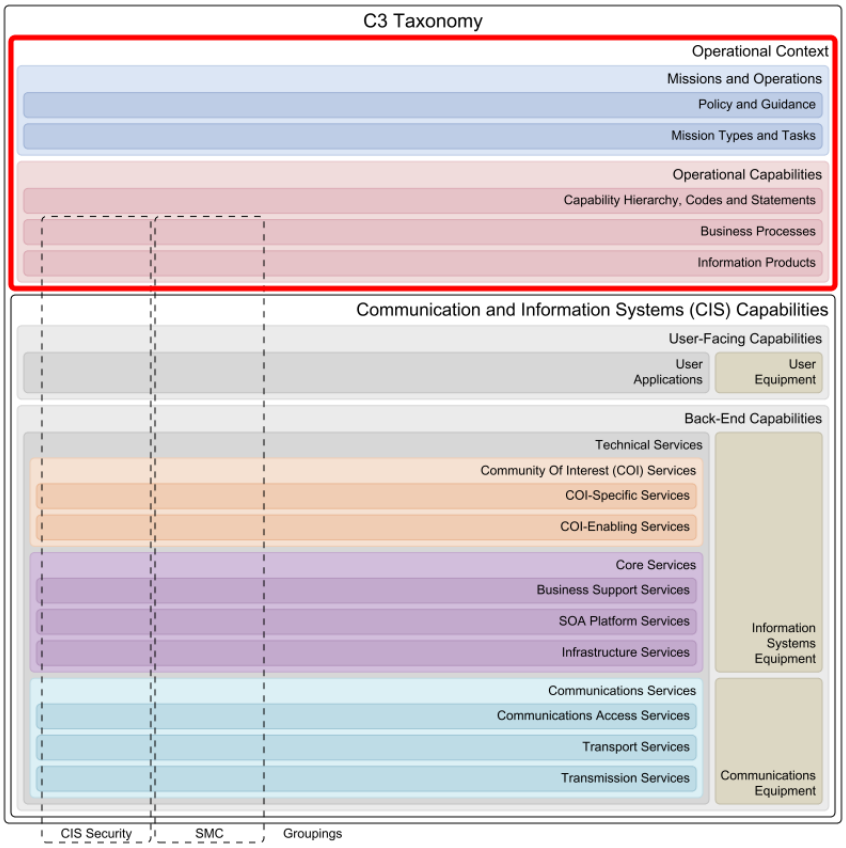
In a complex and federated enterprise like NATO there is a need for a generic structure or framework that can be used to align and synchronize various activities and projects that are on-going in parallel, when the organisation's CIS infrastructure transforms towards a network-enabled capability. The C3 Taxonomy provides that generic framework and contributes to a key component of the Connected Forces Initiative: *Exploiting technology to help deliver interoperability*.

3 C3 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 Taxonomy, connecting political and military ambitions to CIS capability components through mission types, capability codes and statements, business processes and information products. Furthermore, this document provides definitions for the higher taxonomy components as extracted from the Enterprise Mapping (EM) Wiki on the date shown at the bottom of the page.



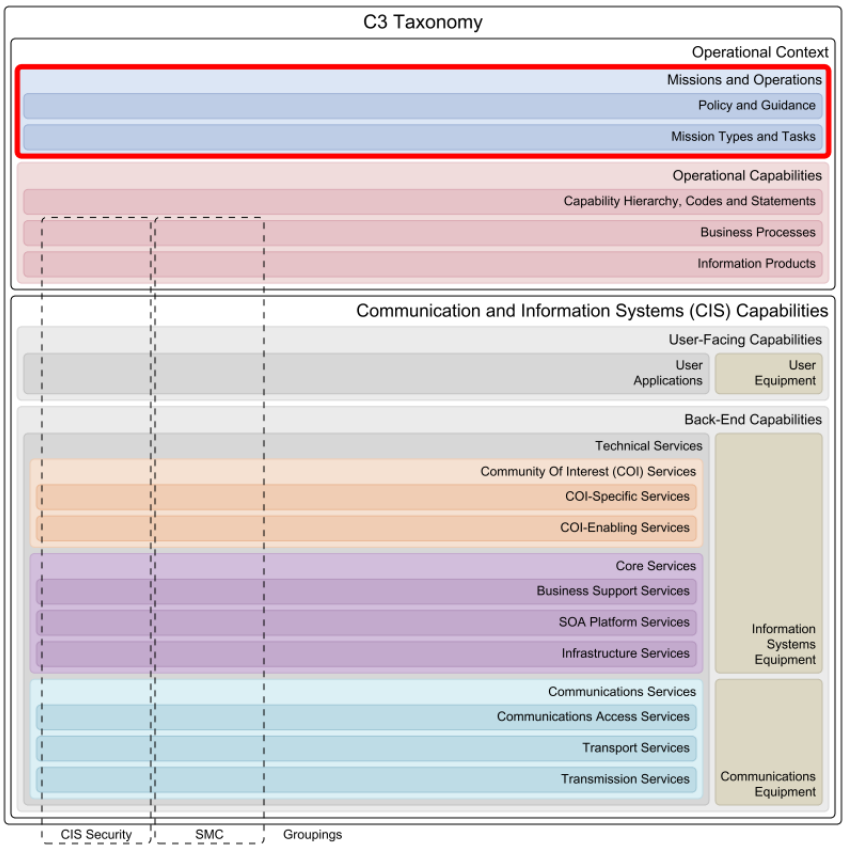
4 Operational Context



The C3 Taxonomy layer for the "Operational Context" represents the environment in which CIS Capabilities will be deployed. The context and scope for these CIS Capabilities are defined by the capture of NATO's overarching political and military guidance and policies, the identification of mission types and key tasks, the cataloging of needed capabilities, and the description of business processes and their related information products.

Information in this part of the C3 Taxonomy is primarily obtained from the NATO Defence Planning Process (NDPP) and business process analysis.

4.1 Missions and Operations



The "Missions and Operations" layer in the C3 Taxonomy represents NATO's political and military ambitions as derived from the Strategic Concept and Political Guidance. These ambitions are expressed in a series of possible Mission Types and related Key Tasks, as well as references to relevant concepts, guidance, policies and publications. The Mission Types are identified in policy and guidance, and subsequently, the Key Tasks are derived though the Mission-to-Task Decomposition (MTD), as expressed in the NATO Defence Planning Process (NDPP).

4.1.1 Policy and Guidance

The "Policy and Guidance" taxonomy layer represents NATO's political and military ambitions. These ambitions are based on a Strategic Concept that serves as the Alliance's roadmap. Derived political and military guidance reflects the political, military, economic, legal, civil and technological factors which could (and should) impact the development of the capabilities that are required to fulfill the ambitions. Furthermore, this level captures the policies and other reference documents that guide and support 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 structured documents of standardized organizations, processes and procedures, published by NATO.

4.1.1.5 Policies and Directives

Policies and Directives are information products used to regulate NATO matters. Policies provide guidelines, principles and/or rules. Through them the organization presents where it stands on important issues. The policies are mainly used to regulate organizational affairs. A directive may establish policy, assign responsibilities, define objectives and delegate authority to those working in and with the authoritative figure.

4.1.2 Mission Types and Tasks

The "Mission Types and Tasks" taxonomy layer represents the missions and operations that the Alliance is expected to be capable to perform, as derived from NATO's policy and guidance. They are expressed as a set of Military Strategic Objectives (MSOs) and Operational Objectives (OO) required to achieve a specified end-state. The circumstances for the occurrence of a specific Mission Types (MT) are described in a Generic Planning Situation (GPS) that provides generalized descriptions of the affiliated political, military, socio-economic and geographic environment.

A Key Task (KT) defines the activities that need to be performed by the Alliance in order to achieve the stated objectives or desired effect of a specific Mission Type. Key Tasks are identified through the Mission-to-Task Decomposition (MTD), which is part of the NATO Defence Planning Process (NDPP). Key Tasks are decomposed into sub-tasks and sub-sub-tasks.

4.1.2.1 Mission Type - Collective Defence (CD)

The Collective Defence (CD) mission type 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 upon them all. Consequently, the NATO 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 - Antiterrorism (AT)

The Antiterrorism (AT) mission type consists of activities taken for defensive and preventive measures to reduce the vulnerability of forces, individuals, and property to terrorism. Such measures include protective and deterrent measures aimed at preventing an attack or reducing its effects which support the overall force protection (FP) effort.

The challenge is to produce effective protective measures to reduce the probability of a successful terrorist attack against installations, forces, individuals, and property. AT includes those defensive measures used to reduce vulnerability of forces, individuals, and property to terrorist acts, to include limited response and containment by local military forces. They also consist of personal security and defensive measures to protect military members, high-risk personnel, civilian employees, family members, facilities, information, and equipment. Personal security measures consist of common-sense rules of on- and off-duty conduct for every military member.

Terrorist activity may be discouraged by varying the security posture through the use of a random AT measures program which may includevarying land, maritime, and air patrol routes; staffing guard posts and towers at irregular intervals; and conducting vehicle and vessel inspections, personnel searches, and identification chekcs on a set but unpredictable pattern.

4.1.2.3 Mission Type - Consequence Management (CM)

The Consequence Management (CM) mission type consists of activities to maintain or restore essential services and to manage and mitigate problems resulting from disasters and catastrophes, including natural, man-made, or terrorist incidents. Chemical, biological, radiological, nuclear, and high yield explosives (CBRNE) CM activities are specifically conducted to alleviate the effects of deliberate and inadvertent releases of CBRNE which have the potential to cause high casualties and large levels of destruction.

4.1.2.4 Mission Type - Counter Insurgency (COIN)

The Counter Insurgency (COIN) mission type consists of political, economic, social, military, law enforcement, civil, and psychological activities that aim to defeat insurgency and address any core grievances. COIN is a politically motivated, intelligence-driven activity and the aim of COIN is to defeat the insurgents. All insurgencies are unique in their political, social, and historical contexts and they demand that the counterinsurgent adapt with skill and knowledge to meet specific socio-political and military conditions. COIN operations often include security assistance programs such as military education and training programs because properly trained and motivated local security and military forces provide the best COIN operators.

Conducting successful COIN operations requires an adaptive and flexible mindset and an understanding that the population is the critical dimension; and a key part of understanding the population is having cultural competence and an intimate knowledge of what causes and perpetuates insurgency. It is equally important as understanding physical terrain is to the successful conduct of conventional land operations. A second aspect of the counterinsurgent mindset is being able to think like an insurgent in order to stay ahead of or at least anticipate the actual insurgents' decisions and actions. Third, successful counterinsurgents must understand it is essential to establish an enduring presence within the population to create confidence and provide continuous security and development efforts, which are vital to assuring the population's sense of security and long-term outlook. This will isolate the insurgents from the population, thus depriving them of recruits, resources, intelligence, and credibility. Finally, it must be clearly understood that the military instrument is only one part of a comprehensive approach for successful COIN, although the security situation may require the joint force to execute tasks that other organizations are better suited to conduct.

4.1.2.5 Mission Type - Counter Terrorism (CT)

The Counterterrorism (CT) mission type consists of activites taken for offensive measures to neutralize terrorism before and after hostile acts are carried out. Such measures include those counterforce activities justified for the defence of individuals as well as containment measures implemented by military forces or civilian organizations. CT is primarily conducted by specially organized, equipped, and trained CT assets; however, by exception, theymay also be accomplished by conventional forces. Accordingly, CT is included as a special operational task.

CT contains its own unique characteristics and problems for NATO forces conducting them. CT may be conducted in the context of an undeclared conflict against state-sponsored or transnational, autonomous armed groups who are not easily identified, and who often do not fall under the categories of combatants defined in the applicable international law. NATO forces engaged in a CT operation may be required to operate in conflict areas with or eithout the assistance of the local government.

4.1.2.6 Mission Type - Peacekeeping (PK)

The Peacekeeping (PK) mission type consists of activities 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 Peace Enforcement (PE) operation. Thus, the conduct of PK is driven by the requirement to build and retain perceived legitimacy.

4.1.2.7 Mission Type - Peace Enforcement (PE)

The Peace Enforcement (PE) mission type consists of activities that are coercive in nature and 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.

Peace Enforcement normally takes 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.

4.1.2.8 Mission Type - Conflict Prevention (CP)

The Conflict Prevention (CP) mission type consists of activities that are normally conducted in accordance with the principles of Chapter VI of the UN Charter. These 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.

Military assets used for Conflict Prevention should generally be focused on the support they provide to the political and developmental efforts to mitigate the causes of societal tensions and unrest. This can be before the commencement of intervention, or during or after intervention in order to protect and consolidate the reform and development process. Military activities will be tailored to meet political and developmental demands but include: early warning, surveillance, and preventative deployment.

4.1.2.9 Mission Type - Peacemaking (PM)

The Peacemaking (PM) mission type consists of 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.

4.1.2.10 Mission Type - Peacebuilding (PB)

The Peacebuilding (PB) mission type consists of activities 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. 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.

4.1.2.11 Mission Type - Support to Humanitarian Assistance (SHA)

The Support to Humanitarian Assistance (SHA) mission type consists of activities to relieve or reduce human suffering. Humanitarian Assistance (HA) 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 HN civil authorities or agencies that may have the primary responsibility for providing that assistance. They normally supplement the activities of governmenral authorities, Non-Governmental Organisations (NGOs), and Intergovernmental Organisations (IGOs).

Support to Humanitarian Assistance may be conducted at the request of the Host Nation (HN) as part of another operation, such as a Peace Support Operations (PSO) or Counter Insurgency (COIN), or as an independent distinct operation specifically mounted to alleviate human suffering especially where responsible civil actors are unable or unwilling to support a population adequately. NATO military activities may support short-term tasks such as communications restoration, relief supply management, providing emergency medical care, humanitarian demining, and high priority relief supply delivery. They could also take the form of advice and selected training, assessments, and providing manpower and equipment.

4.1.2.12 Mission Type - Support to Disaster Relief (DR)

The Support to Disaster Relief (DR) mission type consists of activities to provide 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 UN or government, including host government (where one exists), NGOs, and the civil sector.

Military forces should be ready to assist in relief operations when the need for them arises, and to cooperate with other organizations concerned. Normally, military forces work to create the conditions in which these other agencies can operate more freely and effectively. NATO forces, such as the standing naval forces, may be in the area as a result of an unrelated exercise or operation and could be diverted by direction of the NAC or MC; however, because of the need for speed, it is likely that immediate reaction will be provided unilaterally by nations. Disaster relief could bconducted as a standalone operation; however, because of the requisite response times, it is more likely to take place within the context of an ongoing Non-Article 5 Crisis Response Operation (NA5CRO).

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

The Support of Non-Combatant Evacuation Operations (NEOs) mission type consists of activities from 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) nocombatants 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.

4.1.2.14 Mission Type - Extraction Operation (EOP)

The Extraction Operation (EOP) mission type consists of activities to cover or assist in the withdrawal of a UN or other military mission from a crisis region by a NATO-led force. A force committed to an extraction operation should have similar capabilities to those required by a force operating in support of NEO and should in 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.

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

The Military Aid/Support to Civil Authorities (SCA) mission type consists of 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 overtaxes the capabilities of the civil authorities. Categories of support include military assistance to covil authorities and support to numanitarian assistance operations.

Military Assistance to Civil Authorities includes military support to civil authorities, civil law enforcement, economic recovery, and military assistance for civil disturbance. Implementation of a civil plan in response to a crisis may depend on the military to provide a stable and secure environment for its implementation. Support might include providing security assistance to an election process and supervising the transition to a democratically elected public administration, training local police and security forces, mine and unexploded ordnance clearing and training of the local population, assisting in public administration, maintaining public services, supporting public administration in coordinating a humanitarian operation, or providing security for individuals, populations, or installations. In exceptional circumstances, within a mandate for a larger mission, NATO military forces could be called on to contribute to tasks related to public security which are the responsibility of a mandated civil authority, organization, or agency. Specifically, military support to public securitywill depend entirely on the mission and the residual local policing and judicial capability, and may require involvement in civil security tasks, including operations to maintain local law and order during the initial stage of an operation, until appropriate civilian authorities can take over thier tasks. This assistance will normally be provided by multinational specialized units (MSUs) or, in special circumstances, other forces.

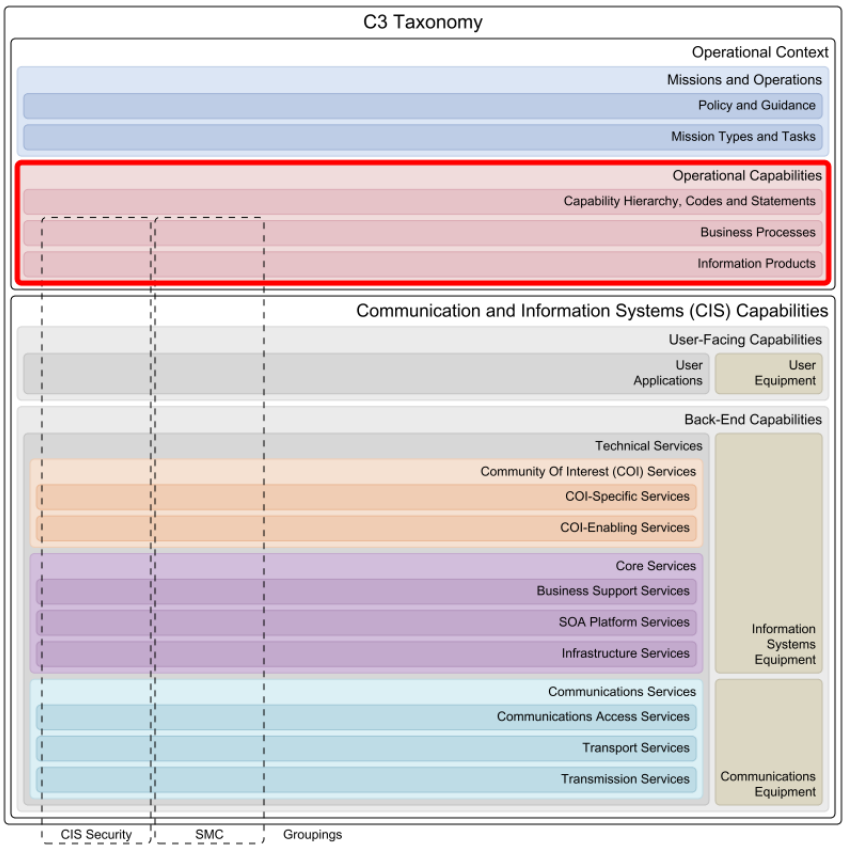
4.1.2.16 Mission Type - Enforcement of Sanctions and Embargoes (ESE)

The Enforcement of Sanctions and Embargoes (ESE) mission type consists of activities 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).

4.1.2.17 Mission Type - Permanent Tasks

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

4.2 Operational Capabilities



The "Operational Capabilities" layer in the C3 Taxonomy represents all the capabilities required by the Alliance for the successful completion of missions - stated in Mission Types and refined in Key Tasks - and the achievement of stated ambitions. Operational Capabilities are captured in a Capability Hierarchy Framework (CHF) and are expressed as a set of Capability Codes and Statements (CC/CS). In the same way as the Key Tasks are further refined in Business Processes and their related Information Products, the Capability Codes and Statements are materialized by means of the User-Facing Capabilities (Applications and Equipment).

4.2.1 Capability Hierarchy, Codes and Statements

The "Capability Hierarchy, Codes and Statements" taxonomy layer represents the capability needs resulting from the NATO Defence Planning Process (NDPP) in two distinguished but related models: the Capability Hierarchy Framework (CHF) and the Capability Codes and Statements (CC/CS).

The Capability Hierarchy Framework incorporates the full spectrum of capabilities required to conduct Article 5 Collective Defence, Non-Article 5 Crisis Response and Consultation and Co-operation missions. The top tier of this framework is comprised of seven broad capability areas. These seven areas were identified through comparison and harmonization of a broad range of national and multinational capability hierarchies. In this structure, the framework supports the expression of Minimum Capability Requirements (MCRs) and Priority Shortfall Areas (PSA).

The Capability Codes (CCs) and Capability Statements (CSs) are used for the specification of capability requirements, and so form the basis for requirements apportionment and target setting. The codes are unique alphanumeric descriptors for functional capability groups and contain the applicable statements. The statements capture capability requirements along the DOTMLPFI lines of development in four different groupings: capstone, principle, enabling and improvement statements.

4.2.1.1 Capability Hierarchy Framework

The Capability Hierarchy Framework (CHF) integrates with and complements the mission and situation analysis of the Capability Requirements Review (CRR) in support of the NATO Defence Planning Process (NDPP). It provides a structure to substantiate the expression of NATO's minimum capability requirements (MCR) and Priority Shortfall Areas (PSA). The structure of the framework is found through a functional decomposition of capabilities at various levels of aggregation, and thus enables the capture and description of capability requirements at alternative levels of granularity. The MCR for the

short/medium term will be expressed in terms of the Bi-SC agreed Capability Codes and Statements (CC/CS).

4.2.1.2 Capability Codes

The Capability Codes (CC) 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. The codes are accompanied by a selection of Capability Statements (CS).

The Capability Codes are linked to the Capability Requirements Review (CRR) in a manner that reflects the various functional capability contributions delivered by that capability code. This allows to translate capability code shortfalls (identified during step 2 of the NATO Defence Planning Process or NDPP) into related functional capability shortfalls in the Capability Hierarchy Framework (CHF). These non-solution specific functional capability shortfalls then provide the basis for Priority Shortfall Areas (PSA) and ultimately, the longer term solution development activities in NDPP steps 3 and 4.

4.2.1.3 Capability Statements

The Capability Statements (CS) capture the capability requirements along the DOTMLPFI (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability) lines of development in groupings of capstone, principal, enabling and improvement statements. The statements are part of the common language used to describe capabilities in both the Defence Planning and Operations Planning frameworks. Capability Statements are relevant for the specification of particular Capability Codes (CC).

4.2.2 Business Processes

The "Business Processes" taxonomy layer represents a collection of related, structured processes and activities that produce a specific service or product (serve a particular goal) for a particular customer or customers. The definition of these business processes are linked with roles, activities, information products and automation needs (applications, services and their respective functions).

4.2.2.1 CIS Security Processes

The CIS Security Processes are composed of a collection of business processes that are implemented and executed to support an adequate level of security for information handled by Communication and Information Systems (CIS) in an organization.

The CIS Security Processes enable to create a secure environment to meet the security objectives to ensure: the confidentiality of information by controlling the disclosure of, and access to, information, supporting systems, services and resources; the integrity and availability of information, supporting systems, services and resources; the reliable identification and authentication of persons, devices and services accessing CIS; and appropriate non-repudiation for individuals and entities having processed the information.

4.2.2.2 SMC Processes

The Service Management and Control (SMC) Processes are composed of a collection of business processes that are implemented and executed to support the coherent management of components in a service-enabled Communication and Information Systems (CIS) environment.

4.2.2.3 Governance Processes

The "Governance Processes" are composed of a collection of business processes that are implemented and executed to 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 prioritization 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

The "Management Processes" are composed of a collection of business processes that are implemented and executed to 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

The "Consultation Processes" are composed of a collection of business processes that are implemented and executed to 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

The "Cooperation Processes" are composed of a collection of business processes that are implemented and executed to support the 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 C2 Processes

The "Command and Control (C2) Processes" are composed of a collection of business processes that are implemented and executed to support the execution of military missions. Mission Types and Tasks provide the Operational Mission Area context for the development of complete processes descriptions.

4.2.2.8 Support Processes

The "Support Processes" are composed of a collection of business processes that are implemented and executed to support day-to-day operations of the Alliance, such as finance and administration, communication, manpower, security, logistics and other.

4.2.3 Information Products

The "Information Products" taxonomy layer represents the collections of information that are regarded as the formal output of a business process and/or can be used as an input to other business processes. Information Products consist of several information elements. They can be seen as any communication or representation of knowledge such as facts, data, or opinions in any medium or form.

4.2.3.1 CIS Security Information

CIS Security Information is composed of a collection of information products that are processed and and created for the implementation and enforcement of Communication and Information Systems (CIS) Security, including Information Assurance (IA) and Cyber Defence (CD).

CIS Security Information is any information on CIS security , current in time that needs to be managed (e.g. collected, assessed, shared, and exploited). It contains:

- Intel information
- CIS value information
- CIS information, such as:
  - Network topology
  - Source entities
  - CIS (external) services
  - CIS components dependencies (internal/external)
  - HW/SW components
  - HW/SW configurations
- Reference information:
  - CIS component certification report
  - CIS component trustworthiness report
- Threat Information:
  - Threat Analysis

4.2.3.2 SMC Information

Service Management and Control (SMC) Information is composed of a collection of information products that are processed and created for the implementation and enforcement of SMC policies at all levels.

4.2.3.3 Intent and Guidance

The "Intent & Guidance" are composed of a collection of information products that are processed and created for the representation of the intentions and key directions issued by a leader. Intent provides the keystone doctrine for the planning, execution and support of Allied 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, a 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 the instructions and advice on the execution of plans, operations, and support of operational activities.

4.2.3.4 Rules and Measures

The "Rules & Measures" are composed of a collection of information products that are processed and created for the representation of the constraints issued by authorities and for the measurement of compliance with those constraints. Rules are authoritative statements of what to do or not to do in a specific situation, issued by an appropriate person or body. Rules clarify, demarcate, or interpret a law or policy. Measures indicate the degree or grade of excellence expressed in terms of performance or effectiveness.

4.2.3.5 Plans

The "Plans" are composed of a collection of information products that are processed and created for the representation of 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

The "Tasking & Orders" are composed of a collection of information products that are processed and created for the representation of the assignment of work to an individual or group of individuals by a leader. Taskings are the result of the translation of an 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

The "Situational Awareness (SA)" is composed of a collection of information products that are processed and created for 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. Situational Awareness 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. It provides critical information to decision-makers in complex, dynamic areas such as military command and control.

4.2.3.8 Resource Status

The "Resource Status" is composed of a collection of information products that are processed and created for the representation of the current state or condition of resources. This then provides information about any entity available for use, such as ammunition, equipment, manpower, funding, etcetera.

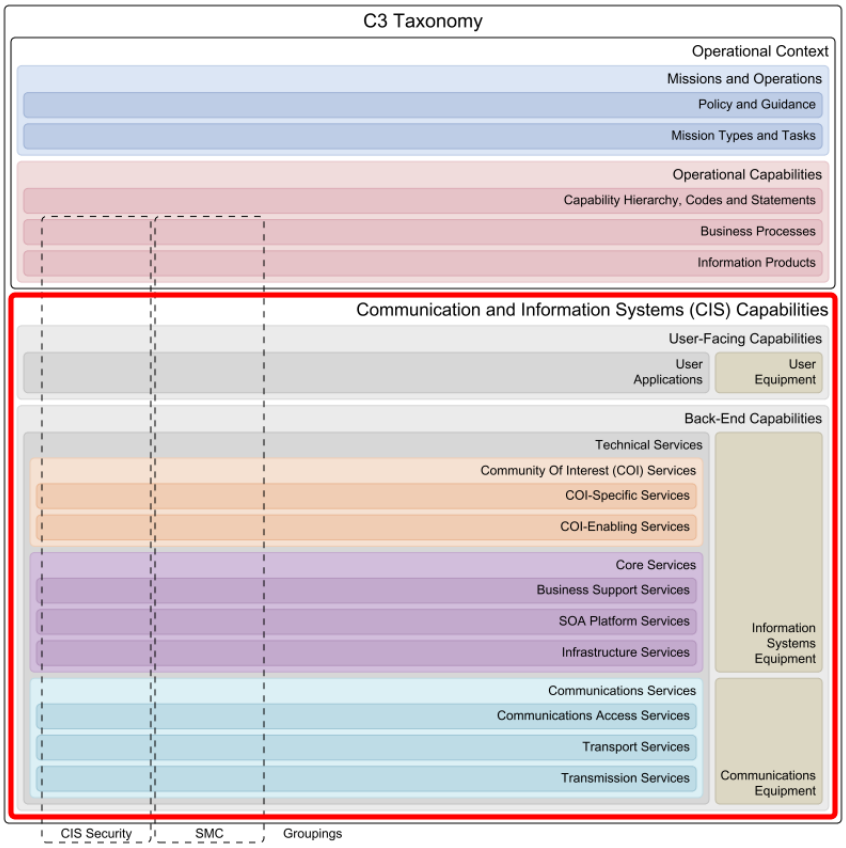
4.2.3.9 Requests and Responses

The "Requests & Responses" are composed of a collection of information products that are processed and created for the representation of 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.

4.2.3.10 Reports

The "Reports" are composed of a collection of information products that are processed and created for the representation of key indicators for business process transactions. These results can be gathered through collection of output data, quality analysis and additional research on the process, its outcomes and its stakeholders.

5 CIS Capabilities

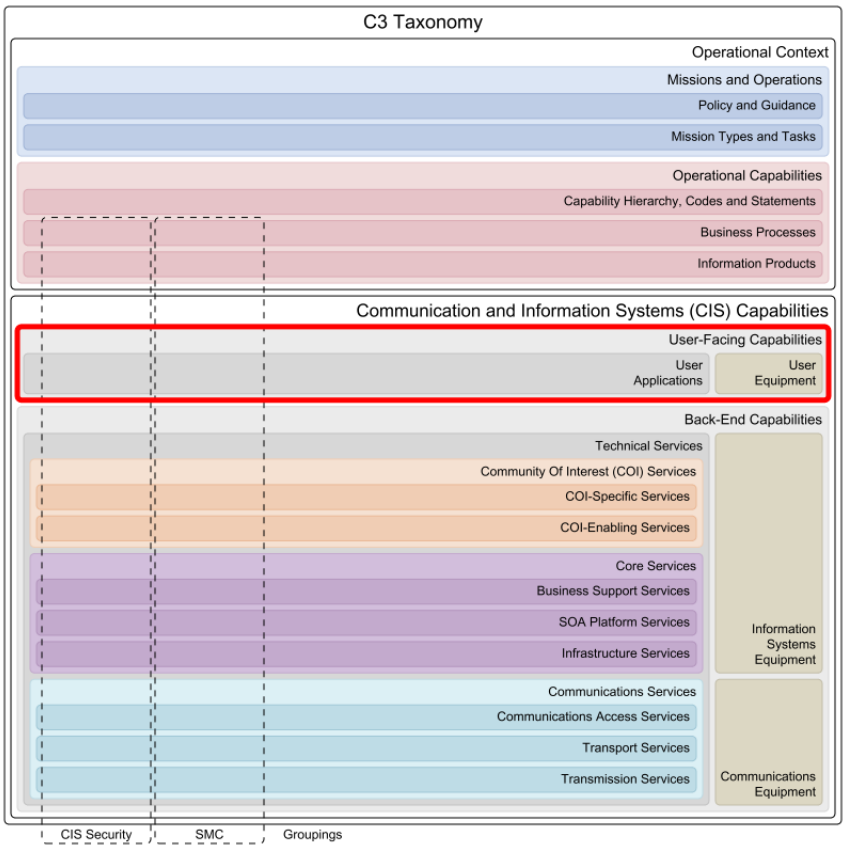


The C3 Taxonomy layer for the "Communication and Information System (CIS) Capabilities" represents the logical components of the capabilities required to meet NATO's information system and communication needs in support of Missions and Operations.

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, and digital products. Organizations and individuals rely on information systems to manage their operations, supply services, and augment personal lives.

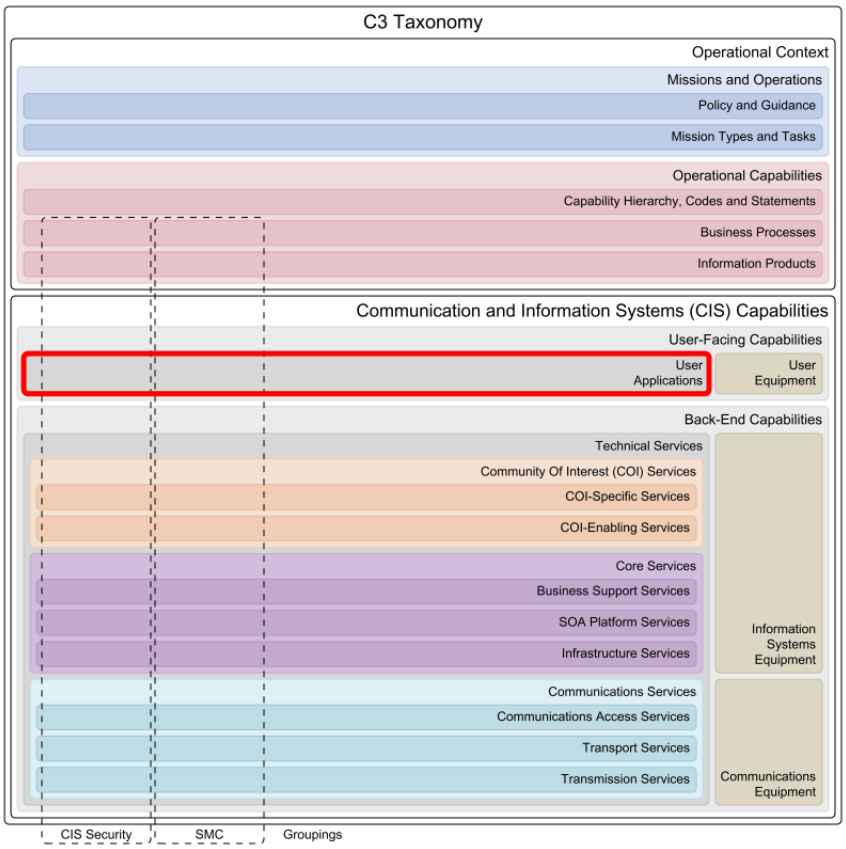
5.1 User-Facing Capabilities



The "User-Facing Capabilities" layer in the C3 Taxonomy represents the interaction between users and Communication and Information Systems (CIS) Capabilities, in order to process the Information Products in support of Business Processes.

User-Facing Capabilities incorporate the User Equipment, as well as the User Applications that run on that equipment.

5.1.1 User Applications



The "User Applications" taxonomy layer represents the collection of applications - also known as application software, software applications, applications or "apps" - that enable users to perform singular or multiple related tasks through the provision of functionally designed computer software components. User Applications in the C3 Taxonomy are defined just up to a level of detail enough to describe what they 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. They are executed on User Equipment.

The applications and their supporting Back-End Capabilities are defined without any constrains from or references to actual technology implementations. User Applications change over time to reflect changes in their supported business processes and independently of the evolution of technology.

5.1.1.1 CIS Security Applications

The CIS Security Applications enable users to create and maintain a secure environment that meets the security objectives of Communications and Information Systems (CIS) to handle all information.

The CIS Security Applications aim to ensure: the confidentiality of information by controlling the disclosure of, and access to information, supporting systems, services and resources; the integrity and availability of information, supporting systems, services and resources; the reliable identification and authentication of persons, devices and services accessing CIS; and the appropriate non-repudiation for individuals and entities having processed the information.

5.1.1.2 SMC Applications

The Service Management and Control (SMC) Applications enable users to 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.

5.1.1.3 Joint Applications

The Joint 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.

5.1.1.4 Air Applications

The Air 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 Applications

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

5.1.1.6 Maritime Applications

The Maritime 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 Applications

The Space 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 Applications

The Special Operations 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 Applications

The Joint Intelligence, Surveillance and Reconnaissance (JISR or Joint ISR) 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 Applications

The Logistics 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 Electronic Warfare Applications

The Electronic Warfare (EW) 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 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 Applications

The Environmental 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 Applications

The Missile Defence (MD) 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 Applications

The Civil-Military Co-operation (CIMIC) 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 Applications

The Chemical, Biological, Radiological and Nuclear (CBRN) 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 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 Applications

The Education, Training, Exercises and Evaluation (ETEE) 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 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 Stratcom Applications

The Strategic Communications (Stratcom) Applications enable users to collect, process, present and distribute information that supports the coordinated and appropriate use of NATO communications activities and capabilities on behalf of the Alliance policies, operations and activities, and in order to advance NATO's aims.

The aim of NATO Stratcom is to ensure that NATO audiences whether in the Nations or in a region where NATO operation is taking place, either friendly or adversarial, receives truthful, accurate and timely information that will allow them to understand and assess the Alliance’s actions and intentions.

The list of associated disciplines includes Public Diplomacy, Public Affairs (PA), Military Public Affairs, Information Operations (Info Ops), Psychological Operations (PSYOPS).

5.1.1.18 Modelling and Simulation Applications

The Modelling and Simulation (M&S) 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&S techniques and procedures can still produce invaluable contributions to military decision making.

5.1.1.19 Legal Applications

The Legal Applications enable users to collect, process, present and distribute information that supports the legal community. The legal community provides support in the disciplines of operational law, international law, contract and fiscal law, civilian and limited military personnel law, and environmental law.

5.1.1.20 Nuclear Applications

The Nuclear Applications enable users to collect, process, present and distribute information that supports the major functions of nuclear operations. Nuclear Operations are the set of military activities that are conducted by specially assigned forces from the military services, engaged in the planning and execution of operations and activities that involve nuclear weapons.

5.1.1.21 Human Resources Applications

The Human Resources (HR) Applications enable users to access, process and disseminate information on personnel and manpower. Through this application, operators can identify manpower levels, skill availability and manage personnel assignments. The application enables efficient and effective management of "Human Capital". The application function consists of tracking existing employee data which traditionally includes personal histories, skills, capabilities, accomplishments and salary.

The list of associated disciplines includes: Payroll, Work Time, Benefits Administration, Manpower, Human Resources (HR) Management Information, Recruiting, Training/Learning Management, Performance Record, and Employee Self-Service.

5.1.1.22 Information Management Applications

The Information Management (IM) Applications enable users to maintain assurance and management of information exchange for Information Superiority across an integrated and federated information sharing network. They specifically support those staff assigned formal responsibility for specific IM roles for planning, archiving, oversight, or registry.

IM features of Information Assurance, Information Security, and Identity Management (amongst others) are expressed in other application areas of the taxonomy. Basic Information Management functionality is provided to all information systems and applications through the Information Management Services.

5.1.1.23 Geospatial Applications

The Geospatial Applications enable users to view and manipulate geospatial information in two, three or four (with time) dimensional format. Geospatial applications support the concept of layering, filtering, time-space navigation and drill-down.

5.1.1.24 Office Automation Applications

The Office Automation Applications enable users to more effectively support, streamline, control and even automate office activities normally undertaken by individual users. The capabilities they support include generic business operations to collect, create or generate information, to organise, store and protect information, to retrieve, access, use, modify and disseminate information and to support its disposition and final destruction.

Office Automation Applications typically provide tailored User Interfaces specific to the type of information being created or manipulated and the office activities being undertaken. Such information types include documents, presentations, spreadsheets, projects, audio, video, still imagery and other standard information/data formats. Master data types include but may not be limited to Customer, Project and Workflow/Task records. Functionality to access and provision information and to automate processes may be limited or enhanced depending upon the Technical Services delivering them, the User Equipment supporting them and the User Profiles (metadata) of consumers accessing them.

Office Automation Applications should provide seamlessly integrated, consolidated, coherent and interoperable services and functionality, whilst maintaining assurance of and management of information and knowledge development; ensuring users are better able to produce information products as quickly as possible, with the least amount of human effort and of acceptable quality and assurance. To this end, they must also be integrated with other Information and Knowledge

Management applications and services, in order to ensure that they support the NATO Information Lifecycle.

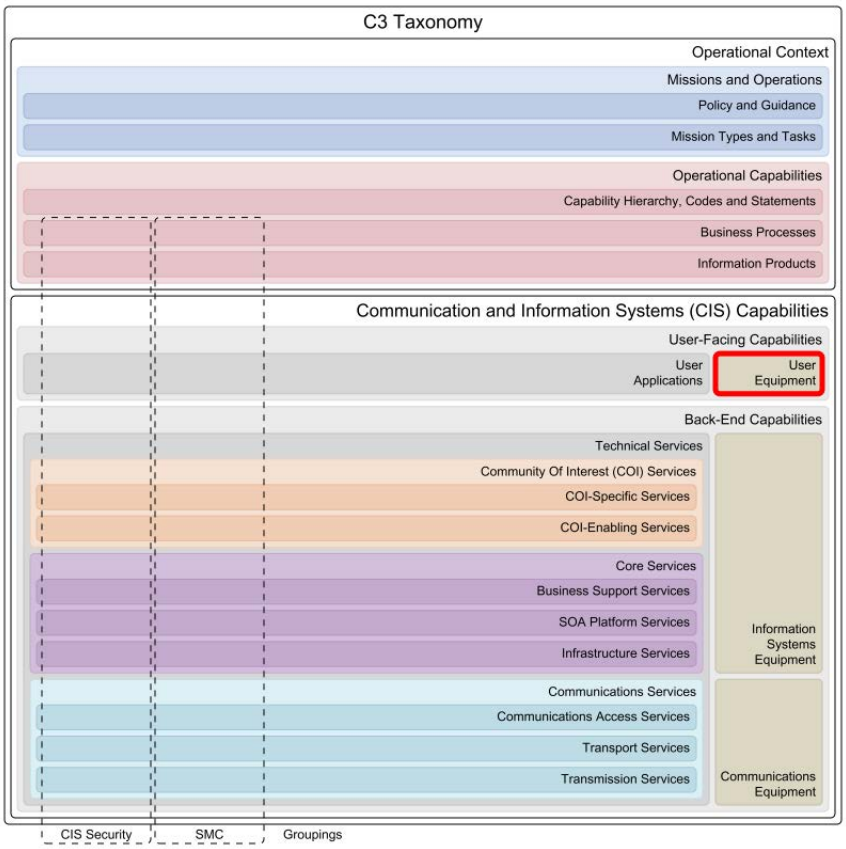
5.1.1.25 Communication and Collaboration Applications

The Communication and Collaboration Applications enable users to more effectively support the sharing of information and corporate knowledge between users across geographic locations. They facilitate an efficient and effective environment for coordination and cooperation between those users in achieving some determined and meaningful outcome to shared activities. The capabilities they support include conferencing, digital messaging, collaborative working and social networking.

Communication and Collaboration Applications support tailored User Interfaces specific to the communication channel and tool to be used and the collaborative activity to be undertaken. Functionality to communicate, access and provision information may be limited or enhanced depending upon the Technical Services delivering them, the User Appliances supporting them and the User Equipment (metadata) of consumers accessing them.

To be used effectively, Communication and Collaboration Applications should be employed to provide seamlessly integrated, consolidated, coherent and interoperable services and functionality. Indeed, these applications are often provided in a single package as unified messaging and collaboration platforms. However, it is important that they maintain the assurance of and management of information and knowledge exchange; ensuring collaborative users have the right information in the right place and at the right time and are able to stay connected with each other.

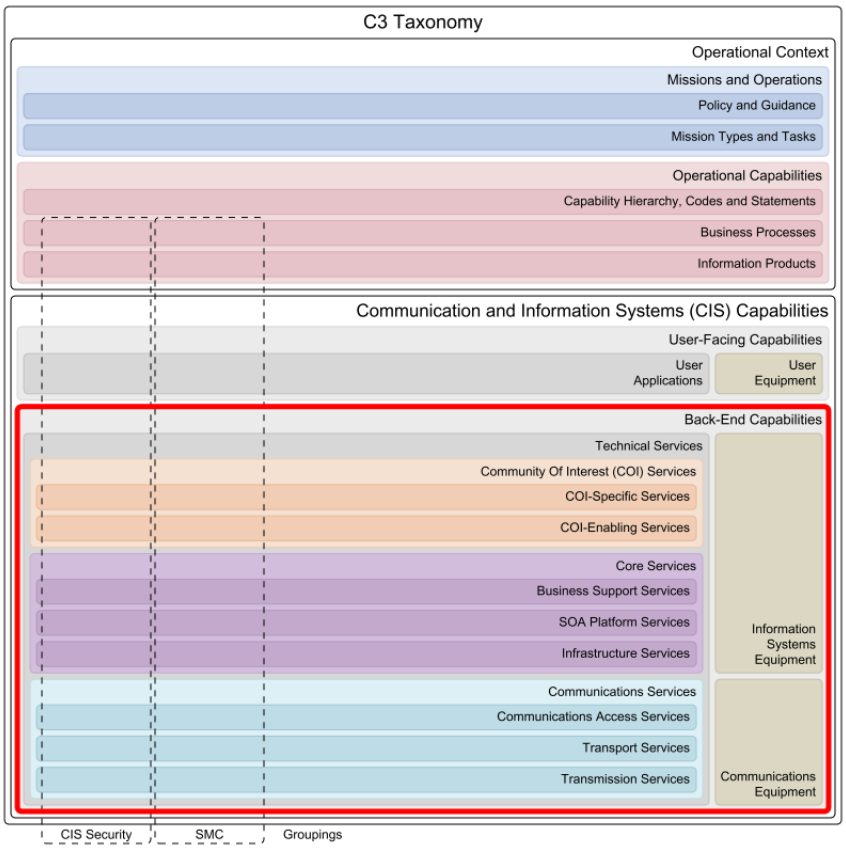
5.1.2 User Equipment



The "User Equipment" taxonomy layer represents the collection of equipment that is involved in the physical interface between users and User Applications. This equipment is deployed in various environments, which will have implications for ergonomics, form factors, physical and electrical specifications, and more.

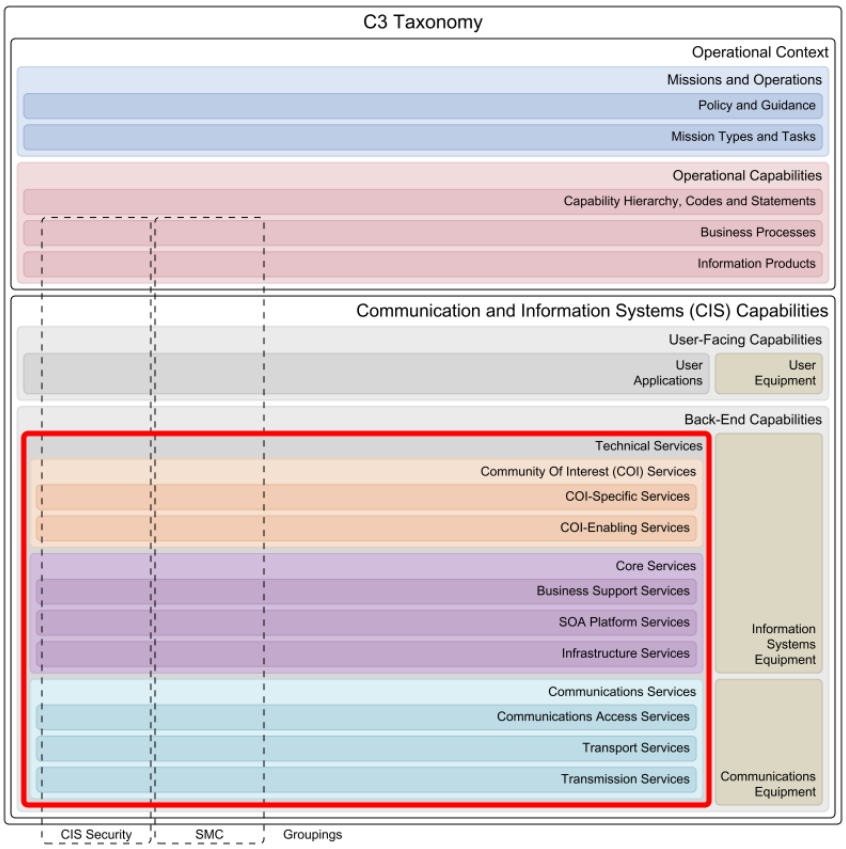
Examples of User Equipment are telephones, computers, laptops, tablets and peripherals (I/O units) including: terminals, card readers, optical character readers, magnetic tape units, mass storage devices, card punches, printers, video display units, data entry devices, teletypes, teleprinters, plotters, scanners, or any device used as a terminal to a computer and control units for these devices.

5.2 Back-End Capabilities



The "Back-End Capabilities" layer in the C3 Taxonomy represents the catalogue of services and equipment that is required to enable User-Facing Capabilities. The catalogue expresses the requirements for data processing and communications.

5.2.1 Technical Services

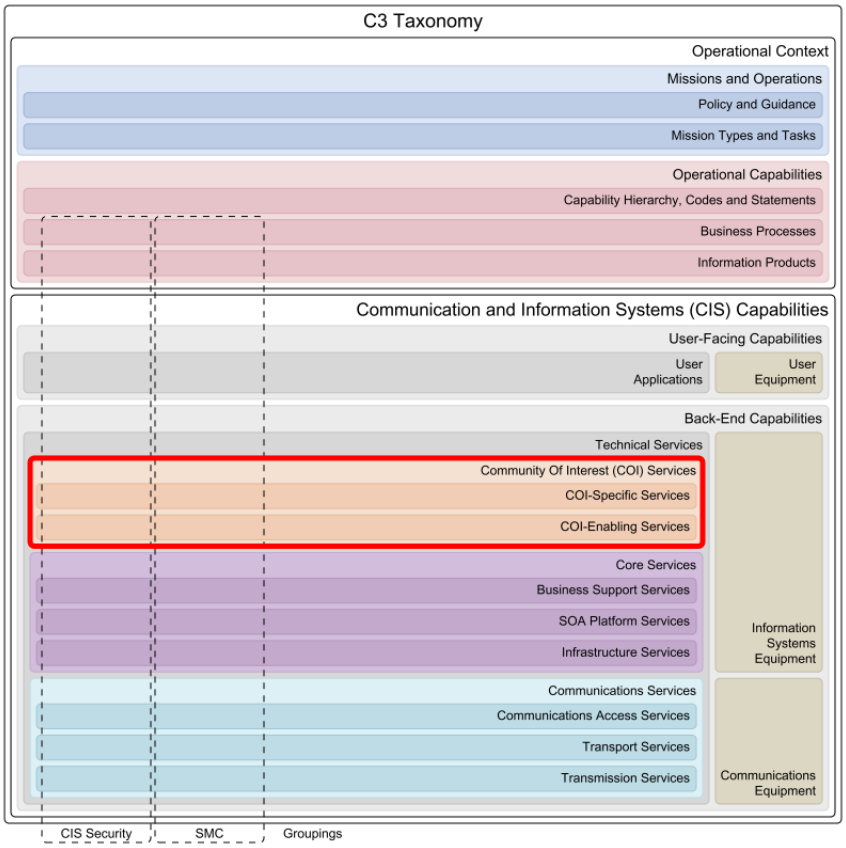


The "Technical Services" taxonomy layer represents the collection of services with requirements for software and hardware functionalities that can be reused for different purposes, together with the policies that should control their usage. These requirements are derived from the operational needs expressed by the collection of User-Facing Capabilities. Inherently, the Technical Services must support all Mission Types and Operational Capabilities.

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 sometimes referred to as the "Technical Services Framework" (TSF) or "NNEC Services Framework" (NSF).

5.2.1.1 Community Of Interest (COI) Services



The Community 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.

5.2.1.1.1 COI-Specific Services

The Community of Interest (COI)-Specific Services provide functionality as required by user communities in support of NATO operations, exercises and routine activities. These COI-Specific Services may have been previously referred to as "functional services" or "functional area services".

The NATO Network Enabled Capability (NNEC) shall provide a set of specific COI services in support of NATO operations and exercises that implement the tenets, architecture and standards set forth in the NNEC program and are interoperable with similar national capabilities.

5.2.1.1.1.1 COI-Specific CIS Security Services

The Community of Interest (COI)-Specific CIS Security Services provide the necessary means to implement and enforce CIS Security policies at the COI-specific level.

5.2.1.1.1.2 COI-Specific SMC Services

The Community of Interest (COI)-Specific Service Management and Control (SMC) Services provide the means to implement and enforce SMC policies at the COI-specific level.

5.2.1.1.1.3 Joint Services

The Joint 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.

When Joint Operations are carried out by military forces of two or more nations, they are known as Combined Joint Operations.

5.2.1.1.1.4 Air Services

The Air Services provide support to 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.

5.2.1.1.1.5 Land Services

The Land 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.

5.2.1.1.1.6 Maritime Services

The Maritime 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.

5.2.1.1.1.7 JISR Services

The Joint Intelligence, Surveillance and Reconnaissance (JISR) 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.

5.2.1.1.1.8 Logistics Services

The Logistics 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 execution of the movement, sustainment, and maintenance of forces.

5.2.1.1.1.9 Electronic Warfare Services

The Electronic Warfare (EW) Services provide unique computing and information services in support of Electronic Warfare operations, including tools for EW threat assessment, response planning, and coordination of force deployment, and operational reporting. 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.

5.2.1.1.1.10 Environmental Services

The Environmental 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.

5.2.1.1.1.11 CIMIC Services

The Civil-Military Co-operation (CIMIC) Services provide unique computing and information services for CIMIC 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.

5.2.1.1.1.12 ETEE Services

The Education, Training, Exercises and Evaluation (ETEE) Services provide unique computing and information services in support of ETEE Management, Education and Individual Training, Collective Training and Exercises and Evaluation.

5.2.1.1.1.13 Modeling and Simulation Services

The Modeling and Simulation (M&S) Services provide unique computing and information services for modeling and simulation support to operations. Modeling and Simulation are the set of activities that are undertaken to use models, emulators, simulators, and stimulators, to develop data in support of decision making.

5.2.1.1.2 COI-Enabling Services

The 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 group of communities (e.g. operational planning and situational awareness capabilities). A second distinction is that COI-Enabling Services tend to be specific for NATO's Consultation, Command and Control (C3) processes whereas Enterprise Support Services tend to be more generic and can be used by any business or enterprise.

5.2.1.1.2.1 COI-Enabling CIS Security Services

The Community of Interest (COI)-Enabling CIS Security Services provide the necessary means to implement and enforce CIS Security policies at the COI-enabling level.

5.2.1.1.2.2 COI-Enabling SMC Services

The 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.

5.2.1.1.2.3 Operations Planning Services

The Operations Planning Services provide the means to facilitate the collaborative development of plans and orders detailing the means to achieve a desired end state by employing available resources. Collaborative planning requires the decomposition of a plan to be defined and implemented by subordinated units. Once a plan is converted into an order and authorised, it is disseminated to the subordinated units for execution.

5.2.1.1.2.4 Tasking and Order Services

The Tasking and Order Services provide the means to develop and manage tasks and orders for operational forces. The services take into account national caveats, resource requirements and availability.

5.2.1.1.2.5 Situational Awareness Services

The Situational Awareness (SA) Services provide the means to support the knowledge of the elements in the battlespace required by a military commander to plan operations and exercise command and control and make well-informed decisions. The major components of Situational Awareness include an understanding of the status and disposition of the adversary, friendly forces, and the operational environment.

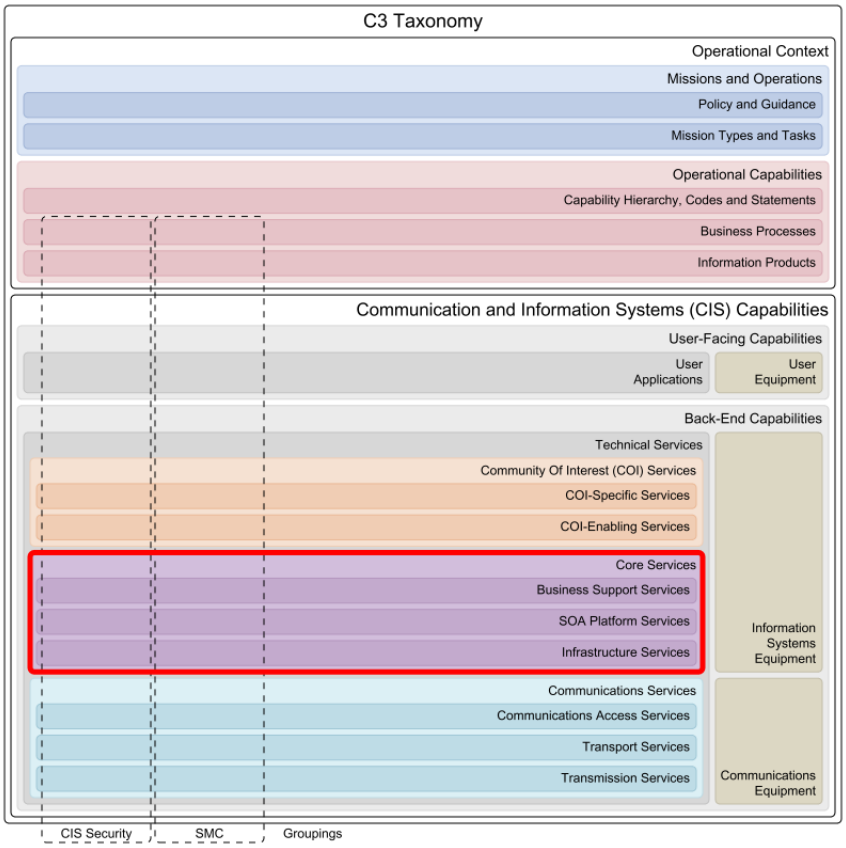
5.2.1.1.2.6 Battlespace Information Services

The Battlespace Information Services provide the means to allow the discovery, identification, access and collaboration of operationally relevant information. This information includes, but is not limited to, Battlespace Objects, Battlespace Events and Tracks.

5.2.1.1.2.7 Modeling and Simulation Enabling Services

The Modeling and Simulation (M&S) Enabling Services provide the means to enable simulation of tactical radio communications, understanding of Coalition Battle Management Language (CBML) and allow for the generation and management of Ground Truth Battlespace Objects (BSOs) and events which are used as input to simulations.

5.2.1.2 Core Services



The Core Services provide generic, Community of Interest (COI)-independent, technical functionality to implement service-based environments using infrastructure, architectural and enabling building blocks. Core Services provide these building blocks so that these generic, common capabilities do not have to be implemented by individual applications or other services.

5.2.1.2.1 Business Support Services

The Business Support Services provide the means to facilitate other service and data providers on the enterprise network by providing and managing underlying capabilities for collaboration and information management. These services are enablers used by other services and users across the whole network-enabled enterprise, acting as "building blocks" for developing more sophisticated Community Of Interest (COI) services and applications. Therefore, they are COI independent and they must be available to all enterprise members.

5.2.1.2.1.1 Business Support CIS Security Services

The Business Support CIS Security Services provide the necessary means to implement uniform, consistent, interoperable and effective web service security. These services also implement and enforce CIS Security policies at the enterprise support level.

5.2.1.2.1.2 Business Support SMC Services

The Business Support Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the enterprise support level.

5.2.1.2.1.3 Unified Communication and Collaboration Services

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

5.2.1.2.1.4 Information Management Services

The Information Management Services provide the means 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 organization. These services support 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.

5.2.1.2.1.5 ERP Services

The Enterprise Resource Planning (ERP) Services provide the means to cross-functional support for enterprise internal business processes by providing a real-time view of financial resource management, human resource management, supply chain management, customer relationship management, project management and process management activities.

5.2.1.2.1.6 Geospatial Services

The Geospatial Services provide the means to 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. Nonetheless, specialized services are also required, based on specific needs such as transformation of geographic coordinates and querying of catalogues.

5.2.1.2.2 SOA Platform Services

The 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.

5.2.1.2.2.1 SOA Platform CIS Security Services

The Service Oriented Architecture (SOA) Platform CIS Security Services provide a foundation to implement uniform, consistent, interoperable and effective web service security. They also provide the necessary means to implement and enforce CIS Security policies at the SOA platform level.

5.2.1.2.2.2 SOA Platform SMC Services

The 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.

5.2.1.2.2.3 Message-Oriented Middleware Services

The 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 different models of message exchange (direct, brokered, queues), exchange patterns (request/response, publish/subscribe, solicit response (polling for response), and for fire and forget), topologies (one-to-one, one-to-many) and modes of delivery (synchronous, asynchronous, long running). They also provide the support for routing, addressing, and caching.

5.2.1.2.2.4 Web Platform Services

The 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.

5.2.1.2.2.5 Information Platform Services

The 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.

5.2.1.2.2.6 Composition Services

The Composition Services will access and fuse data and behavior on demand, and return a single result to the consumer. The 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.

5.2.1.2.2.7 Mediation Services

The 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.

5.2.1.2.3 Infrastructure Services

The Infrastructure Services provide the foundation to host infrastructure services in a distributed and/or federated environment in support of NATO operations and exercises. They include computing, storage and high-level networking services that can be used as the basis 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 industry today as part of their Cloud Computing developments.

5.2.1.2.3.1 Infrastructure CIS Security Services

The Infrastructure CIS Security Services provide the necessary means to implement and enforce CIS Security policies at the infrastructure level.

5.2.1.2.3.2 Infrastructure SMC Services

The Infrastructure Service Management and Control (SMC) Services provide the means to implement and enforce SMC policies at the Infrastructure level. The services coordinate and communicate with other technical services (Communications Services, SOA Platform Services, etc.) to fulfill the requirements of service delivery. The requirements are translated into Infrastructure specific parameters and distributed to other Infrastructure Services.

5.2.1.2.3.3 Infrastructure Processing Services

The Infrastructure Processing Services provide shared access to physical and/or virtual computing resources. 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.

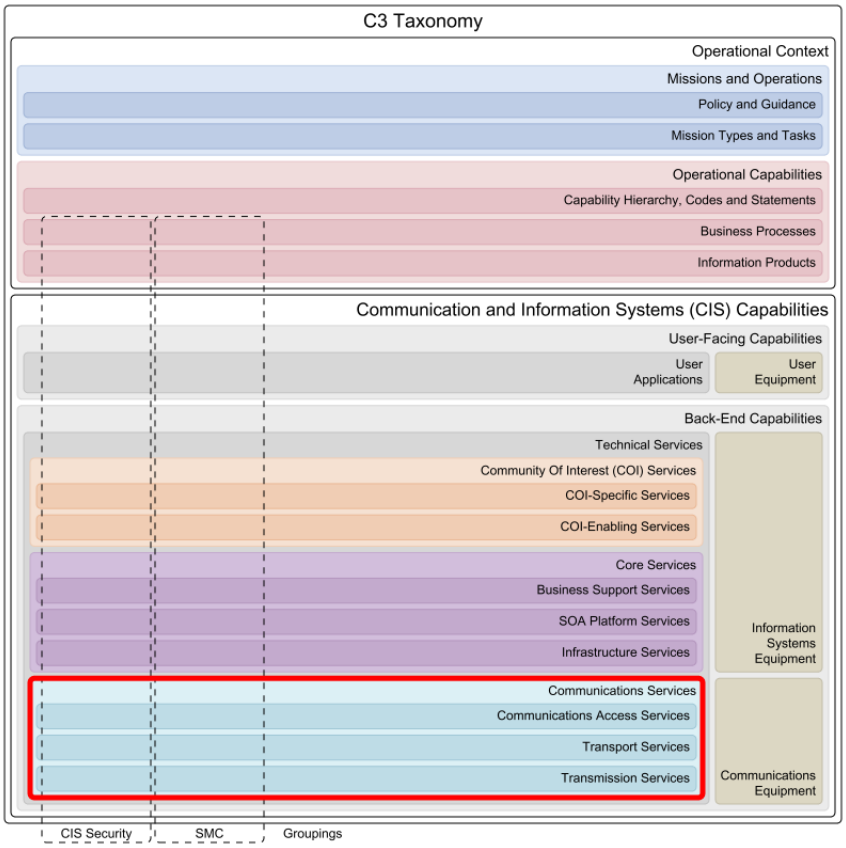
5.2.1.2.3.4 Infrastructure Storage Services

The 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.

5.2.1.2.3.5 Infrastructure Networking Services

The 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.

5.2.1.3 Communications Services



The 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.

The taxonomy of Communications Services takes a generic approach, listing elementary (vice complex) communications services, as building blocks of complex, end-to-end communications services. The granularity of the services described in this taxonomy is such that even the lowest level communications service, e.g. a user typing short free-text messages on a keypad and transmitting them over a UHF satcom DAMA radio, can be represented.

The required granularity is achieved by defining elementary service blocks. These are building blocks in complex end-to-end services, as those formulated in the NSOVs of the relevant reference architectures and derived target architectures. Elementary service blocks are agnostic to the resources and solutions that service providers can adopt to implement them and can be implemented over different communications segments (terrestrial, radio, satcom), by different service providers.

By concatenating these elementary services as building blocks, service architects can streamline and specify any complex communications service, end-to-end (e.g. DCIS service). In particular:

- Service blocks are concatenated to follow the flow of information, in a way similar to the actual communications infrastructure that is physically supporting the services. That makes the resulting Comms Service Maps understandable by network architects, service managers, and service providers. Comms Service Maps can be exported and used for a variety of purposes, from service level specification, to service management and control.
- Comms maps are two-dimensional representations of a complex communications service. Each service block along the chain can be assigned to different service providers, and clear interface and service delivery or service peering boundaries can be defined between them.
- Service providers can select and involve the resources and the technical solutions that best meet the service level specifications for each block, under the constraints posed by the operational context, and by the connectivity/interaction with adjacent service blocks (implemented by other service providers). These constraints shall be reflected in the service level specification.
- In the NATO context, service providers can be NATO organic providersproviders (e.g. NCI Agency, e.g. providing Access Services), a NATO Nation or a consortium/group of nations (e.g. providing Transport Services and Transmission Services over military-controlled communications infrastructure), as well as commercial providers (e.g. providing Transmission

Services over commercial infrastructure).

5.2.1.3.1 Communications Access Services

The 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. Because they are defined end-to-end, in a comms service map, the same Access Service block can be found at both ends of the link, and will often (but not necessarily) be implemented and managed by the same service provider.

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. In most cases, they involve the direct connection of hosts or end-user devices that interface the service on a given layer of the communications stack.

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

5.2.1.3.1.1 Communications Access CIS Security Services

The Communications Access CIS Security Services provide a foundation to implement and enforce CIS Security policies at the communications access level.

5.2.1.3.1.2 Communications Access SMC Services

The Communications Access Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the communications level.

The Communications Access SMC Services are based on the TM Forum Business Process Framework (eTOM) process area Operations and specifically Resource Management & Operations.

Within the context of SMC for all Communications Services, the functions and subsequent requirements on each the three layers - Communications Access Services, Transport Services and Transmission Services - experience a great overlap and high level of similarity. Therefore all SMC Services for these layers are defined under Communications Access SMC Services, while they are valid for the other two layers just the same.

5.2.1.3.1.3 Analogue Access Services

The Analogue Access Services provide the delivery or exchange of analogue signals over an analogue interface port, without manipulation (encoding, compression) of the original signal, and directly interfacing a Transmission Service.

5.2.1.3.1.4 Digital Access Services

The Digital (link-based) Access Services provide the delivery or exchange of digital signals (synchronous or asynchronous) over a native digital interface port, usually a port providing Transmission Services, at channel access level (e.g. the modem port of a handheld satcom terminal).

5.2.1.3.1.5 Message-based Access Services

The Message-based Access Services provide the delivery or exchange of formatted messages, through user appliances that are directly connected to a Transmission Service (e.g. the keypad of a VHF radio).

5.2.1.3.1.6 Packet-based Access Services

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

5.2.1.3.1.7 Frame-based Access Services

The Frame-based Access Services provide the 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.

5.2.1.3.1.8 Circuit-based Access Services

The Circuit-based Access Services provide the delivery or exchange of raw user data, via fractional access to digital lines (circuits), e.g. ISDN BRI, fractional E1, etc. These services are provided 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 Access Services), or directly to Transmission Services (e.g. ISDN port of an Inmarsat satcom terminal).

5.2.1.3.1.9 Multimedia Access Services

The Multimedia Access Services provide the delivery or exchange of multimedia data via interaction with the end-user or end-user application. The services support the adaptation of the media involved (analogue voice, video, digital desktop, etc) for delivery or exchange over packet-based, frame-based, circuit-based, or digital (link-based) access services (through e.g. routers, switches, terminal adapters or multiplexers, or directly over a digital port).

5.2.1.3.2 Transport Services

The Transport Services correspond to 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.

5.2.1.3.2.1 Transport CIS Security Services

The Transport CIS Security Services provide a foundation to implement and enforce CIS Security policies at the communications transport level.

5.2.1.3.2.2 Transport SMC Services

The Transport Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the communications transport level.

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.

Within the context of SMC for all Communications Services, the functions and subsequent requirements on each the three layers - Communications Access Services, Transport Services and Transmission Services - experience a great overlap and high level of similarity. Therefore all SMC Services for these layers are defined under Communications Access SMC Services, while they are valid for this layer just the same.

5.2.1.3.2.3 Edge Services

The 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).

5.2.1.3.2.4 Transit Services

The Transit 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 Transit Services (e.g. routers, switches, radio relays, SATCOM transponders, etc) may operate at different points across the core of the network. The Transit 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 Packet-, Frame- and Circuit-based Transport Services. Nonetheless, Transit Services are not concerned with emulated Communications Access Services or Packet-, Frame- and Circuit-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.

Transit 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 Transit Service is specified and will form part of the Service Level Specification (SLS).

5.2.1.3.2.5 Aggregation Services

The Aggregation Services provide the aggregation of traffic over parallel converging transmission paths, and involves Packet-, Frame- and Circuit-based 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 Transit Services, Aggregation Services can be closely mapped to the OSI stack lower layers.

5.2.1.3.2.6 Broadcast Services

The Broadcast Services provide the distribution of transport flows through a combination both the "within the core" and "at the edge" infrastructure types to form a logical "ring'. Broadcast Services within the core involve the broadcast of transport flows towards multiple edge-points that connect to the broadcast node either directly over transmission lines or through Transit Services. Broadcast Services at the edge involve the broadcast of traffic flows towards multiple end-nodes that connect to the broadcast node over transmission lines.

Broadcast Services involve Packet-, Frame- and Circuit-based 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).

5.2.1.3.3 Transmission Services

The 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.

5.2.1.3.3.1 Transmission CIS Security Services

The Transmission CIS Security Services provide a foundation to implement and enforce CIS Security policies at the communications transmission level.

5.2.1.3.3.2 Transmission SMC Services

The Transmission Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the communications transmission level.

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.

5.2.1.3.3.3 Wired Transmission Services

The Wired Transmission Services support physical transfer of data, point-to-point or point-to multipoint, using wired transmission medium amongst two or more static nodes. Based on range and capacity, these services are distinguished for Local Area Networks (LAN - over relatively short distances), Metropolitan Area Networks (MAN - medium to high capacity over distances spanning tens of kilometers) or Wide Area Networks (WAN - high capacity wired transmission medium over long distances).

5.2.1.3.3.4 Wireless LOS Static Transmission Services

The 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.

5.2.1.3.3.5 Wireless LOS Mobile Transmission Services

The 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).

5.2.1.3.3.6 Wireless BLOS Static Transmission Services

The 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.

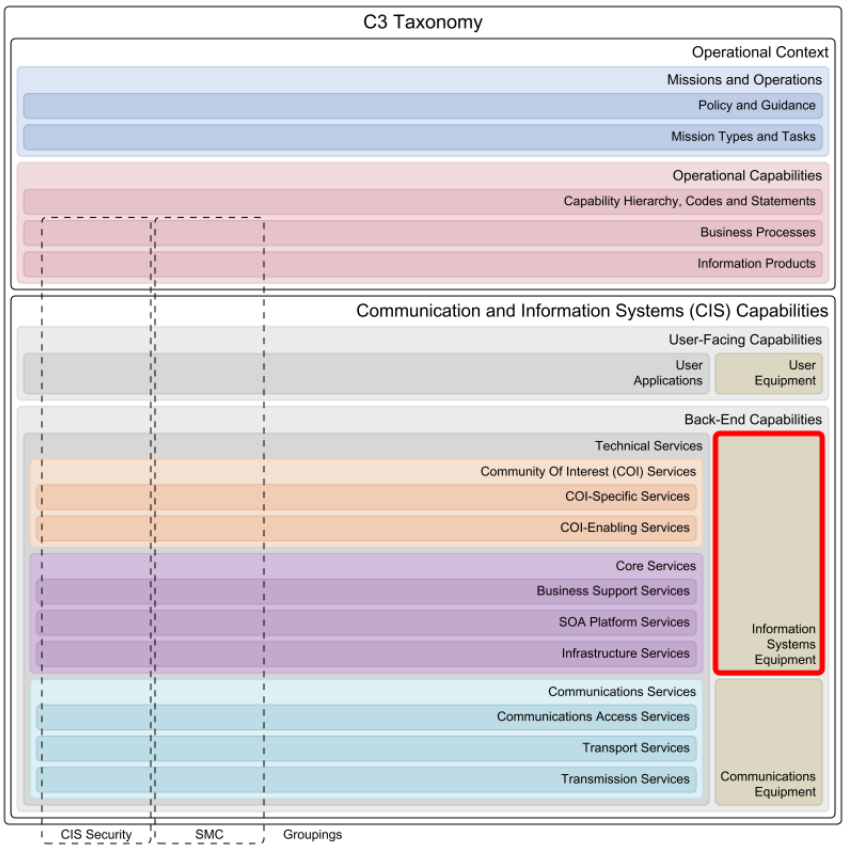
In the context of these services, the wireless transmission path between the static nodes can be established passively (i.e. wireless signal is refracted back to earth by different atmospheric layers) or actively (i.e. wireless signal is transmitted back to earth via a transponder). In the case when 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.

5.2.1.3.3.7 Wireless BLOS Mobile Transmission Services

The 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).

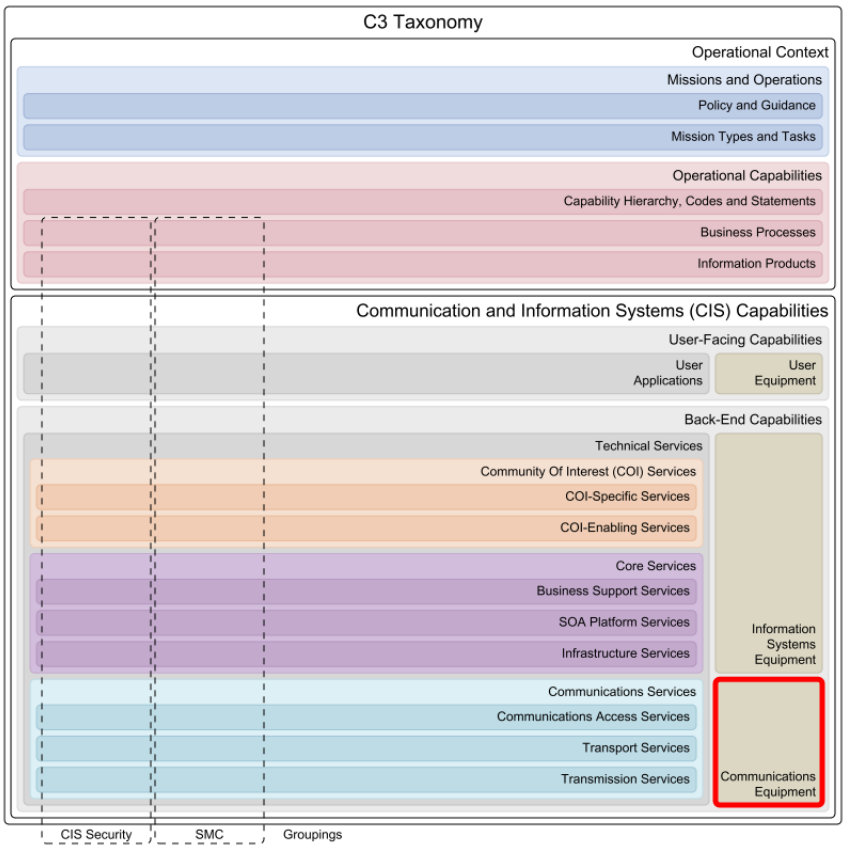
5.2.2 Information Systems Equipment



The "Information Systems Equipment" taxonomy layer represents the collection of equipment that is involved in hosting software for the provision of Community Of Interest (COI) Services and Core Services, as well as the handling of operational data of the enterprise.

Examples of Information Systems (IS) Equipment include database servers, file servers, application servers, 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.

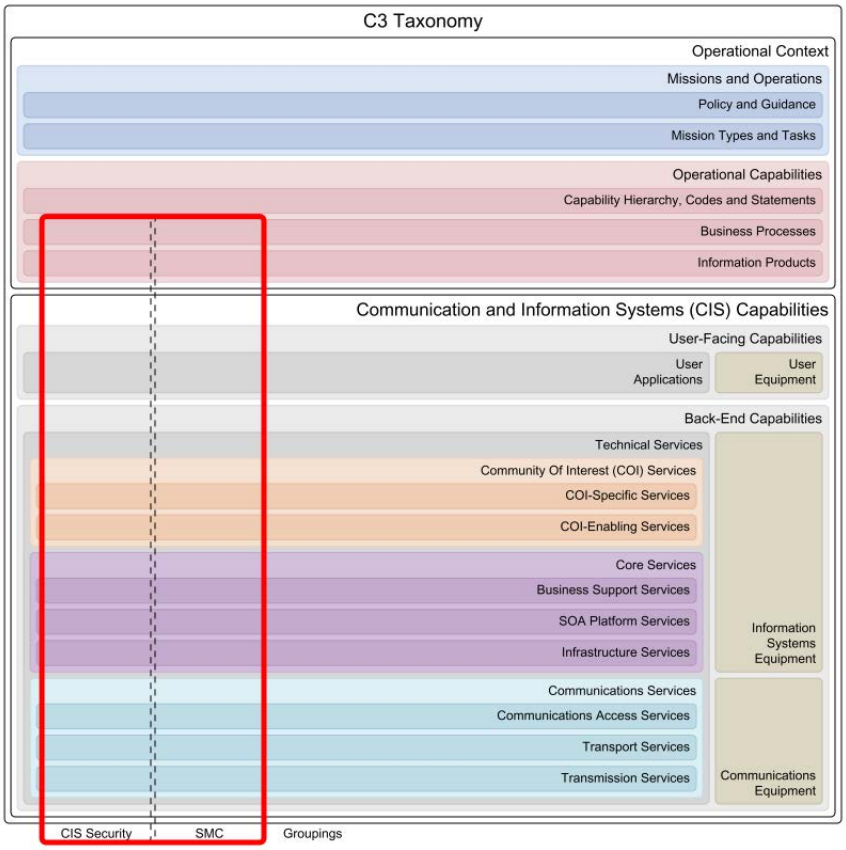
5.2.3 Communications Equipment



The "Communications Equipment" taxonomy layer represents the collection of equipment that is involved in the 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 Taxonomy into a collection with a particular common characteristic. Two significant examples are the CIS Security 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 CIS Security

CIS Security provides a collection of measures to protect the information that is processed, stored or transmitted in communication, information or other electronic systems in respect to confidentiality, integrity, availability, non-repudiation and authentication.

The CIS Security grouping overlaps with most levels (horizontal layers) of the C3 Taxonomy. It should therefore not be seen as a level itself and rather as a logical grouping of critical components that jointly implement the tenets of CIS Security 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 levels (horizontal layers) of the C3 Taxonomy. It should therefore not be seen as a level by itself and rather as a logical grouping of critical components that jointly provide the tools to manage and control a distributed and federated service-oriented enterprise.

C3 Taxonomy

Operational Context

Missions and Operations

Policy and Guidance

- Strategic Concept
- Political Guidance
- Military Guidance
- Allied Publications
- Policies and Directives

Mission Types and Tasks

- Collective Defence (CD)
- Counter Terrorism (CT)
- Conflict Prevention (CP)
- Support to Humanitarian Assistance (SHA)
- Military Aid/Support to Civil Authorities (SCA)
- Antiterrorism (AT)
- Counter Insurgency (COIN)
- Peace Enforcement (PE)
- Peacebuilding (PB)
- Support of Non-Combatant Evacuation Operations (NEO)
- Permanent Tasks
- Consequence Management (CM)
- Peacekeeping (PK)
- Peacemaking (PM)
- Support to Disaster Relief (DR)
- Extraction Operation (EOP)
- Enforcement of Sanctions and Embargoes (ESE)

Operational Capabilities

Capability Hierarchy, Codes and Statements

- Prepare
- Project
- Engage
- Sustain
- Protect
- Inform
- Consult, Command & Control

Business Processes

- CIS Security Processes
- SMC Processes
- Governance Processes
- Management Processes
- Consultation Processes
- Cooperation Processes
- C2 Processes
- Support Processes

Information Products

- CIS Security Information
- SMC Information
- Intent & Guidance
- Rules & Measures
- Plans
- Tasking & Orders
- Situational Awareness
- Resource Status
- Requests & Responses
- Reports

Communication and Information Systems (CIS) Capabilities

User-Facing Capabilities

User Applications

- CIS Security Applications
- SMC Applications
- Joint Applications
- Space Applications
- Logistics Applications
- Environmental Applications
- CBRN Applications
- Modelling and Simulation Applications
- Geospatial Applications
- Communication and Collaboration Applications
- Air Applications
- Maritime Applications
- JISR Applications
- CIMIC Applications
- ETEE Applications
- Legal Applications
- Human Resources Applications
- Office Automation Applications
- Land Applications
- Special Operations Applications
- Electronic Warfare Applications
- Missile Defence Applications
- Stratcom Applications
- Nuclear Applications
- Information Management Applications

User Equipment

Back-End Capabilities

Technical Services

Community Of Interest (COI) Services

COI-Specific Services

- COI-Specific CIS Security Services
- COI-Specific SMC Services
- Joint Services
- Maritime Services
- Logistics Services
- Environmental Services
- ETEE Services
- Air Services
- Land Services
- JISR Services
- Electronic Warfare Services
- CIMIC Services
- Modeling and Simulation Services

COI-Enabling Services

- COI-Enabling CIS Security Services
- COI-Enabling SMC Services
- Operations Planning Services
- Tasking and Order Services
- Situational Awareness Services
- Battlespace Information Services
- Modeling and Simulation Enabling Services

Core Services

Business Support Services

- Business Support CIS Security Services
- Business Support SMC Services
- Unified Communication and Collaboration Services
- Information Management Services
- ERP Services
- Geospatial Services

SOA Platform Services

- SOA Platform CIS Security Services
- SOA Platform SMC Services
- Message-Oriented Middleware Services
- Web Platform Services
- Information Platform Services
- Composition Services
- Mediation Services

Infrastructure Services

- Infrastructure CIS Security Services
- Infrastructure SMC Services
- Infrastructure Processing Services
- Infrastructure Storage Services
- Infrastructure Networking Services

Information Systems Equipment

Communications Services

Communications Access Services

- Communications Access CIS Security Services
- Communications Access SMC Services
- Analogue Access Services
- Digital Access Services
- Message-based Access Services
- Packet-based Access Services
- Frame-based Access Services
- Circuit-based Access Services
- Multimedia Access Services

Transport Services

- Transport CIS Security Services
- Transport SMC Services
- Edge Services
- Transit Services
- Aggregation Services
- Broadcast Services

Transmission Services

- Transmission CIS Security Services
- Transmission SMC Services
- Wired Transmission Services
- Wireless LOS Static Transmission Services
- Wireless LOS Mobile Transmission Services
- Wireless BLOS Static Transmission Services
- Wireless BLOS Mobile Transmission Services

Communications Equipment

CIS Security | SMC | Groupings

Baseline 2.0 - Tuesday, 10 November 2015

ENCLOSURE 4 TO
6300 TSC FCX 0010/TT-151521
DATED: 19 NOV 15

RELEASE NOTES FOR C3 TECHNICAL SERVICES TAXONOMY

BASELINE 2.0

Introduction

The C3 Technical Services (C3TS) Taxonomy has been developed by the Technology and Human Factors (THF) Branch at Headquarters SACT, as a product complementary to the C3 Taxonomy. Both products, at different levels, help to map the complexities of NATO C3 landscape and to provide an environment in which relevant and meaningful architectural products can be generated, analyzed, improved, and disseminated. Where the scope of the C3 Taxonomy covers the whole NATO Federated Environment - connecting political and military ambitions to CIS capability components - the C3TS Taxonomy classifies in more detail the technical services of NATO and National CIS capabilities.

Background

The C3TS Taxonomy has become a foundation piece for the Enterprise Architecture program of work of Allied Command Transformation, streamlining the production and use of architectures. The product however was never formally endorsed by the C3 Board, and remained used internally.

The THF architecture team worked on the Enterprise Architecture and the further development and improvement of the Enterprise Mapping (EM) Wiki, their architecture tool. As a product of this continued effort, the C3TS Taxonomy has proven to be useful as a common language for CIS community while addressing complex issues of interoperability and standardization.

A new federated approach to operations, promoted by the FMN concept, has highlighted the need for a common language for the definition of technical services in order to enable interoperability. The C3 Board advised ACT to seek the formal endorsement of the C3TS Taxonomy to support development of federated architectures. Following the C3 Board advice, and after having received valuable input

from the Nations, ACT is releasing with this document a baselined, initial version of C3TS Taxonomy.

To simplify configuration management, a version of both the C3 Taxonomy and the C3TS Taxonomy have been baselined at the same time and labeled as version 2.0. Therefore the first formal release of the C3TS Taxonomy will be referred to as "C3TS Taxonomy 2.0".

Purpose

The main purpose of the C3TS Taxonomy is to provide the common language and understanding of the CIS technical services landscape. The taxonomy has emerged as a consensus building effort, where exerts from Nations, academia and industry contributed their perspectives and knowledge.

The C3TS Taxonomy is already enabling the NATO Enterprise to develop new and update existing CIS capabilities in a coherent manner. Ultimately, it shall form the common foundation for all logical level architectures in the Alliance and partner nations. The use of a common C3TS Taxonomy will considerably simplify the identification and standardization of interoperability points, and promote the fast development and reuse of technology solutions.

ENCLOSURE 5 TO
6300 TSC FCX 0010/TT-151521
DATED: 19 NOV 15

C3 Technical Services Taxonomy Perspective, Baseline 2.0

Table of Contents

1 Introduction

The "Technical Services" layer in the C3 Taxonomy represents the collection of services with requirements for 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 Mission Types and Operational Capabilities.

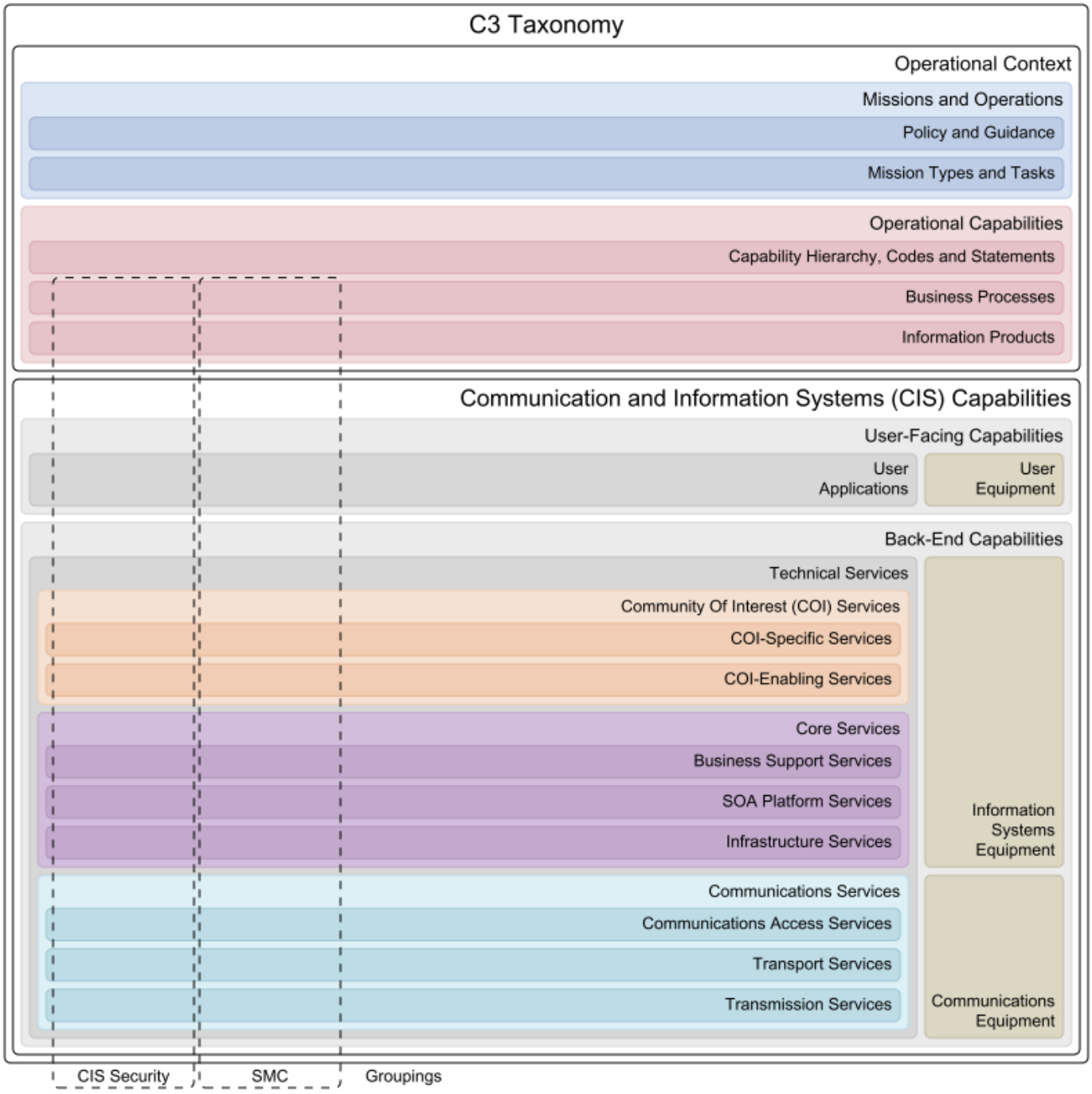
Technical Services are implemented in a federated model that allows NATO and the Nations to jointly provide a robust and secure platform on top of which powerful User Applications can be run. Thus the Technical Services provide the foundation for the NATO Network Enabled Capability (NNEC). They must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

This document contains the C3 Technical Services Taxonomy Perspective that accompanies the C3 Technical Services Taxonomy Poster. All information in this document is automatically derived from the Allied Command Transformation (ACT) Command, Control, Deployability and Sustainability (C2DS) Division's Enterprise Mapping (EM) Wiki. A version of this document is generated every day and the date on the cover must be used for version control purposes.

The complete taxonomy of Technical Services is sometimes referred to as the "Technical Services Framework" (TSF) or "NNEC Services Framework" (NSF).

For the purpose of this document, a 'taxonomy' is defined as a 'particular' classification arranged in a hierarchical structure organised by supertype-subtype relationships. 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.

2 Overarching Context



2.1 C3 Taxonomy

The C3 Taxonomy is a model that represents the concepts and their relationships involved in all the life-cycle activities for NATO's Consultation, Command and Control (C3) capabilities. The C3 Taxonomy provides a tool and common language to synchronize these activities and improve connecting NATO's Strategic Concept and Political Guidance through levels of ambition expressed in 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 NATO's CIS capabilities but did so in relative isolation. Today, we are confronted with a patchwork quilt of systems, applications, services, standards, vocabularies and taxonomies. Even simple English words, such as service or capability, have become highly ambiguous. As a result of this stove-piping, NATO now faces a very complex CIS fabric that is not interoperable and attempts to solve this

problem is often hampered by lack of mutual understanding.

The purpose of this C3 Taxonomy is to capture concepts from various communities and record them for item classification, integration and harmonization purposes. Recognizing their dependencies and relationships, the taxonomy plots and associates political and military ambitions, Mission-to-Task Decomposition, Capability Hierarchy, Statements and Codes, Business Processes, Information Products, User Applications, Technical Services and Equipment definitions and requirements to Reference Documents, Standards, Patterns, Increments and other concepts.

In an analogy to geographical surveying, this approach is referred to as "enterprise mapping", since the C3 Taxonomy charts NATO's complex C3 landscape. As with geographic elements on maps, the assignment of colors, fonts and positions of taxonomy elements in the poster, and the assignment of text, numbering and indentation in the report have particular meaning. The mapping of the taxonomy elements is rich in semantic relations that provide the orientation between the concepts. The environment of the concepts is arranged in separate "layers" (vs. grid) and the granularity (vs. scale) in the "levels" of detail.

The data for the C3 Taxonomy is registered, processed and maintained on the Enterprise Mapping (EM) Wiki, a protected internet-facing website run by Allied Command Transformation (ACT). This website contains far more information than is made available through the C3 Taxonomy poster and this document; information about lower levels in the taxonomy and the linkage between the here mentioned taxonomy items and other concepts are available for registered users on the EM Wiki via https://tide.act.nato.int/em.

2.2 CIS Capabilities

The C3 Taxonomy layer for the "Communication and Information System (CIS) Capabilities" represents the logical components of the capabilities required to meet NATO's information system and communication needs in support of Missions and Operations.

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, and digital products. Organizations and individuals rely on information systems to manage their operations, supply services, and augment personal lives.

2.3 Back-End Capabilities

The "Back-End Capabilities" layer in the C3 Taxonomy represents the catalogue of services and equipment that is required to enable User-Facing Capabilities. The catalogue expresses the requirements for data processing and communications.

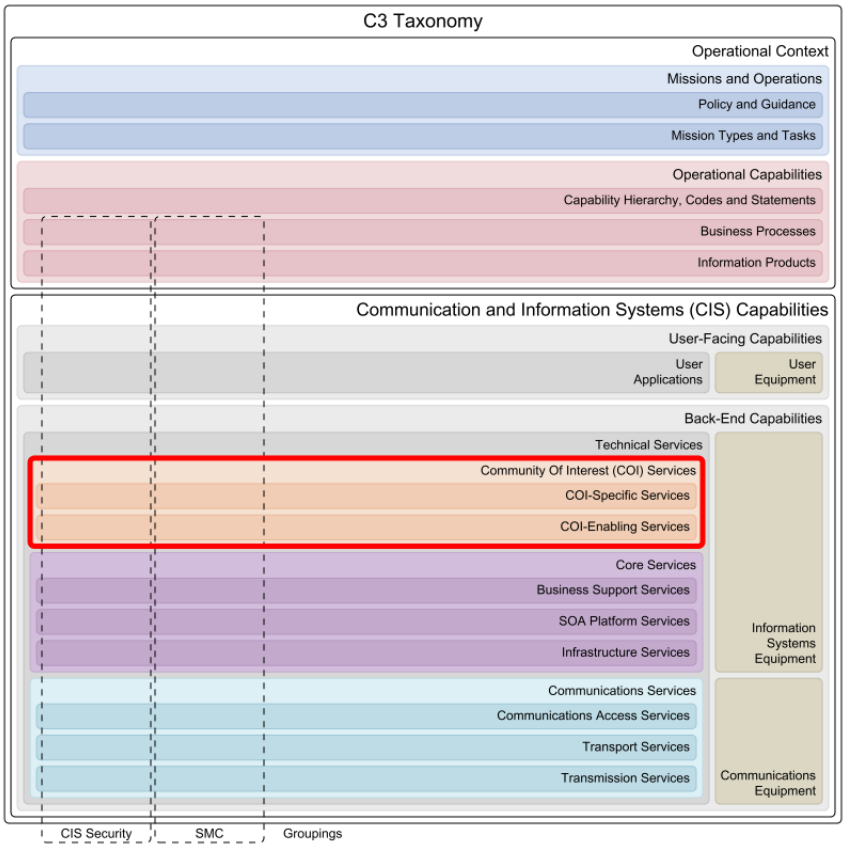
2.4 Technical Services

The "Technical Services" taxonomy layer represents the collection of services with requirements for 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 Mission Types and Operational Capabilities.

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.

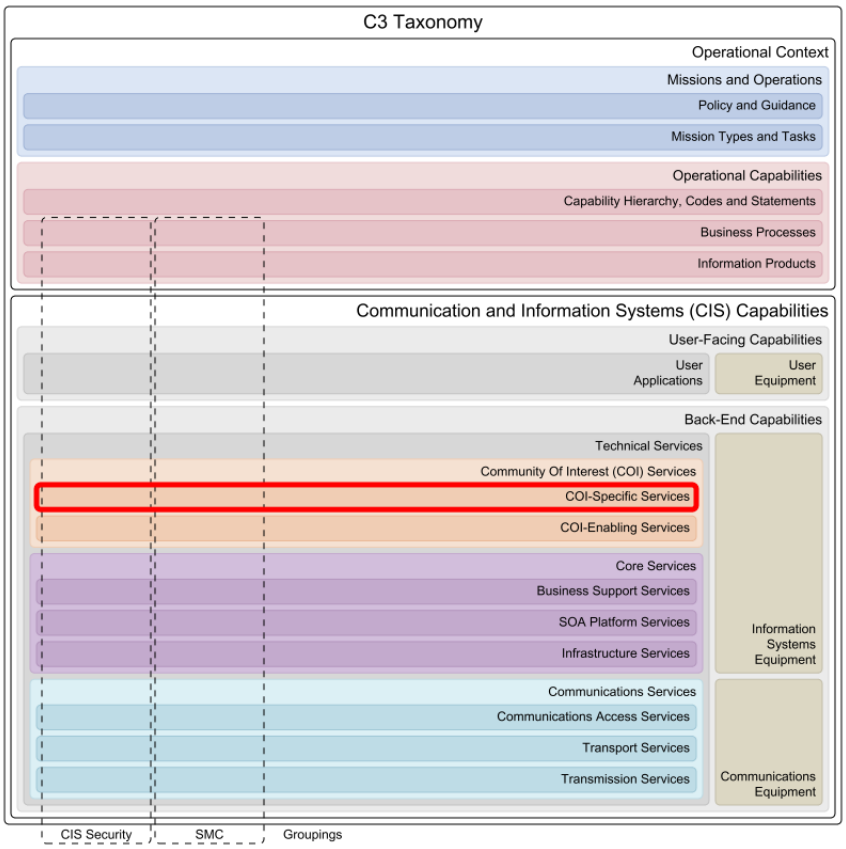
The complete collection of Technical Services is sometimes referred to as the "Technical Services Framework" (TSF) or "NNEC Services Framework" (NSF).

3 Community Of Interest (COI) Services



The Community 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.

3.1 COI-Specific Services



The Community of Interest (COI)-Specific Services provide functionality as required by user communities in support of NATO operations, exercises and routine activities. These COI-Specific Services may have been previously referred to as "functional services" or "functional area services".

The NATO Network Enabled Capability (NNEC) shall provide a set of specific COI services in support of NATO operations and exercises that implement the tenets, architecture and standards set forth in the NNEC program and are interoperable with similar national capabilities.

3.1.1 COI-Specific CIS Security Services

The Community of Interest (COI)-Specific CIS Security Services provide the necessary means to implement and enforce CIS Security policies at the COI-specific level.

3.1.1.1 Recognized Cyber Picture Services

The Recognized Cyber Picture (RCP) Services provide means to produce, manage and disseminate the correlated and fused cyber picture, providing enhanced situational awareness of the cyber domain, including on-going activities and their relationships. The Recognized Cyber Picture Services provide a near-real-time representation of all-source cyber data (current and planned).

3.1.1.2 Cyber Defence Services

The Cyber Defence Services provide the means to plan, develop, disseminate, execute and manage cyber defence tasks and activities.

3.1.1.3 CIS Security Audit Analysis Services

The CIS Security Audit Analysis Services provide functionality to periodically and systematically review the application of CIS security during operations. The CIS Security Audit Analysis Services process collected information relating to policy compliance and risk management to gather evidence of undesirable behaviors and effects. These services support the presentation of findings to the appropriate authorities for the purpose of accountability.

3.1.1.4 Advanced Threat Management Service

The Advanced Threat Management Service enable to collect data, process data into data objects and control that the process is followed.

3.1.1.5 Electronic Key Management Services

The Electronic Key Management Services (EKMS) provide the means to centrally manage electronic cryptography keys, including related accounting, distribution and technologies. The services also support entities that use key material by producing and consuming the keys in common key formats.

3.1.2 COI-Specific SMC Services

The Community of Interest (COI)-Specific Service Management and Control (SMC) Services provide the means to implement and enforce SMC policies at the COI-specific level.

3.1.2.1 Spectrum Management Services

The Spectrum Management Services provide the means to assign, regulate and police the assignment of Radio Frequency (RF) spectrum. The Spectrum Management Services support the aim to maximise the utilization of RF spectrum, while avoiding interference and and pollution of the RF spectrum.

3.1.2.2 Spectrum Usage Information Services

The Spectrum Usage Information Services provides access to information describing the actual usage of the Radio Frequency (RF) spectrum.

3.1.2.3 Call Management Services

The Call Management Services provide the means to design and implement rules and parameters governing the routing of inbound telephone calls through a network. These rules determine how calls are distributed according to the time and/or date of the call as well as the location of the caller (usually defined by the outbound Caller ID). Call Management Services also incorporate the use of calling features such as Call Queues, IVR Menus, Hunt Groups and Recorded Announcements to provide a customised experience for the user and to maximize the efficiency of inbound call handling.

3.1.2.4 VTC Management Services

The Video Tele-Conference (VTC) Management Services provide the means to manage and maintain a video conferencing network and the scheduling of video meetings. These services provide diagnostic tools for system-by-system and conference-by-conference records, diagnostics for rapid support response, management of on-site and remote video systems, and scheduling of video, audio, web and data conferences.

3.1.3 Joint Services

The Joint 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.

When Joint Operations are carried out by military forces of two or more nations, they are known as Combined Joint Operations.

3.1.3.1 Surface Area Management Services

The Surface Area Management Services provide the means to manage requests and allocation of 2-D surface areas. The Surface Area Management Services support the determination of resource availability, deconfliction and scheduling of 2-D areas.

3.1.3.2 NATO Crisis Response Measures Services

NATO Crisis Response Measures Services provide supporting functionalities for planning applications.

3.1.4 Air Services

The Air Services provide support to 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.

3.1.4.1 Recognized Air Picture Services

The Recognized Air Picture (RAP) Services provides the means to produce, manage and disseminate the Recognized Air Picture. These services will generate a de-conflicted and agreed picture of the air environment through the collection, aggregation, correlation and fusion of information from multiple sources.

3.1.4.2 Aeronautical Information Services

The Aeronautical Information Services ensure the flow of information necessary for the safety, regularity and efficiency of international air navigation.

The manner in which aeronautical information is gathered and managed is governed by Annex 15 to the Convention on International Civil Aviation (ICAO Annex 15), which defines how Aeronautical Information Services shall receive and/or originate, collate or assemble, edit, format, publish/store and distribute specified aeronautical information/data. The goal is to satisfy the need for uniformity and consistency in the provision of aeronautical information/data that is required for operational use by international civil aviation.

ICAO Annex 15 specifies that aeronautical information should be published as an integrated aeronautical information package (IAIP), composed of the following elements: The Aeronautical Information Publication (AIP), including amendment services, Aeronautical Information Circulars (AIC), NOTAM (Notice to Airmen) and Pre-flight Information Bulletins (PIB).

Each element is used to distribute specific types of aeronautical information.

3.1.4.3 ACO Services

The Airspace Control Order (ACO) Services provide the ability to create, update, manage, validate, consume and disseminate Airspace Control Orders.

3.1.4.4 Air Asset List Services

The Air Asset List Services provide functionality to create, update and prioritize information objects in the form of an asset list. The service will allow for the management of multiple asset lists, including, but not limitted to: the Critical Asset List (CAL), Joint Prioritized Critical Asset List (JPCAL) and Joint Prioritized Defended Asset List (JPDAL).

3.1.4.5 ATO Services

The Air Tasking Order (ATO) Services create, maintain and manage the information object representing the ATO.

3.1.4.6 Airspace Management Services

The Airspace Management Services provide the functionality for allocation, management and deconfliction of the air space by implementing, specifying and providing guidance on Fire Support Control Measures (FSCMs) and Airspace Control Means (ACMs).

3.1.4.7 Airspace Structure Management Services

The Airspace Structure Management Services deliver functionality to create, maintain, update, de-conflict and prioritize the information objects representing Airspace Structures. Airspace Structures are divided into two main categories: controlled airspace and uncontrolled airspace. In controlled airspace, aircraft in the air or on the ground, receive Air Traffic Control (ATC) service in accordance with the airspace classification. In uncontrolled airspace, all aircraft do their own separation according to general rules.

3.1.4.8 Airlift Services

The Airlift Services provide the ability to create, update manage and prioritize execution processes and communications connectivity for tasking and coordination of airlift operations.

3.1.4.9 Air Threat Analysis Services

The Air Threat Analysis Services provide automated threat ranking and notification of airborne vehicles according to a pre-configured set of threat ranking criteria.

3.1.4.10 Air Weapon Matching Services

The Air Weapon Matching Services deliver functionality to match targets to platforms able to achieve desired effects (lethal and non-lethal) whilst minimising undesirable effects (e.g collateral damage). The services provide the best combination of aircraft, missiles, weapons, yields, heights of burst, fuses and delivery tactics to use against individual targets.

3.1.4.11 Air Mobility Analysis Services

The Air Mobility Analysis Services provide the means to analyse, de-confilict and manage all air mobility operations into, out of, and within multiple Areas of Responsibility (AOR) and/or Joint Operations Areas (JOA).

3.1.5 Land Services

The Land 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.

3.1.5.1 Recognized Ground Picture Services

The Recognized Ground Picture (RGP) Services provide the means to produce, manage and disseminate the Recognised Ground Picture (RGP). The RGP is the compilation of validated data relating to a defined ground area that is disseminated to enable situational awareness and support decision making at all levels. The RGP Services will support the development of the RGP through the collection, aggregation, correlation and fusion of information from multiple sources.

3.1.5.2 Manoeuver Planning Services

The Manoeuver Planning Services establish manoeuver corridors, Angles of Attack (AOAs), and optimal path, taking into account constraints imposed unit formations, equipment, topography and coverage areas.

3.1.5.3 Task Time Location Management Services

The Task Time Location Management Services provides the means to manage temporal and location constraints on an assigned task. The Task Time Locations Management Services provide support for both branch and sequel courses of action.

3.1.5.4 Terrain Analyzer Services

The Terrain Analyzer Services provides the means to identify constraints and opportunities driven by the terrain through analysis of sensor coverage, weapon coverage, communication coverage and topography.

3.1.5.5 Task Classifier Services

The Task Classifier Services provides the means to classify assigned, implied and supported tasks into the standardised Force Tasks terms defined by NATO.

3.1.5.6 Force Comparison Services

The Force Comparison Services provide quantitative and qualitative comparison of forces and specifies Measures of Effectiveness (MOEs) / Measures of Effectiveness (MOPs) for force component combinations.

3.1.6 Maritime Services

The Maritime 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.

3.1.6.1 Recognized Maritime Picture Services

The Recognized Maritime Picture (RMP) Services provide the means to create, manage and disseminate the Recognised Maritime Picture. These services will generate a de-conflicted and agreed picture of the maritime environment through the collection, aggregation, correlation and fusion of information from multiple sources.

3.1.6.2 Maritime Anomaly Detection Services

The Maritime Anomaly Detection Services provide information and alerts about merchant shipping behavior that differs from the expected behaviour. Maritime shipping anomalies include, but are not limited to: ships outside shipping lanes; ships that loiter at drift, that rendezvous, or hug the coast; ships that suddenly accelerate to leave an area; ships in high interest areas known for smuggling, and AIS ship identification (MMSI, Name, IMO, Call Sign) discrepancies.

3.1.6.3 Water Space Management Services

The Water Space Management (WSM) Services provide the means to perform computational analysis concerning WSM / Prevention of Mutual Interference (PMI) of tracks over specified periods of time. This include interference checking, request and notification; waterspace request management; waterspace deconfliction; waterspace allocation.

3.1.6.4 Mine Warfare Services

The Mine Warfare Services provides the means to calculate the percentage cleared of single and multiple coverage plans (uniform and non-uniform) against known mine threats. The Mine Warfare Services provide the means to perform risk analysis (including mine burial prediction) for routes, segments and patrol areas.

3.1.6.5 Amphibious Warfare Services

The Amphibious Warfare Services deliver functionality to automatically determine delay and distance measurements, Position of Intended Movement (PIM), Closest Point of Approach (CPA) interception directions, Modified Surf Index (MSI) values and suitability of landing areas.

3.1.6.6 Sonar Prediction Services

The Sonar Prediction Services provides the access to analytical functions required to predict sonar behavior as a function of environment, target, automatic target recognition algorithm, and sensor characteristics. These services provide the probability of detection, false alarm and classification for a specific sonar.

3.1.7 JISR Services

The Joint Intelligence, Surveillance and Reconnaissance (JISR) 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.

3.1.7.1 Intelligence Requirements Management Services

The Intelligence Requirements Management Services provide the means to access and manage intelligence requirements, related information objects, their status and relationship to decision making. The Intelligence Requirements Management Services will also provide the means to generate and consume Requests for Information (RFIs).

The services will allow for the management and tracking of intelligence requirements, and related information objects, throughout the intelligence cycle (direction, collection, processing, analysis, dissemination and feedback).

3.1.7.2 JISR Collection and Exploitation Plans Services

The Joint Intelligence, Surveillance and Reconnaissance (JISR) Collection and Exploitation Plans Services provide the means to create and manage collection and exploitation plans for required intelligence. These plans include collection and exploitation activities, resource allocation, linkages to battlespace objects, and traceable relationship to intelligence requirements.

3.1.7.3 JISR Sensor Services

The Joint Intelligence, Surveillance and Reconnaissance (JISR) Sensor Services provide the means to retrieve sensor capabilities, plan sensor usage, exercise command & control and manage sensor observations.

3.1.7.4 JISR Exploitation Services

The Joint Intelligence, Surveillance and Reconnaissance (JISR) Exploitation Services provides the means to exploit collected JISR data. The services will provide the means to analyse and verify the collected data against the intelligence requirements. In support of analysis, the JISR Collection and Exploitation Plans Services will allow for the transformation, classification, and matching of collected data.

3.1.7.5 JISR Analysis and Production Services

The Joint Intelligence, Surveillance and Reconnaissance (JISR) Analysis and Production Services provide the means to correlate and fuse multi-source data, and analyze correlated/fused data for the purposes of battle damage assessment. The Services support the production of information products required for decision making.

3.1.7.6 JISR Reporting Services

The Joint Intelligence, Surveillance and Reconnaissance (JISR) Reporting Services provide the means to retrieve exiting information structures required to produce intelligence reports. These structures may originate from multiple supporting services and include extracted or compiled ISR products, data and metadata, including their relationships to JISR products and intelligence requirements.

3.1.7.7 JISR Imagery and Video Services

The Joint Intelligence, Surveillance and Reconnaissance (JISR) Imagery and Video Services provide the means to manage, analyze and manipulate imagery and video products. The service maintains the relationships between the imagery, video products and intelligence requirements while supporting the production of intelligence products sufficient for decision making.

3.1.8 Logistics Services

The Logistics 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 execution of the movement, sustainment, and maintenance of forces.

3.1.8.1 Recognized Logistic Picture Services

The Recognized Logistics Picture (RLP) Services provide the means to create, manage and disseminate the Recognized Logistics Picture. These services will generate a de-conflicted and agreed picture of the logistics environment through the collection, aggregation, correlation and fusion of information from multiple sources.

3.1.8.2 Recognized Medical Picture Services

The Recognized Medical Picture (RMedP) Services provide the means to create, manage and disseminate the Recognised Medical Picture. These services will generate a de-conflicted and agreed picture of the medical environment through the collection, aggregation, correlation and fusion of information from multiple sources.

3.1.8.3 Casualty Rate Estimation Services

The Casualty Rate Estimation Services provide functionality to estimate casualty rates based on various scenarios (e.g. conventional, CBRN). These services will evaluate risk probabilities as well as provide confidence levels for these estimates.

3.1.9 Electronic Warfare Services

The Electronic Warfare (EW) Services provide unique computing and information services in support of Electronic Warfare operations, including tools for EW threat assessment, response planning, and coordination of force deployment, and operational reporting. 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.

3.1.9.1 Emitter Services

The Emitter Services provide the means to access, manage and distribute parametric and related information, on electromagnetic emitters. The Emitter information is relevant to the conduct of Electronic Warfare (EW).

3.1.9.2 Emitter Analysis Services

The Emitter Analysis Services provide standardised functions used in the analysis and assessment of observed and deployed emitters. The functions will include, but are not limited by: correlation, direction finding, coverage analysis, threat rings, lines of bearing, etc.

3.1.9.3 Restricted Frequency List Services

The Restricted Frequency List Services provide the means to create, manage and share a list of restricted frequencies and related meta-data.

3.1.10 Environmental Services

The Environmental 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.

3.1.10.1 Recognized Environmental Picture Services

The Recognized Environmental Picture (REP) Services provides the means produce, manage and disseminate the Recognized Environmental Picture. These services provide the means produce a de-conflicted and agreed picture of the geospatial, oceanographic, hydrographic and meteorological environment through the combination, aggregation, correlation and fusion of data from multiple sources.

3.1.10.2 Geography Services

The Geography Services provide access to high-level spatial and temporal value-added information, and related computation functions. Geography Services provide geographers the means to analyse the spatial and the temporal distribution of phenomena, processes, and features, as well as, the interaction of humans with their environment.

3.1.10.3 Meteorology Services

The Meteorology Services provide the means to access to atmospheric information and weather forecasting algorithms. The Meteorology Services provide the means to manage and retrieve value added information relating to meteorological information.

3.1.10.4 Oceanography Services

The Oceanography Services provide access to high-level value-added information, and related computational functions required by oceanographers. The Oceanography Services assist oceanographers in the study and prediction of marine ecosystems dynamics, ocean currents, waves, geophysical fluid dynamics; plate tectonics and the geology of the sea floor; fluxes of various chemical substances and physical properties within the ocean and across its boundaries.

3.1.10.5 Hydrography Services

The Hydrography Services provide access to high-level and value-added information, and related conputational functions required by hydrographers. The Hydrography Services assist hydrographers in mapping/charting the water's topographic features by measuring the depths, tides, and currents of a body of water, establishing the topography and morphology of seas, rivers, and lake beds.

3.1.10.6 Space Weather Services

The Space Weather Services provide access to high-level information and computational algorithms for forecasting weather in space. The Space Weather Services provide information and forecasts of conditions on the sun, in the solar wind, magnetosphere, ionosphere and thermosphere that can influence the performance and reliability of space-borne and ground-based technological systems and can endanger human life or health.

3.1.11 CIMIC Services

The Civil-Military Co-operation (CIMIC) Services provide unique computing and information services for CIMIC 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.

3.1.11.1 Behaviour Analysis Services

The Behaviour Analysis Services provide the means to analyse current behaviour, and predict future behaviour, of civilian populations with respect to changes in environmental stimulus. The Behaviour Analysis Services utilizes demographic information and specialized behaviour models to preform these analyses. The analysis will include the identification population segments, their location, key stimuli, predicted behaviour, and timeline for forthcoming activities and events.

3.1.11.2 Pattern Analysis Services

The Pattern Analysis Services provide the means to derive key factors, in real-time, from multiple information sources and compare them against predetermined patterns and thresholds for a match. Matched patterns will trigger an alert to inform key personnel to take action. These services will provide quick identification of changes in the environment that affect the civilian population. The alerting function supports a timely and measured response.

3.1.12 ETEE Services

The Education, Training, Exercises and Evaluation (ETEE) Services provide unique computing and information services in support of ETEE Management, Education and Individual Training, Collective Training and Exercises and Evaluation.

3.1.12.1 Objectives Management Services

The Objectives Management Services provide the means to develop and manage exercise, experimentation and training objectives of a collective training and exercise event in order to deliver approved objectives of the event.

3.1.12.2 MEL MIL Management Services

The Master Event List (MEL) / Master Incident List (MIL) Management Services provide the means to collaboratively develop event and incident lists in support of Exercise planning. The MEL/MIL Services will also provide support to Exercise Control during exercise execution.

3.1.13 Modeling and Simulation Services

The Modeling and Simulation (M&S) Services provide unique computing and information services for modeling and simulation support to operations. Modeling and Simulation are the set of activities that are undertaken to use models, emulators, simulators, and stimulators, to develop data in support of decision making.

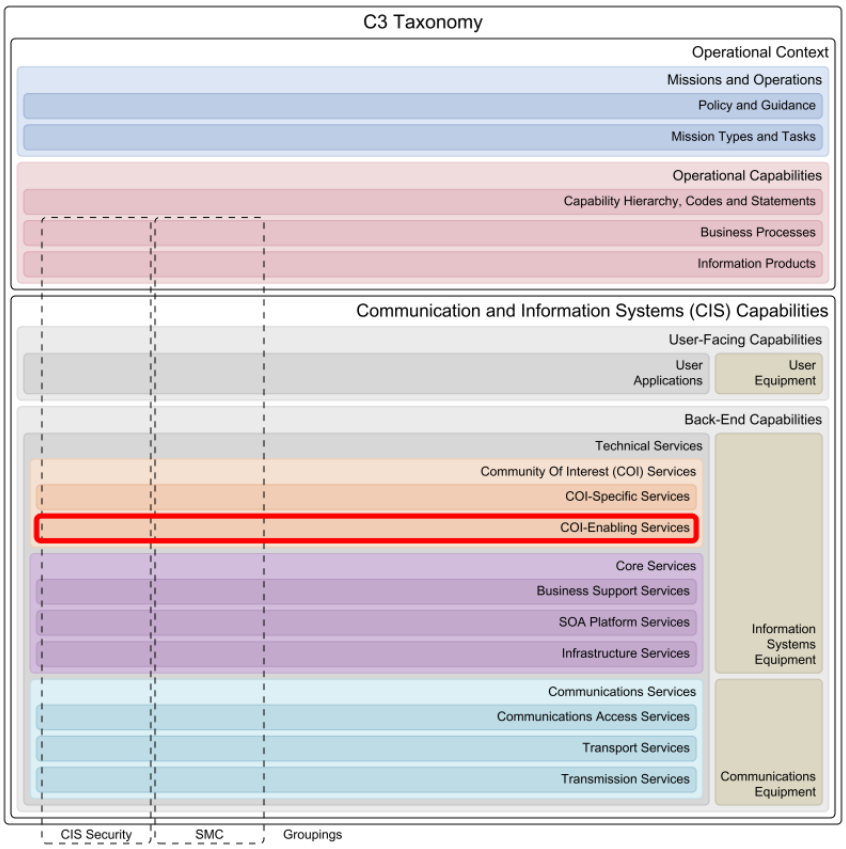
3.1.13.1 Modeling and Simulation Infrastructure Services

The Modeling and Simulation Infrastructure Services provide the services to build and maintain an infrastructure environment for Modeling and Simulation (M&S) activities.

3.1.13.2 Modeling and Simulation Integration Services

The Modeling and Simulation Integration Services provide the services to configure and integrate Modeling and Simulation (M&S) activities into service architectures.

3.2 COI-Enabling Services



The 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 group of communities (e.g. operational planning and situational awareness capabilities). A second distinction is that COI-Enabling Services tend to be specific for NATO's Consultation, Command and Control (C3) processes whereas Enterprise Support Services tend to be more generic and can be used by any business or enterprise.

3.2.1 COI-Enabling CIS Security Services

The Community of Interest (COI)-Enabling CIS Security Services provide the necessary means to implement and enforce CIS Security policies at the COI-enabling level.

3.2.1.1 Cyber Threat Detection Services

The Cyber Thread Detection Services detect multiple types of malware, as well as blended threats and spam. It works closely with other security services to provide a security approach that protects from multiple simultaneous types of attack vectors.

3.2.2 COI-Enabling SMC Services

The 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.

3.2.2.1 Data Exchange Monitoring Services

The Data Exchange Monitoring Services (DEMS) provide a capability to monitor, measure and assess connectivity, quality of data exchanges and information flows between Community of Interest (COI) Services. The DEMS will leverage existing open standards and STANAGs to monitor and assess the quality of existing data flows.

3.2.3 Operations Planning Services

The Operations Planning Services provide the means to facilitate the collaborative development of plans and orders detailing the means to achieve a desired end state by employing available resources. Collaborative planning requires the decomposition of a plan to be defined and implemented by subordinated units. Once a plan is converted into an order and authorised, it is disseminated to the subordinated units for execution.

3.2.3.1 Deployment Plan Services

The Deployment Plan Services enable the creation and management of Detailed Deployment Plans (DDP) which describe the planned movement of military units in support of an operation in accordance with the commanders requirements. It supports the synchronization of resources to ensure the right units, equipment, supplies, and capabilities arrive in the correct order at the appropriate locations to avoid saturation of nodes and Lines of Communication (LOC). Deployment Plan Services also provide the means for the coordination of air, sea, rail and road movements, tracking, reprioritization and re-routing. It supports alternative routes and the assessment of the implications and results of such alternatives, providing deconfliction and validation of plans feasibility.

3.2.3.2 Courses of Action Services

The Courses of Action (COAs) Services support development, update, validation, wargaming and comparison of COAs. A Course of Action is an option that during the estimate process, contributes to the accomplishment of a task and from which a detailed plan is developed.

3.2.3.3 Synchronisation Matrix Services

The Synchronisation Matrix Services facilitates the development of a timeline of planned effect, tasks, objectives and the phasing information within a Course of Action (COA). It provides functionality to identify the potential interdependencies between events. During the execution of an operation the Synchronisation Matrix Services supports the comparison of actual operational data with the selected COA to ensure efforts are actually aligned and effective.

3.2.3.4 Order of Battle Services

The Order of Battle (ORBAT) Services enable the management and sharing of the military organizational structures including all command relationships, rotation of forces, transfer of authority and changes to these factors over time. It provides functionality to manage updates such as the transfer of a force that moves out of the ORBAT while another unit moves in.

3.2.3.5 Operation Plan Development Services

The Operation Plan Development Services enables creation and management of strategic, operational and tactical Operation Plans (OPLANs) including the development of Concept of Operations (CONOPS) and provisional Combined Joint Statement of Requirements (CJSOR).

3.2.3.6 Targeting Services

The Targeting Services provide the means to select and prioritize targets, while matching the appropriate target response. A target is an entity or object considered for possible engagement or action. It may be an area, complex, installation, force, equipment, capability, function, individual, group, system, entity, or behavior identified for possible action to support the Commander's objectives, guidance, and intent.

3.2.4 Tasking and Order Services

The Tasking and Order Services provide the means to develop and manage tasks and orders for operational forces. The services take into account national caveats, resource requirements and availability.

3.2.4.1 Resource Request Services

The Resource Request Services enable the development, disemination and management of resource requests. It provides functionality to analyze and collate resource requests so that they are prioritized considering the competing needs, the associated risks and return on investment.

3.2.4.2 Resource Allocation Services

The Resource Allocation Services support the development, management and dissemination of resource allocations. The Resource Allocation Services utilize Measures of Effectiveness (MOEs) and Measures of Performance (MOPs) as optimizing criteria and constraints. The Resource Allocation Services allow the specification of rules for automatic allocation of tasks to units and equipment.

3.2.4.3 Operations Estimation Services

The Operations Estimation Services enables analysis of the required resources needed to achieve success in the execution of an operation or task under certain constraints. An operation or a task is achieved successfully when the objectives and effects set by the Commander are met.

3.2.4.4 Tasking Services

The Tasking Services enable users to construct and issue tasking, as well as receive responses from assets and track the execution of the task.

3.2.4.5 Operations Assessment Services

The Operations Assessment Services provide assessment support during the execution of operations. The services calculate the Measures of Effectiveness (MoE) and Measures of Performance (MoP) from operational data to determine how well an operation is progressing toward the desired effects, objectives and end state.

3.2.4.6 Operations Order Services

The Operations Order Services provide the means to create, manage, disseminate, track and view digital representation of the Operations Order (OPORD), Warning Order (Wng O) and Fragmentary Orders (FRAGOs).

3.2.5 Situational Awareness Services

The Situational Awareness (SA) Services provide the means to support the knowledge of the elements in the battlespace required by a military commander to plan operations and exercise command and control and make well-informed decisions. The major components of Situational Awareness include an understanding of the status and disposition of the adversary, friendly forces, and the operational environment.

3.2.5.1 Recognized Picture Services

The Recognized Picture Services provide the means to create, manage and disseminate Recognized Pictures required by the Commander to monitor and plan operations, enabling situational awareness and supporting decision making. The Recognized Picture Services support the generation of a de-conflicted and agreed picture through the collection, aggregation, correlation and fusion of information from multiple sources.

3.2.5.2 Symbology Services

The Symbology Services enables rendering of standard military or mission specific symbology sets. The Symbology Services allows the rendered images to be used as overlays on maps or as standalone illustrations.

3.2.6 Battlespace Information Services

The Battlespace Information Services provide the means to allow the discovery, identification, access and collaboration of operationally relevant information. This information includes, but is not limited to, Battlespace Objects, Battlespace Events and Tracks.

3.2.6.1 Battlespace Event Services

The Battlespace Event Services allow retrieval, storage and processing of data about an incident, phenomenon or occasion of military significance for which planning is not known. Battlespace Event Services provide also the means to mantain record of actions of own troops, enemy activity, illegal activities such as Improvised Explosive Device (IED) finds, natural disasters and major accidents which happen in a particular time and place and impact (effect) someone or something (objective).

3.2.6.2 Battlespace Object Services

The Battlespace Object Services allow for the discovery, identification, access, exchange and modification of operationally relevant Battlespace Objects (BSOs). It enables Order of Battle (ORBAT), Operations and Orders, and Key Personnel to uniquely reference BSOs.

3.2.6.3 Track Services

The Track Services provide functionality to collect and monitor the precise position and movement details of relevant entities in near-real time to enhance Situational Awareness and Command and Control. The Track Services allows for the combination, processing and dissemination of all tracks available from all sensors while allowing for consumer driven filtering when required.

3.2.7 Modeling and Simulation Enabling Services

The Modeling and Simulation (M&S) Enabling Services provide the means to enable simulation of tactical radio communications, understanding of Coalition Battle Management Language (CBML) and allow for the generation and management of Ground Truth Battlespace Objects (BSOs) and events which are used as input to simulations.

3.2.7.1 Battlespace Simulation Services

The Battlespace Simulation Services enables the storage and processing of a language that describes a commander's intent and is to be understood by simulation systems.

3.2.7.2 Radio Simulation Services

Radio Simulation Services provides the means to simulate tactical radio communication. Such a simulation is desirable in situations where real radio frequency devices cannot be used or during Collective Training Exercises (CTE).

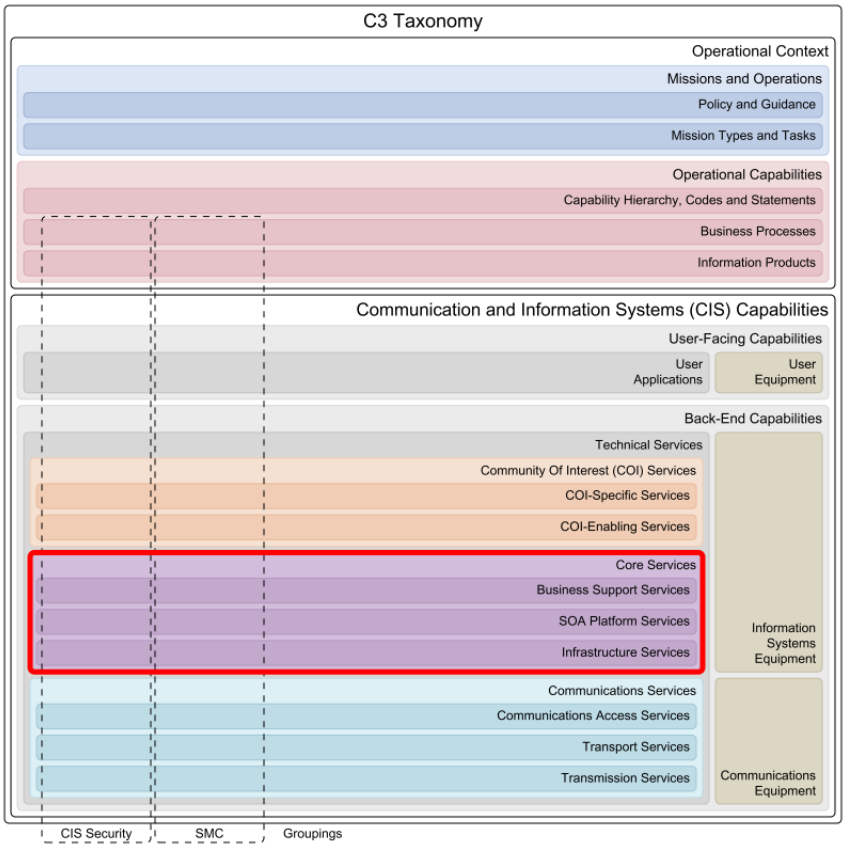
3.2.7.3 Ground Truth Battlespace Objects Services

Ground Truth Battlespace Objects Services allow for the discovery, exchange, access and modification of Ground Truth Battlespace Objects (BSOs) which are generated as input to simulations. Ground Truth Battlespace Objects Services enable the stimulated development of percieved truth BSOs by Battlespace Object Services.

3.2.7.4 Ground Truth Battlespace Events Services

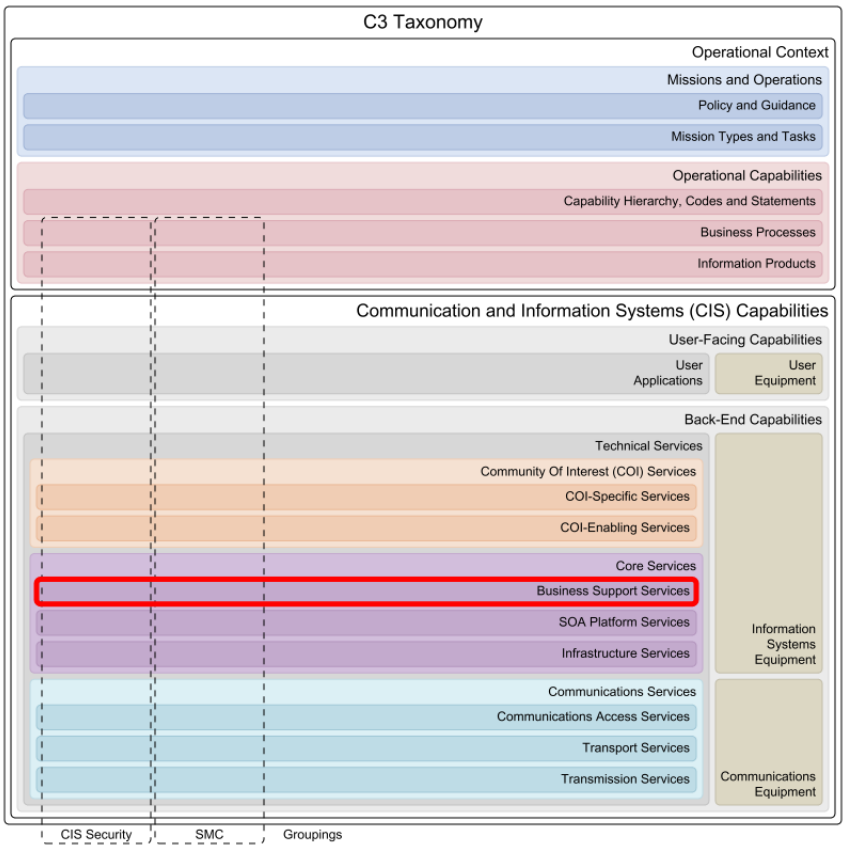
Ground Truth Battlespace Events Services allow for the discovery, exchange, access and modification of Ground Truth Battlespace Events and Incidents which are generated as input to simulations. Ground Truth Battlespace Events Services enable the stimulated development of percieved truth events by Battlespace Events Services.

4 Core Services



The Core Services provide generic, Community of Interest (COI)-independent, technical functionality to implement service-based environments using infrastructure, architectural and enabling building blocks. Core Services provide these building blocks so that these generic, common capabilities do not have to be implemented by individual applications or other services.

4.1 Business Support Services



The Business Support Services provide the means to facilitate other service and data providers on the enterprise network by providing and managing underlying capabilities for collaboration and information management. These services are enablers used by other services and users across the whole network-enabled enterprise, acting as "building blocks" for developing more sophisticated Community Of Interest (COI) services and applications. Therefore, they are COI independent and they must be available to all enterprise members.

4.1.1 Business Support CIS Security Services

The Business Support CIS Security Services provide the necessary means to implement uniform, consistent, interoperable and effective web service security. These services also implement and enforce CIS Security policies at the enterprise support level.

4.1.1.1 Business Support Guard Services

The Business Support Guard Services connect networks of different security policy and usage areas to control traffic flow in-between the networks following a set of predefined rules.

4.1.2 Business Support SMC Services

The Business Support Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the enterprise support level.

4.1.2.1 Application Store Services

The Application Store Services provides a form of application provisioning. It provides the means to download executable content over a network. It also provides the means to search and discover applications, including application data, from an application repository, typically through the use of an application provisioning portal.

4.1.2.2 Configuration Management Database Services

The Configuration Management Database (CMDB) Services provide access to a repository that is designed to store many of the components of an information system. A CMDB contains data describing managed resources like computer systems and application software and/or process artifacts like incident, problem and change records, and the relationships among these entities.

In the context of ITIL (Information Technology Infrastructure Library), a CMDB represents the authorized configuration of the significant components of the IT environment. A key goal of CMDB is to help an organization understand the relationships between different components and track their configuration. The CMDB is a fundamental component of the ITIL framework's Configuration Management process. CMDB implementations may integrate with change management, knowledge management and/or authorization.

4.1.3 Unified Communication and Collaboration Services

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

4.1.3.1 Military Messaging Services

The Military Messaging Services provide a reliable, store and forward message transfer service for both users and applications in support of organizational messaging (messaging between organizations and organizational units). The service supports different qualities of service for different message priorities (e.g. expediting higher priority messages, timing out higher priority messages more quickly) to honour the precedence of the military messages. The Military Message Transfer Service supports a range of elements of service including access management, alternate recipients, conversion prohibition, deferred delivery, delivery notification, distribution list expansion, latest delivery, and message security labelling.

4.1.3.2 Informal Messaging Services

The Informal Messaging Services provide the capability to exchange digital messages (electronic mail or email) from a provider to one or more recipients using a store and forward model. They provide the ability to accept, forward, deliver and store messages. Messages can be relayed from one domain to another.

The Informal Messaging Services support store-and-forward model, supporting email messages consisting of three main components, the message envelope, the message header, and the message body. The message header contains control information, including an originator's email address and one or more recipient addresses as well as the subject header field and a message submission date/time stamp.

4.1.3.3 Fax Services

The Fax Services provide the ability to send and receive bitmaps of electronic material (both text and images) using an analogue signal over a telephone network, normally to a telephone number connected to a printer or other output device. The telephone number of a receiving device is normally required to deliver the fax message across a telephone network. Alternatively, services using FoIP to deliver faxes across IP networks can extend fax delivery to multiple IP and email addressees.

4.1.3.4 Calendaring and Scheduling Services

The Calendaring and Scheduling Services provide functionality for managing calendars, the timing of tasks and task assignments for users. This includes event definitions and actions in the form of notifications or alerts.

4.1.3.5 Video-based Communication Services

The Video-based Communication Services provide a two-way video transmission between different parties on the network, including call set-up, call co-ordination, full motion display of events and participants in a bi-directional manner, support for the management of directing the cameras, ranging from fixed position, to sender directed, to receiver directed, to automated sound pickup.

These services also provide simultaneous videoconferencing among two or more remote points by means of a Multipoint Control Unit (MCU). This is a bridge that interconnects calls from several sources (in a similar way to the audio conference call). All parties call the MCU unit, or the MCU unit can also call the parties which are going to participate, in sequence. There are MCU bridges for IP and ISDN-based videoconferencing. There are MCUs which are pure software, and others which are

a combination of hardware and software. An MCU is characterized according to the number of simultaneous calls it can handle, its ability to conduct transposing of data rates and protocols (translating and transcoding), and features such as Continuous Presence, in which multiple parties can be seen onscreen at once.

4.1.3.6 Audio-based Communication Services

The Audio-based Communication Services provide a two-way audio transmission between different parties on the network, including call set-up and call co-ordination in a bi-directional manner. These services also provide simultaneous audio conferencing among two or more remote points by means of a Multipoint Control Unit (MCU). This is a bridge that interconnects calls from several sources (in a similar way to the video conference call). All parties call the MCU unit, or the MCU unit can also call the parties which are going to participate, in sequence. There are MCU bridges for IP and ISDN-based videoconferencing. There are MCUs which are pure software, and others which are a combination of hardware and software. An MCU is characterized according to the number of simultaneous calls it can handle, its ability to conduct transposing of data rates and protocols (transrating and transcoding), and features such as Continuous Presence, in which multiple parties can be seen onscreen at once.

4.1.3.7 Text-based Collaboration Services

The Text-based Collaboration Services provide the ability to exchange relatively brief text messages, in near real-time, between network addressable entities. Text-based Collaboration Services offers capability to exchange messages supporting the multiple scenarios including One-to-One messaging exchange between any two network addressable entities, Multi-Party messaging exchange between multiple network addressable entities, Notification or alerting messaging exchange between network addressable entities, Structured request and response messaging exchange between network addressable entities and cross-domain sharing information exchanges.

4.1.3.8 Whiteboarding Services

The Whiteboarding Services provide the means to mirrors the experience of collaborating on a whiteboard in a conference room. It allows for the capture of freeform ideas by bringing together a group of people's thoughts, all in one place. Whiteboarding Services provides a virtual whiteboarding capability for shares, images or files and lets multiple participants work and annotate on these images or files concurrently, with real-time updates being shared between all participants.

4.1.3.9 Presence Services

The Presence Services advertise the network availability of other entities hence providing the knowledge of whether those entities are online and available for communication. Presence Services manage a subscription model, in effect a simple publish-subscribe method, whereby entities that have subscribed to another entity's presence receive updated presence information when that entity comes online and goes offline.

4.1.3.10 Document Sharing Services

The Document Sharing Services provide a capability to upload or choose from the library a document and then share it with peers for simultaneous preview and collaborative editing.

4.1.3.11 Application Sharing Services

The Application Sharing Services provide the capability to share an application's user interface over the network infrastructure. All participating actors can view and use the shared application simultaneously.

4.1.4 Information Management Services

The Information Management Services provide the means 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 organization. These services support 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.

4.1.4.1 Content Management Services

The Content Management Services support the management and lifecycle of information (from creation to destruction, structured or unstructured, static or dynamic, transitory or operational record) such as images, audio, video, web content, messaging and email, office documents, PDFs, XML, etc.

4.1.4.2 Workflow Services

The Workflow Services provide technical services to support business activities (manual, semi-automated or automated) and coordination of information, people and services involved. This includes supporting services for the management of business processes, their creation, execution and monitoring.

4.1.4.3 Distributed Search Services

The Distributed Search Services provide the safe and secure search and discovery of information (structured, semi-structured and unstructured, in any format, transitory or operational record) to and from integrated and federated services and data sources, and in compliance with relevant governance.

4.1.4.4 Report Generation Services

The Report Generation Services enable the development, management, generation and dissemination of reports from identified information sources in a format most readily understood by the target reader and possibly based on specified templates.

4.1.4.5 Analytics Services

The Analytics Services provide analytical services to support the decision-making needs of the enterprise, using information produced by gathering, consolidating, cross-referencing and enhancing information from various sources. Different types of analytics can be applied: Descriptive analytics looks at past performance and understands that performance by mining historical data to look for the reasons behind past success or failure. Predictive analytics is an area of data mining that deals with extracting information from data and using it to predict trends and behavior patterns. It is trying to answer the question what will happen.

4.1.4.6 Language Support Services

The Language Support Services provide enterprise linguistic functions for multiple human languages in the form of typographic and grammatical verification and auto-correction, thesaurus and natural language translation capabilities.

4.1.5 ERP Services

The Enterprise Resource Planning (ERP) Services provide the means to cross-functional support for enterprise internal business processes by providing a real-time view of financial resource management, human resource management, supply chain management, customer relationship management, project management and process management activities.

4.1.5.1 Financial Resource Management Services

The Financial Resource Management Services provide support for budgeting, cost management, general ledger, payables, receivables, cash management, financial consolidation and financial auditing processes.

4.1.5.2 Human Resource Management Services

The Human Resource Management Services will provide support for recruiting, in-processing, separation, training, skill-set management, payroll, job description management and organizational structure management processes.

4.1.5.3 Supply Chain Management Services

The Supply Chain Management Services provide the functionality for managing and locating objects or materials including capacity, stock levels, re-order levels, historical demand records and specialised storage capacity (e.g. environmentally controlled).

4.1.5.4 Project Planning Services

The Project Planning Services typically provide the following capabilities across the enterprise or federation: project planning, resource assignment, project accounting, project collaboration and project tracking, integrating information for other Support services and systems like Workforce Management Systems and Accounting Systems.

Web-based Project Management Appplications and tools typically model and enforce best practices that facilitate reliable and consistent project planning, launch and delivery across the enterprise or federation.

4.1.6 Geospatial Services

The Geospatial Services provide the means to 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. Nonetheless, specialized services are also required, based on specific needs such as transformation of geographic coordinates and querying of catalogues.

4.1.6.1 Geospatial Catalog Services

The Geospatial Catalog Services define common interfaces to discover, browse, and query metadata about geospatial data, services, and other potential resources.

4.1.6.2 Geospatial Web Map Services

The Geospatial Web Map Services provide a HTTP interface for requesting geo-registered map images from one or more distributed geospatial databases. A WMS request defines the geographic layer(s) and area of interest to be processed. The response to the request is one or more geo-registered map images. Typical image formats for the map result are PNG, JPEG, GIF or SVG. There are open source WMS Servers such as UMN Mapserver and Mapnik. Commercial alternatives exist from most commercial GIS vendors, such as ESRI ArcIMS, ArcGIS Server, GeoClip, Intergraph Geomedia WebMap, and others.

4.1.6.3 Geospatial Web Feature Services

The Geospatial Web Feature Services provide interfaces for describing data manipulation operations (e.g. Create, Delete, Update, Get or Query) on geospatial features which are primarily based on vector data.

4.1.6.4 Geospatial Web Coverage Services

The Geospatial Web Coverage Services support requests for geographical coverages across the web using platform-independent calls. The coverages are objects (or images) in a geographical area, whereas the WMS interface or online mapping portals like Google Maps return only an image, which end-users cannot edit or spatially analyze.

4.1.6.5 Geospatial Web Map Tile Services

The Geospatial Web Map Tile Services provide access to cartographic maps using predefined image tiles. Geospatial Web Map Tile Services provide a complementary approach to the Geospatial Web Map Services for tiling maps.

Geospatial Web Map Services focus on rendering custom maps and is an ideal solution for dynamic data or custom styled maps. Geospatial Web Map Tile Services trade the flexibility of custom map rendering for the scalability possible by serving of static data (base maps) where the bounding box and scales have been constrained to discrete tiles which enables the use of standard network mechanisms for scalability such as distributed cache systems to cache images between the client and the server, reducing latency and bandwidth use.

The service advertises the tiles it has available through a standardized declaration in the ServiceMetadata document common to all geospatial web services. This declaration defines the tiles available in each layer (i.e. each type of content), in each graphical representation style, in each format, in each coordinate reference system, at each scale, and over each geographic fragment of the total covered area. The ServiceMetadata document also declares the communication protocols and encodings through which clients can interact with the server. Clients can interpret the Service Metadata document to request specific tiles.

4.1.6.6 Geospatial Network Analysis Services

The Geospatial Network Analysis Services perform network analysis operations such as routing (shortest path, fastest path), closest facility location, or area analysis.

4.1.6.7 Geospatial Coordinate Services

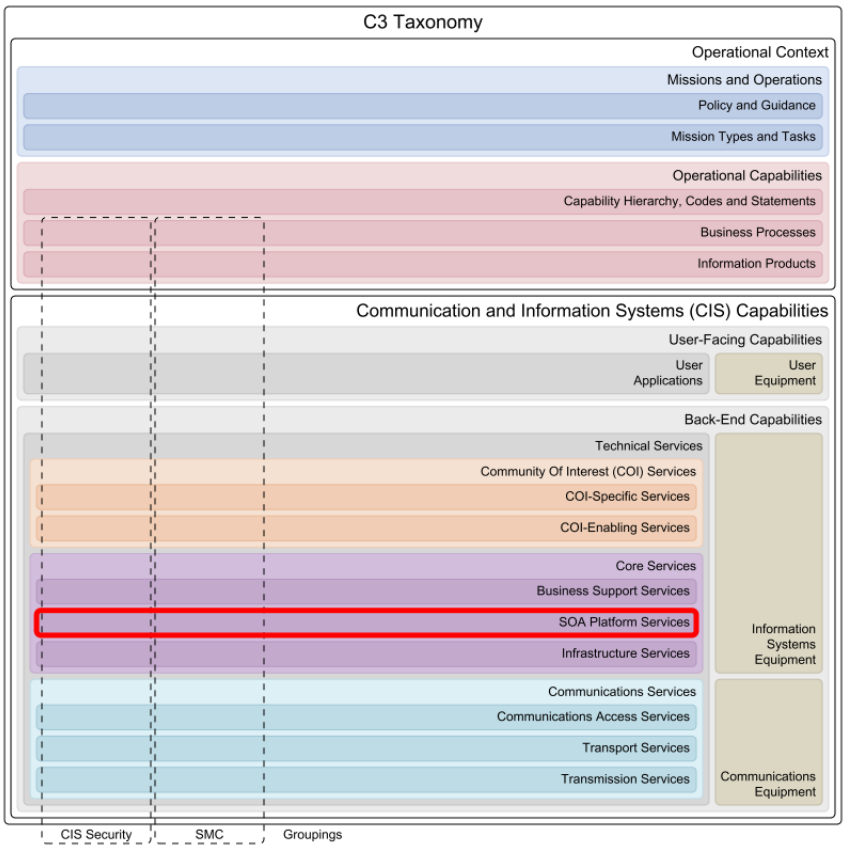
The Geospatial Coordinate Services translate geospatial coordinates between spatial reference systems. A spatial reference system (SRS) is a coordinate-based local, regional or global system used to locate geographical entities. A spatial reference system defines a specific map projection, as well as transformations between different spatial reference systems.

4.1.6.8 Geospatial Terrain Analysis Services

The Geospatial Terrain Analysis Services support planning and predictive decision tools by providing information and knowledge products that capture integrated terrain and weather effects.

Terrain and weather effects represent a fundamental, enabling piece of battlefield information supporting situation awareness and the decision-making processes within Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR). These effects can both enhance or constrain force tactics and behaviors, platform performance (ground and air), system performance (e.g. sensors) and the soldier.

4.2 SOA Platform Services



The 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.

4.2.1 SOA Platform CIS Security Services

The Service Oriented Architecture (SOA) Platform CIS Security Services provide a foundation to implement uniform, consistent, interoperable and effective web service security. They also provide the necessary means to implement and enforce CIS Security policies at the SOA platform level.

4.2.1.1 SOA Platform Guard Services

The SOA Platform Guard Services connect networks of different security policy and usage areas to control traffic flow in-between the networks following a set of predefined rules for SOA services. The intended function is to allow automated data exchange between two network enclaves that belong to different security domains. From the guard's perspective one enclave is defined as high security domain and the other enclave as the low security domain.

In cross-domain information exchange scenario the following threats to the high security domain are recognized: leakage of confidential information from the high security domain to the low security domain and degradation of the integrity or availability of resources in the high security domain

The purpose of the SOA Platform Services is to enable a cross-domain information exchange by mediating traffic flows, while offering sufficient protection against the threats mentioned above by enforcing an appropriate access control policy.

4.2.1.2 Security Token Services

The Security Token Services (STS) provide functionality of identity providers responsible for issuing Security Tokens, which may or may not be structured as XML. The Security Tokens are issued after entity authentication to the STS, and are used to pass entity identity information to other services (Relying Parties) which trust the STS and its tokens.

4.2.1.3 Policy Enforcement Point Services

The Policy Enforcement Point (PEP) Services protect other services by providing a logical entry point that serves as an intermediary between a call from a service consumer to a service provider. The PEP can either be deployed as a separate device or appliance that sits between the consumer and provider, or as an inline component that is deployed as part of the container infrastructure of the service. The PEP validates the structure of the message, including the digital signature, and the credentials that are provided with the message. This provides a common mechanism to extract and pass on identity information from the service consumer to the service provider so that an Authorisation decision can be made, either locally or through the use of a Policy Decision Point (PDP).

4.2.1.4 Policy Decision Point Services

The Policy Decision Point (PDP) Services provide authorization decisions by evaluating digital policies against the attributes of an authorization request. The request can contain attributes about the subject of the request (the service consumer), the object of the request (the resource that is being accessed), the action that is being performed and other attributes not related to the subject or resource (the "environment"). A decision is returned to the requesting entity, which can contain further obligations about how the request is to be treated. The PDP can be collocated with a Policy Enforcement Point (PEP) to improve performance.

4.2.1.5 Policy Administration Point Services

The Policy Administration Point (PAP) Services provide functionality required to compose, modify, manage, and control access control policies in a standard policy exchange format, enabling the policy enforcement through the Policy Enforcement (PEP) and Policy Decision Point (PDP) components.

4.2.1.6 Information Labeling Services

The Information Labeling Services provide functionality required to apply metadata to an information object for the purpose of creating a label or mapping labels of "foreign" security policy.

Labeling facilitates the determination of the protection requirement for an information object, the release of an information object, or the determination of the mission value of an information object, as captured by release and protection policies defined for each metadata entry.

4.2.2 SOA Platform SMC Services

The 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.

4.2.2.1 SOA SMC Policy Enforcement Services

The Service Oriented Architecture (SOA) Service Management and Control (SMC) Policy Enforcement Services enforce technical and business policies related to performance, quality of service, agreed service levels, and ensures compliance with business and legal rules. SOA SMC Policy Enforcement Services act as effectors that enforce policies at run-time.

SOA SMC Policy Enforcement Services enforce policies on services hosted within the SOA Platform. Depending on implementation, the SOA SMC Policy Enforcement Services can be standalone components in front of protected services (e.g. functioning like reverse proxy); or they can be part of the Web Hosting Platform (e.g. a pipeline in an application server).

4.2.2.2 Service Discovery Services

The Service Discovery Services enable a requester to discover a target service that matches certain functional and non-functional requirements. In this context discovery is the act of locating a service description of target service(s) which contain information about the (syntactic and semantic) interface of the service and other (non-functional) aspects of its service contract. The resulting service description is sufficient to inform a consumer on the mechanism required to bind to an instance of the target service.

4.2.2.3 SOA Platform Logging Services

The SOA Platform Logging Services provide facilities for capturing, filtering and writing information about calls between services hosted in the SOA Platform. The logs can be used for auditing purposes, for troubleshooting, performance optimizations, etc.

4.2.2.4 SOA Platform Monitoring Services

The SOA Platform Monitoring Services provide information on the actual utilization and performance of monitored SOA Platform Services. The SOA Platform Monitoring Services monitor service communication based on service calls and message exchange to identify performance issues and determine current availability.

The SOA Platform Monitoring Services provide information about service failures and exceptions and support root-causes analysis to help locate performance bottlenecks, errors, or incomplete transactions. They ensure that any failures are detected proactively, isolated, analyzed, and resolved with as little impact on the end user as possible.

4.2.2.5 SOA Platform Metering Services

The SOA Platform Metering Services measures measures levels of SOA platform resource utilization such as number of web service/application requests, CPU cycles/time used to process requests to specific web service/application, number of transactions, number of message queue requests, incoming and outgoing network bandwidth (total size of incoming and outgoing messages), data storage volume used by application/service over various periods of time (e.g. second, hour, week, month, year).

Calculated average values of the measures can be then used to enforce service SLAs (e.g. to throttle service requests when the total number of requests in specific period of time exceeds limit defined in SLA), load balancing (e.g. to add new application server instances when the average time to process requests exceeds values specified in SLA), for billing purposes (e.g. to provide monthly report with total resource utilization converted to agreed currency) and overall usage trend forecasting.

4.2.3 Message-Oriented Middleware Services

The 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 different models of message exchange (direct, brokered, queues), exchange patterns (request/response, publish/subscribe, solicit response (polling for response), and for fire and forget), topologies (one-to-one, one-to-many) and modes of delivery (synchronous, asynchronous, long running). They also provide the support for routing, addressing, and caching.

4.2.3.1 Direct Messaging Services

The Direct Messaging Services are any services that can communicate by exchanging messages in a direct communication with another services. The exchange of messages can be implemented using any Message Exchange Pattern (e.g. request/response, publish/subscribe, fire and forget, solicit response). The Direct Messaging Services can be implemented to use synchronous (i.e. blocking) and asynchronous (i.e. non-blocking) communication modes. For example in a Publish-Subscribe scenario a notification producer would be one Direct Messaging Service sending one-way messages to a notification consumer that would be another Direct Messaging Service receiving the message.

4.2.3.2 Message Brokering Services

The Message Brokering Services act as an intermediary between Message Publishers and Message Consumers in order to permit the Message Consumer to subscribe to Messages produced by Publishers.

Within this Message Publish-Subscribe pattern, senders of messages (called Publishers) do not send messages directly to specific receivers (called Subscribers), but instead send them to Message Brokering Services for further distribution to registered Subscribers.

4.2.3.3 Message Routing Services

The Message Routing Services are services that can dynamically route messages at run time based on different criteria, e.g. message content or metadata or for load-balancing purposes. The routing logic shall be configurable. The Message Routing Services can be also used to provide one-to-many message delivery by multiplying a message and sending it to many recipients, e.g. this can be used to implement multicast messages.

4.2.3.4 Message Proxying Services

The Message Proxying Services are services that act as an intermediary for other services, hiding their actual location and implementation from the service consumers. The proxy services can communicate on a behalf of the underlying service. They offer a capability to expose a virtual endpoint of the underlying service. They supports the loose coupling and service abstraction principles of the SOA design.

The Message Proxying Services tend to sit at the boundaries of organisations, either internal boundaries (between sites, before WAN links) or external boundaries (such as the Internet). They provide a number of benefits over the use of directly communicating through a router:

- Security - A number of security features may be applied in the proxy server, such as content checking, authentication and authorisation, auditing and anonymity (as the identity of the client machine can be hidden).
- Performance - Message Proxy Services can communicate with Message Caching Services to avoid having to make calls across sub-optimal WAN links, and can use other techniques (such as compression) to improve performance.
- Simplicity - Message Proxy Services can simplify the configuration of Firewall rule sets, as only communication through the proxy is allowed outside the organisation.

4.2.3.5 Message Queueing Services

The Message Queueing Services provide message queues as intermediary buffers, allowing services and consumers to process messages independently by remaining temporally decoupled. Thus they supports asynchronous communication.

4.2.3.6 Message Caching Services

The Message Caching Services provide functionality to conditionally store messages sent between producers and consumers. The messages can be later served to consumers if they need to resynchronize their state or were unavailable and lost some messages. The cache can support synchronous (request/response) and asynchronous (fire and forget, publish/subscribe) communication.

4.2.4 Web Platform Services

The 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.

4.2.4.1 Web Hosting Services

The Web Hosting Services provide an environment for operating web applications and services. The hosting services make available a service container that manages the service life cycle and underlying resources (such as memory, storage and CPU) to deliver the required service. The application or web service execution takes place within the container's run time environment.

4.2.4.2 Web Presentation Services

The Web Presentation Services allow combining rich content from different data sources into a single client web page or desktop, using a combination of Web 2.0 technologies such as HTML snippets, scripting code (JavaScript), on demand code (AJAX, JSON), web service calls and proprietary code (Flash, ActiveX and so on).

4.2.4.3 Web Caching Services

The Web Caching Services accelerate service requests by retrieving content saved from a previous request, allowing organizations to significantly reduce their upstream bandwidth usage and costs, while simultaneously increasing performance. This means that the requested resource does not need to be downloaded from a remote server, possibly over a connection with limited bandwidth, but can be retrieved from a store located on the local LAN. Web Caching Services do this by keeping local copies of requested resources and serving those to the client rather than fetching them from the original server. If the resource is not already present in the cache, then it is retrieved from the requested URL, and a copy is written to the local store. Web Caching Services are often used by Web Proxy Services, and are indeed often collocated with them. However, they are separate, and an entire caching infrastructure can be built independent of proxy services.

4.2.4.4 Web Proxying Services

The Web Proxying Services handle HTTP message exchanges on behalf of other entities. From the perspective of the partner in the message exchange, it is communicating with the proxy, and is not necessarily aware that this is the case.

There are three main types of Web Proxying Services:

- Forward Proxy - in this case, the user's client (which may be an Internet Browser or Web Services client) is configured to use the specific proxy in order to make requests on its behalf. The remote service provider sees the request as coming from the proxy, and not from the original client.
- Reverse Proxy - in this case, the proxy is handling requests from clients as if it were the server. The request is sent to the proxy, which may return a response, or may forward the request to the actual server for further processing.

- Transparent Proxy - a transparent proxy acts in much the same way as a forward proxy, but the client requires no configuration to use it. As far as the client is concerned, it is communicating directly with the server, as the communications are intercepted at the network layer rather than the application layer.

Web Proxying Services tend to sit at the boundaries of organisations, either internal boundaries (between sites, before WAN links) or external boundaries (such as the Internet).

4.2.5 Information Platform Services

The 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.

4.2.5.1 Information Discovery Services

The Information Discovery Services provide the functionality to automate the discovery and retrieval of Information Products and their structure.

Information Products, in this regard, are aggregates of structured data. Discovered data is the result of a search upon an entire dataset, a search upon a subset of a dataset, or a search based on dataset and/or content metadata.

4.2.5.2 Information Access Services

The Information Access Services transform information stores or sources into web enabled services.

Information Access Services provide a generic capability that can be configured as required to expose new information stores or sources in the required service protocols and formats. The intent is to minimize custom services and allow agile provisioning of new capabilities based on evolving operational requirements.

By focusing on providing access to information from existing stores and sources, rather than on providing applications which use that information, Information Access Services de-couple the access to information from the use of the information. Since applications can use information in any number of ways to support any number of use cases, de-coupling the access to information from its use reduces the complexity and the combinations of interfaces which must be supported.

4.2.5.3 Information Aggregation Services

The Information Aggregation Services enable easy integration of data into business processes, mash-ups, gadgets, business intelligence applications and any service in general.

4.2.5.4 Metadata Repository Services

The Metadata Repository Services provide the functionality for storing, querying, and retrieving authoritative metadata within the enterprise. Metadata Repository Services provide administrative as well as programmatic interfaces for metadata registries and repositories. The registries and repositories can be federated across the enterprise, thus Metadata Repository Services support federation for storing, querying and retrieving metadata (i.e. for single central registries/repositories as well as multiple registries/repositories throughout the network).

Metadata Repository Services will store a wide range of standards and specifications that describe the structure, format and definitions of data, as well as the relationships among data elements. These standards and specifications are stored in machine readable formats that can be interpreted automatically within the service-oriented environment (e.g. XML schemas, ontologies). It gives developers and architects visibility into methods to compose and encode data and to share usage across the organization. Registration of such metadata is especially critical to achieve the data goals of interoperability and coherence by promoting semantic and structural understanding.

The Metadata Repository Services will also have the capability to maintain references to aforementioned standards and specifications, i.e. for artifacts that are managed by other registries/repositories in a federation. Metadata Repository Services provide controlled access to artifacts, the lifecycle management of the artifacts and support for proper versioning and configuration management of artifacts.

Each object maintained by a Metadata Repository Service has to be uniquely identifiable and will be organized into fully searchable taxonomy. In addition and supported by Information Assurance (IA) services, Metadata Repository Services will ensure the data integrity of the artifacts stored in the repository.

4.2.5.5 Information Annotation Services

The Information Annotation Services provide functionality for annotating or enhancing information objects with additional information such as: metadata, tags, comments, attachments, relationship with other information objects and/or content.

An annotation is a collection of assertions about one or more information objects and so must be able to uniquely reference those objects. Further, annotations are made by an entity, user, system etc. and so information such as who created the annotation, when it was created, the confidence, reliability and authenticity of the assertions must also be recorded.

The Information Annotation Services allow for persisting, searching and retrieving these annotations. Since the annotations are additional information that makes reference to existing information, an Information Annotation Service can be logically decoupled from the service providing that existing information.

The Information Discovery Services complement the Information Annotation Services by allowing information consumers to query not only the original information objects but also any annotations which relate to them.

4.2.5.6 Business Rules Services

The Business Rules Services provide capability to support the creation, testing, management, deployment and maintenance of Business Rules in an operational environment.

A Business Rules are statements describing a business/enterprise policy or procedure (e.g. discount calculation) and can be represented using formal language.

4.2.6 Composition Services

The Composition Services will access and fuse data and behavior on demand, and return a single result to the consumer. The 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.

4.2.6.1 Orchestration Services

The Orchestration Services are responsible for coordinating the execution of multiple technical services in such a way that the coordinated whole of technical services appears as a single, aggregate technical service responding to a single individual request. Such an aggregated service could be said to implement a business process that is characterized by the fact that it runs within own organization boundaries, with the own organization having full control over the execution of the process.

Orchestration describes one particular component activity of the composition that oversees and directs the other component activities. An orchestration has one and only one direction activity. In a service-oriented software solution, the component services of an orchestration are software services performed by software programs.

A service composition described by an orchestration is again a service itself and can be re-used in further compositions.

An orchestration coordinates the other sub-services in a step-wise manner, i.e. it specifies the partial order of all the steps that each of the sub-services has to do in order to produce the desired outputs in a co-operative, joined way.

An orchestration can be (and usually is) stateful as the coordination of sub-services immediately requires to keep track of states. The other sub-services which are controlled by the orchestration do usually not interact with each other directly and do not have to be stateful.

4.2.6.2 Choreography Services

The Choreography Services support modelling of compositions of multiple technical services into so called choreographies and can support specification of interfaces and protocols implemented by services participating in a choreography.

Choreography is a set of autonomous activities that have a defined pattern of behaviour with respect to each other. There is no single activity that directs the other activities in choreography. Choreography distributes the control and relies on the

ability of its component activities to understand and respond to events. Choreography treats services as peers that interact based on an agreement, rather than imposing a single-point-of-entry brokering pattern on top of them. In a choreography scenario composition is understood as the collaborative exchange that takes place based on the description of messages exchange and the interaction of a set of services seen from a global perspective.

Choreographies are not executable in a sense that there is no central controller service that could be executed.

Choreography mechanisms are used to specify the coordination agreement and behaviour of each service in choreography, including the external interfaces exposed by the services involved and the protocol implemented by each of the services involved, including order of messages being exchanged and specification of services that these messages will be exchanged with. These interfaces of services involved and message exchange protocol followed can be used to generate stubs for the actual service implementation (e.g. to be used and exposed by orchestration). However, choreography does not include the internal details of services involved.

4.2.6.3 Transaction Services

The Transaction Services allow multiple individual operations to be linked together as a single, indivisible action. All operations in a transaction are either completed without error or none of them are; if some of the operations are completed but errors occur when the others are attempted, the transaction-processing system "rolls back" all of the operations of the transaction (including the successful ones) thereby erasing all traces of the transaction and restoring the system to the consistent, known state that it was in before processing of the transaction began. In scenarios when usual transactional properties (like atomicity, consistency, isolation, and durability) are too strong or unimplementable (e.g. in complex business processes), some limited transactional properties must be satisfied to guarantee a process is not left in an inconsistent state. For example compensating activities can bring the process to a consistent state, albeit not necessarily identical as the state before the process started.

4.2.7 Mediation Services

The 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.

4.2.7.1 Protocol Transformation Services

The Protocol Transformation Services mediate between communication parties by adjusting the way in which data is exchanged between both parties. Protocol Transformation Services enable the use of different protocols for handling information between information providers and consumers over a possibly heterogeneous network. Protocol Transformation Services are important when different types of communication patterns are being used (e.g. static, deployable or mobile) that would require special protocols to ensure that the information is being transferred in the most efficient possible way.

Protocol transformation services mediate between various transport protocols, which for example in a web services setting usually comprise single protocols like HTTP, HTTPS, TLS, SMTP and FTP, but also entire message-oriented middle-ware solutions like IBM's WebSphere MQ or JMS. We speak of protocol virtualization if a protocol mediation services actually offers to consume a service over a range of different transport protocols.

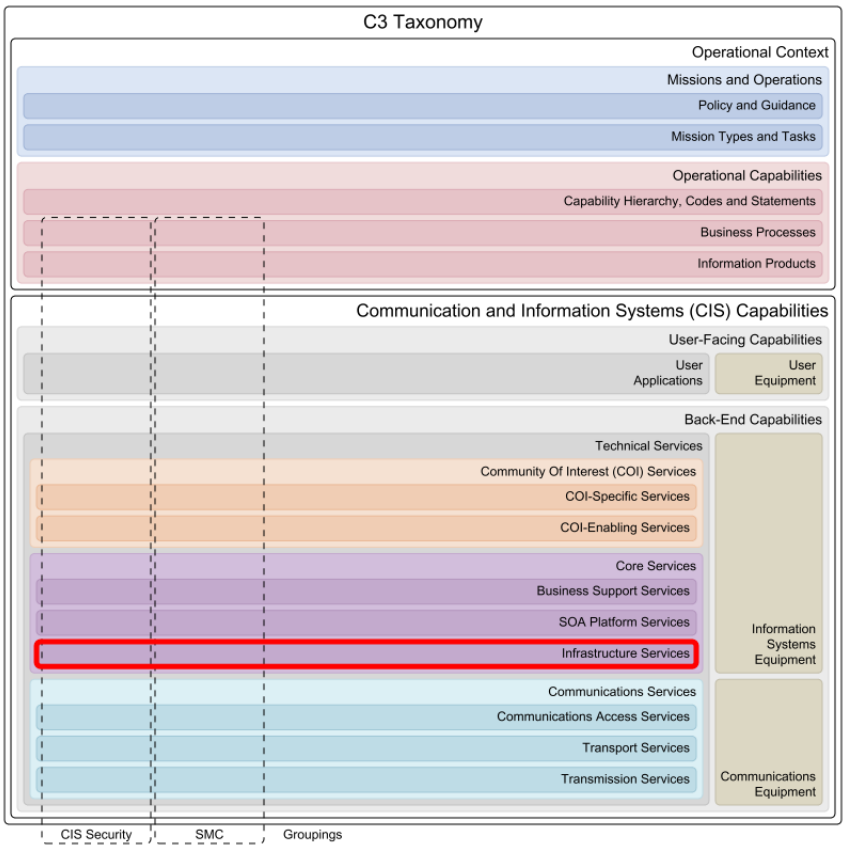
4.2.7.2 Data Format Transformation Services

The Data Format Transformation Services support the encoding of information in different formats. This is needed when information consumers cannot directly process the information in the format chosen by the information provider. Data Format Transformation Services also play a role when the boundary between one network type to another is crossed (e.g. static IP network to tactical radio network) and a conversion from one data representation to another (e.g. for bandwidth utilization purposes) is required.

The relation between the data and the information which it represents can be changed during a data format transformation. To this regard important aspects of data transformation include format conversion where data is encoded differently using another format. Both data encodings represent the same information and are usually compatible. Typical examples are the conversion of temperature from Celsius to Fahrenheit, or the conversion of the bit representation between Big- and Little-Endian formats.

Not all information can always be preserved during the data transformation (lossy). Reasons can be that some information is deliberately omitted and not captured in the new data (e.g. when compressing data), or that the target format is not capable of representing data in a way that the original information is completely preserved.

4.3 Infrastructure Services



The Infrastructure Services provide the foundation to host infrastructure services in a distributed and/or federated environment in support of NATO operations and exercises. They include computing, storage and high-level networking services that can be used as the basis 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 industry today as part of their Cloud Computing developments.

4.3.1 Infrastructure CIS Security Services

The Infrastructure CIS Security Services provide the necessary means to implement and enforce CIS Security policies at the infrastructure level.

4.3.1.1 Digital Identity Services

The Digital Identity Services comprise the services required to capture and validate information to uniquely identify an individual, determine suitability, and create and manage a digital identity over the life cycle. Digital identity is the representation of identity in a digital environment.

4.3.1.2 Credentialing Services

The Credentialing Services support binding an identity to a physical or electronic credential, which can subsequently be used as a proxy for the identity or proof of having particular attributes.

Different types of credentials may be issued (e.g. smart card, badges, identification documents, software certificates or passwords), depending on the acceptable assurance level for the mission.

4.3.1.3 Authentication Services

The Authentication Services provide functionality to verify that a claimed identity is genuine and based on valid credentials. Authentication typically leads to a mutually shared level of assurance by the relying parties in the identity. Authentication may occur through a variety of mechanisms including challenge/response, time-based code sequences, biometric comparison, PKI or other techniques.

The Authentication Services provide also functionality required to manage trust relationships between organizations and/or within an organization to enable access to electronic assets across boundaries of entity's governance realms and/or security domains.

4.3.1.4 Privilege Management Services

The Privilege Management Services provide functionality to establish and maintain the entitlement or privilege attributes that comprise an individual's access profile.

These attributes are features of an individual that can be used as the basis for determining access decisions to both physical and logical resources. The Privilege Management Services govern the management of the data that constitutes the user's privileges and other attributes, including the storage, organization and access to information.

4.3.1.5 Authorization and Access Services

The Authorization and Access Services provide functionality to grant or deny access to information processing services, data and physical facilities. They enforce security policy by ensuring individuals only access those resources they are entitled to use and then only for approved purposes.

The request for access includes the resource and the type of desired access, e.g. reading, writing, opening. The authorization decision is based on the access control rule sets, resulting from privilege management, taking into account the level of assurance of entity's identity determined by the utilized authentication mechanism.

4.3.1.6 Digital Certificate Services

The Digital Certificate Services provide functionality required to create, manage, distribute, use, store, suspend, resume and revoke digital certificates. It provides a trust framework across organizational, operational, physical, and network boundaries, required to enable the services that rely on digital certificates.

4.3.1.7 Intrusion Detection Services

The Intrusion Detection Services provides information on malicious activity and/or security policy violations. The Intrusion Detection Services are primarily focused on identifying possible incidents, logging information about them and reporting.

The Intrusion Detection Services can be used to identify problems with security policy, document existing threats, and deter individuals from violating security policies.

4.3.1.8 Malware Detection Services

The Malware Detection Services are used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worms, trojan horses, spyware, social engineering exploits and ad-ware.

4.3.1.9 Infrastructure Guard Services

The Infrastructure Guard Services connect networks of different security policy and usage areas while controlling data flow between the networks using a set of predefined rules.

4.3.1.10 Infrastructure Cryptography Services

The Infrastructure Cryptography Services supports the use of ciphers including encryption and decryption processes to ensure confidentiality and integrity of data.

Typically, asymmetric cryptography is used for authenticated key exchange, symmetric encryption for data confidentiality, and cryprographic hash functions and digital signatures for data integrity.

4.3.2 Infrastructure SMC Services

The Infrastructure Service Management and Control (SMC) Services provide the means to implement and enforce SMC policies at the Infrastructure level. The services coordinate and communicate with other technical services (Communications Services, SOA Platform Services, etc.) to fulfill the requirements of service delivery. The requirements are translated into Infrastructure specific parameters and distributed to other Infrastructure Services.

4.3.2.1 Infrastructure Provisioning Services

The Infrastructure Provisioning Services manage the instantiation, runtime management and disposal of dynamically scalable and virtualized infrastructure resources. The Infrastructure Provisioning Services sustains the infrastructure footprint for all consumers and locations continuously.

4.3.2.2 Infrastructure Logging Services

The Infrastructure Logging Services capture significant events and/or errors in a distributed often virtualized environment for the purpose of regulatory compliance, auditing or trouble shooting.

4.3.2.3 Infrastructure Monitoring Services

The Infrastructure Monitoring Services provide the ability to monitor the health and performance of Infrastructure Services and services upon which they are dependent. In case of an exception or fault, an alarm will be raised to notify the appropriate actors.

4.3.2.4 Infrastructure Metering Services

The Infrastructure Metering Services measures the utilization of Infrastructure resources over specific period of times.

Metering measures levels of resource utilization such as number of VMs created and used, CPU cycles/time, allocated amount of RAM, incoming and outgoing network bandwidth, data storage volume, etc. over various periods of time (e.g. second, hour, week, month, year).

Calculated average values of the measurements can be then used to enforce Service Level Agreements (SLAs), load balancing, for billing purposes and overall usage trend forecasting.

4.3.3 Infrastructure Processing Services

The Infrastructure Processing Services provide shared access to physical and/or virtual computing resources. 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.

4.3.3.1 Operating System Services

The Operating System (OS) Services provide users with the functionality to manage platform resources, including the processor, memory, files, input and output. The Operating System (OS) Services typically encompasses kernel operations, command interpreter, batch processing, file and directory synchronization services.

4.3.3.2 Virtualized Processing Services

The Virtualized Processing Services hide the physical characteristics of a processing platform and instead present abstracted processing platform to the consumer.

Virtualization enables the provisioning of simplified, fit-for-purpose, tailor-made and on-demand IT-infrastructure resources, sparing the user from having to understand and manage complex details of IT-infrastructure resources. This service supports the centralization of management and maintenance while more flexibly and efficiently allocating IT-infrastructure resources.

4.3.4 Infrastructure Storage Services

The 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.

4.3.4.1 Block-Level Storage Services

The Block-Level Storage Services provide access to physical and/or virtual storage devices that manage their available space as a sequence of fixed size data blocks. Consumers of Block-Level Storage Services are responsible for giving meaning to each of the blocks and often file systems or relational databases are used to abstract block-level storage.

4.3.4.2 Non-relational Structured Storage Services

The Non-relational Structured Storage Services provide a database system where the intention is to handle large sets of data and handle requests/inserts from many users at the same time. They store data schema-free and use eventual consistency (and not ACID).

4.3.4.3 Directory Storage Services

The Directory Storage Services serve as a broker between Directory Service users that provide authoritative information (publishers) and Directory Service users that consume that information (subscribers). Publishers can store their authoritative information in a Directory Service-specific directory/data repository which the Directory Storage Services will use to satisfy queries from subscribers. The information can either be retrieved by the Directory Storage Services service meta-tools and stored in the Directory Service-specific directory/data repository or stored directly into the Directory Storage Services

service-specific directory/data repository by the publisher.

Subscribers will be able to access the Directory Storage Services information over a variety of different interfaces including file-based, remote procedure call (RPC) and service oriented architecture (SOA) interfaces. As well as directly accessing the information according to the schema, the Directory Storage Services will be able to map the information to alternative schemas that are already in use by existing directories/data repositories.

4.3.4.4 File System Storage Services

The File System Storage Services provide controlled hierarchical access to named storage containers. File System Storage Services provide logical access to data since they abstract away physical storage topologies. File System Storage Services also transparently handle fragmentation, caching and storage integrity.

4.3.4.5 Blob Storage Services

The Blob Storage Services provide access to large named objects either for streaming or random access. Blob Storage Services provide next generation storage solutions that scale well horizontally and vertically in a highly mobile/distributed environment.

4.3.4.6 Relational Database Storage Services

The Relational Database Storage Services provide controlled access to a collection of data items organized as a set of formally-described tables from which data can be accessed or reassembled in many different ways without having to reorganize the database tables.

Relational Database Storage Services can be accessed through the Structured Query Language (SQL). SQL statements are used for schema manipulation, data manipulation and information retrieval.

4.3.5 Infrastructure Networking Services

The 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.

4.3.5.1 Host Configuration Services

The Host Configuration Services provide the configuration parameters required by a host to complete a subscription to a network. The required parameters are determined by the network being subscribed to, but may include the host address, sub-net mask, name server and others.

4.3.5.2 Network Load Balancing Services

The Network Load Balancing Services distribute workload across the network, to multiple processing resources, network links, central processing units, disk drives, or other resources, to achieve optimal resource utilization, maximize throughput, minimize response time, and avoid overload. Using multiple components with load balancing, instead of a single component, may increase reliability through redundancy.

4.3.5.3 Printing and Scanning Services

The Printing and Scanning Services enable monitoring, consolidating, controlling, and optimisation of the printing and scanning environment.

4.3.5.4 Data Transfer Services

The Data Transfer Services provide data communication functionality to other services and applications making use of the IP communication layers made available by LAN infrastructure and/or Communications Services. The data transfer functions have many dimensions for various data transfer scenarios, the major emphasis being on the following:

- Synchronous - Asynchronous
- Connection Oriented - Connectionless
- Point to Point - Point to Multipoint
- Real Time - Non Real Time
- Guaranteed - Not Guaranteed

4.3.5.5 Domain Name Services

The Domain Name Services provide access to a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. Domain Name Services associate various information with domain names assigned to each of the participating entities. Most importantly, Domain Name Services translate domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

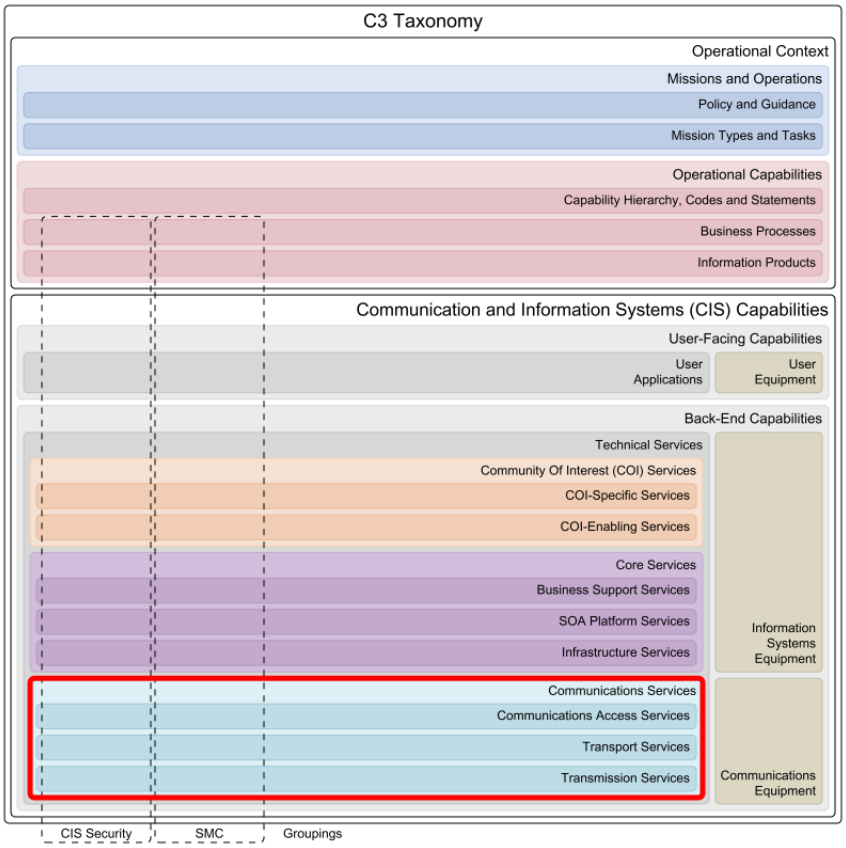
4.3.5.6 Distributed Time Services

The Distributed Time Services provide synchronized time co-ordination as required among distributed processes when executed on different infrastructure segments and across timezones.

4.3.5.7 Remote Access Services

The Remote Access Services enable authorized individuals to remotely access the user interface of a computing resource for the purpose of installation, configuration, monitoring, metering, auditing or process management.

5 Communications Services



The 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.

The taxonomy of Communications Services takes a generic approach, listing elementary (vice complex) communications services, as building blocks of complex, end-to-end communications services. The granularity of the services described in this taxonomy is such that even the lowest level communications service, e.g. a user typing short free-text messages on a keypad and transmitting them over a UHF satcom DAMA radio, can be represented.

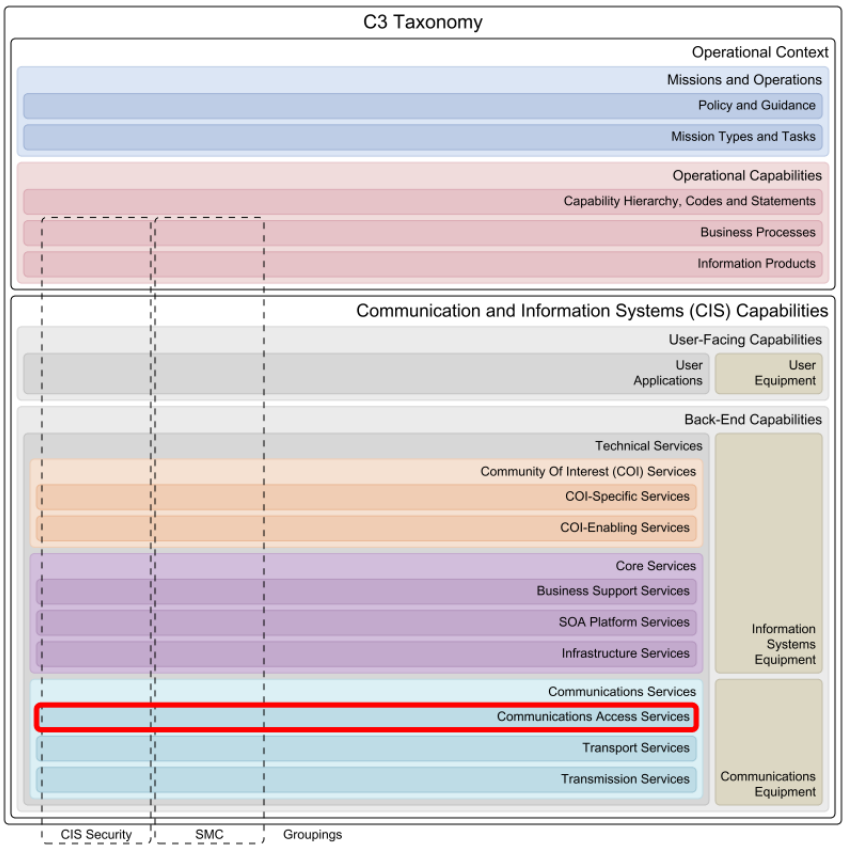
The required granularity is achieved by defining elementary service blocks. These are building blocks in complex end-to-end services, as those formulated in the NSOVs of the relevant reference architectures and derived target architectures. Elementary service blocks are agnostic to the resources and solutions that service providers can adopt to implement them and can be implemented over different communications segments (terrestrial, radio, satcom), by different service providers.

By concatenating these elementary services as building blocks, service architects can streamline and specify any complex communications service, end-to-end (e.g. DCIS service). In particular:

- Service blocks are concatenated to follow the flow of information, in a way similar to the actual communications infrastructure that is physically supporting the services. That makes the resulting Comms Service Maps understandable by network architects, service managers, and service providers. Comms Service Maps can be exported and used for a variety of purposes, from service level specification, to service management and control.
- Comms maps are two-dimensional representations of a complex communications service. Each service block along the chain can be assigned to different service providers, and clear interface and service delivery or service peering boundaries can be defined between them.
- Service providers can select and involve the resources and the technical solutions that best meet the service level specifications for each block, under the constraints posed by the operational context, and by the connectivity/interaction with adjacent service blocks (implemented by other service providers). These constraints shall be reflected in the service level specification.
- In the NATO context, service providers can be NATO organic providersproviders (e.g. NCI Agency, e.g. providing Access Services), a NATO Nation or a consortium/group of nations (e.g. providing Transport Services and Transmission Services

over military-controlled communications infrastructure), as well as commercial providers (e.g. providing Transmission Services over commercial infrastructure).

5.1 Communications Access Services



The 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. Because they are defined end-to-end, in a comms service map, the same Access Service block can be found at both ends of the link, and will often (but not necessarily) be implemented and managed by the same service provider.

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. In most cases, they involve the direct connection of hosts or end-user devices that interface the service on a given layer of the communications stack.

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

5.1.1 Communications Access CIS Security Services

The Communications Access CIS Security Services provide a foundation to implement and enforce CIS Security policies at the communications access level.

5.1.1.1 Communications Security Services

The Communications Security (COMSEC) Services prevent unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering the content to the intended recipients. COMSEC methods include cryptosecurity, transmission security, emission security, traffic-flow security and physical security of COMSEC equipment.

COMSEC is used to protect both classified and unclassified traffic on military communications networks, including voice, video, and data. It is used for both analog and digital applications, and both wired and wireless links.

5.1.1.2 Network Access Control Services

The Network Access Control Services manage the ability of a device to connect to a network based on endpoint security compliance (such as OS patch level, antivirus updates, host IP addresses, etc.) user and system authentication and network security enforcement.

The Network Access Control Services will protect a network by preventing non-compliant devices from accessing the network at the IP-level.

In case of non-compliance a remote user will be redirected to a network quarantine segment where the client can be updated to the level of required compliance.

5.1.1.3 Network Firewall Services

The Network Firewall Services control input, output, and/or access from, to, or by an application or service. They operate by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policies.

5.1.2 Communications Access SMC Services

The Communications Access Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the communications level.

The Communications Access SMC Services are based on the TM Forum Business Process Framework (eTOM) process area Operations and specifically Resource Management & Operations.

Within the context of SMC for all Communications Services, the functions and subsequent requirements on each the three layers - Communications Access Services, Transport Services and Transmission Services - experience a great overlap and high level of similarity. Therefore all SMC Services for these layers are defined under Communications Access SMC Services, while they are valid for the other two layers just the same.

5.1.2.1 Resource Trouble Management Services

The Resource Trouble Management Services are responsible for the management of troubles, including security events, associated with specific resources. The objectives of these processes are to efficiently and effectively manage reported resource trouble, isolate the root cause and act to resolve the resource trouble.

Responsibilities of the Resource Trouble Management servcies include:

- Detecting, analyzing managing and reporting on resource alarm event notifications;
- Initiating and managing resource trouble reports;
- Performing resource trouble localization analysis
- Correcting and resolving resource trouble:
- Reporting progress on resource trouble reports to other processes;
- Assigning & tracking resource trouble testing and repair activities;
- Managing resource trouble jeopardy conditions.

5.1.2.2 Resource Configuration and Activation Services

The Resource Configuration and Activation Services provide the necessary means to implement and enforce SMC resource configuration and activation policies at the communications level.

The Resource Configuration and Activation Services will configure and activate those resources allocated against an issued resource order. At the successful conclusion of configuration and activation the status of the specific resources will be changed from allocated to activated (i.e. in use).

5.1.2.3 Resource Performance Management Services

The Resource Performance Management Services encompass managing, tracking, monitoring, analyzing, controlling and reporting on the performance of specific resources. Resource Performance Management Services use information received from the Resource Data Collection & Distribution Services.

5.1.2.4 Resource Testing Services

The Resource Testing Services provides the necessary means to implement and enforce SMC resource testing policies at the communications level.

Resource Testing Services will test specific resources to ensure they are operating within normal parameters. The objective is to verify whether the resources are working correctly and meet the appropriate performance levels.

5.1.2.5 Resource Data Collection and Distribution Services

The Resource Data Collection and Distribution Services provide the necessary means to implement and enforce SMC resource data collection & distribution policies at the communications level.

Resource Data Collection & Distribution Services are responsible for collection and/or distribution of management information and data records between resource and service instances and other processes. Resource Data Collection & Distribution Services are responsible for collection and/or distribution of management information interact with the resource and service instances to intercept and/or collect usage, network and information technology events and other management information for distribution to other processes and with processes to accept command, query and other management information for distribution to resource and service instances.

5.1.2.6 Resource Discovery Services

The Resource Discovery Services provide the necessary means to implement and enforce SMC resource discovery policies at the communications level. They are automatically discovering the resources and their details through an management channel.

5.1.3 Analogue Access Services

The Analogue Access Services provide the delivery or exchange of analogue signals over an analogue interface port, without manipulation (encoding, compression) of the original signal, and directly interfacing a Transmission Service.

5.1.3.1 Analogue Audio Access Services

The Analogue Audio Access Services provide the delivery or exchange of analogue audio signals without manipulation (encoding, compression) of the original signal, and directly interfacing a Transmission Service.

5.1.3.2 Analogue Video Access Services

The Analogue Video Access Services provide the delivery or exchange of analogue video signals without manipulation (encoding, compression) of the original signal, and directly interfacing a Transmission Service.

5.1.3.3 Analogue Sensor Access Services

The Analogue Sensor Access Services provide the delivery or exchange of analogue sensor signals without manipulation (encoding, compression) of the original signal, and directly interfacing a Transmission Service.

5.1.4 Digital Access Services

The Digital (link-based) Access Services provide the delivery or exchange of digital signals (synchronous or asynchronous) over a native digital interface port, usually a port providing Transmission Services, at channel access level (e.g. the modem port of a handheld satcom terminal).

5.1.4.1 Native Digital Link Access Services

The Emulated Digital Link Access Services provide the delivery or exchange of digital signals over an interface with native digital access into a Transmission Service (e.g. data and clock signals).

5.1.4.2 Emulated Digital Link Access Services

The Emulated Digital Link Access Services provide the delivery or exchange of digital signals over an interface with emulated access, in which case the digital link is emulated over a higher layer protocol (e.g. RS-449 over IP).

5.1.5 Message-based Access Services

The Message-based Access Services provide the delivery or exchange of formatted messages, through user appliances that are directly connected to a Transmission Service (e.g. the keypad of a VHF radio).

5.1.5.1 Tactical Messaging Access Services

The Tactical Messaging Access Services provide the delivery or exchange of Tactical Data Link (TDL)-formatted messages, over a man-machine interface (e.g. a keyboard) or machine-machine interface (e.g. an avionics two-wire data bus).

The physical layer of the Tactical Data Links is covered under Transmission Services (Air-Ground-Air, and Maritime Surface-Surface).

5.1.5.2 Short Messaging Access Services

The Short Messaging Access Services provide the delivery or exchange of formatted, free text short messages, over a man-machine interface (e.g. a keyboard) or machine-machine interface (digital interface). The user interface (device) is part of the service.

5.1.6 Packet-based Access Services

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

5.1.6.1 IPv4 Routed Access Services

The IPv4 Routed Access Services provide the delivery or exchange of IP version 4 packets, subject to dynamic, destination- or policy-based routing, based on different routing protocols. The user's IP v4 address range is assigned by the provider of the Access Service, and it is provided to the Host via a DHCP service.

Each routing protocol is associated to a service type (i.e. an implementation option for the provider). Examples of IPv4 Routed Access Services implementation options are Static routing, Link-state Unicast routing (e.g. RIP, EIGRP), Distance-vector Unicast routing (OSPF), Path-vector Unicast routing (BGP), Policy-based Unicast routing (PBR), Multicast routing, and Mobile Ad-hoc Networking (MANET, e.g. OLSR-based).

5.1.6.2 IPv6 Routed Access Services

The IPv6 Routed Access Services provide the delivery or exchange of IP version 6 packets, subject to dynamic, destination-based routing, based on different routing protocols (each protocol is associated to a Service Type, i.e. an implementation option). The user's IP v6 address range is assigned by the provider of the Access Service.

Each routing protocol is associated to a service type (i.e. an implementation option for the provider). Examples of IPv6 Routed Access Services implementation options are Static routing, Link-state Unicast routing (e.g. RIP, EIGRP), Distance-vector Unicast routing (OSPF), Path-vector Unicast routing (BGP), Policy-based Unicast routing (PBR), Multicast routing, and Mobile Ad-hoc Networking (MANET, e.g. OLSR-based).

5.1.6.3 VPN Access Services

The Virtual Private Network (VPN) Services provide the delivery or exchange of IP version 4 or version 6 packets, subject to dynamic, destination-based routing, over a network of virtual links (tunnels). The user's IP address range is independent of the provider of Access Services.

VPN Services can be considered emulated IPv4 or IPv6 (tunneled in IPv4) routed services, as the routing is constrained to the IP tunnels, which act as point-to-point, virtual interfaces, agnostic to the multi-hop nature of the supporting transport network. Implementation examples are Packet-based VPN services (tunnelling over packet-based access), GRE-based VPN (such as L2TP-based VPN and IPSec VPN), and session-based VPN services (SSH-based or SSL-based tunnelling over session-based access).

5.1.7 Frame-based Access Services

The Frame-based Access Services provide the 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.

5.1.7.1 Native Frame-based Access Services

The Native Frame-based Access Services provide the delivery or exchange of frames over an access device that forwards transparently over to the Transport Services or Transmission Services block.

5.1.7.2 Emulated Frame-based Access Services

The Emulated Frame-based Access Services provide the delivery or exchange of frames over higher layer protocols (e.g. pseudo-wires). The adaptation of the frame layer to the higher layer protocol is performed within the access device. Frame-based protocols (e.g. Ethernet, PPP, PPPoE) and the underlying protocols supporting the emulation, define the various Service Types within this Service Class (e.g. Ethernet over IP/MPLS).

5.1.8 Circuit-based Access Services

The Circuit-based Access Services provide the delivery or exchange of raw user data, via fractional access to digital lines (circuits), e.g. ISDN BRI, fractional E1, etc. These services are provided 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 Access Services), or directly to Transmission Services (e.g. ISDN port of an Inmarsat satcom terminal).

5.1.8.1 Native Circuit-based Access Services

The Native Circuit-based Access Services provide the delivery or exchange of raw user data through adaptation appliances (e.g. ISDN BRI terminal adapter). At implementation level, different service types can be considered, associated to different implementations of TDM technology (e.g. ISDN, T1, etc).

5.1.8.2 Emulated Circuit-based Access Services

The Emulated Circuit-based Access Services provide virtualised circuit-based access services, riding on higher layer protocols (e.g. ISDN BRI over IP, fractional E1 over Ethernet, etc). The adaptation function of the circuit layer to the underlying carrier protocol is performed within the access device. At the implementation level, different Service Types can be considered, associated to the circuit technology emulated, and the underlying carrier protocol.

5.1.9 Multimedia Access Services

The Multimedia Access Services provide the delivery or exchange of multimedia data via interaction with the end-user or end-user application. The services support the adaptation of the media involved (analogue voice, video, digital desktop, etc) for delivery or exchange over packet-based, frame-based, circuit-based, or digital (link-based) access services (through e.g. routers, switches, terminal adapters or multiplexers, or directly over a digital port).

5.1.9.1 Voice Access Services

The Voice Access Services provide the delivery or exchange of voice information over packet-based, frame-based, circuit-based, or digital (link-based) access services, through adaptation (e.g. encoding and compression) the capability for voice appliances like VoIP phones, microphones, handsets, etc.

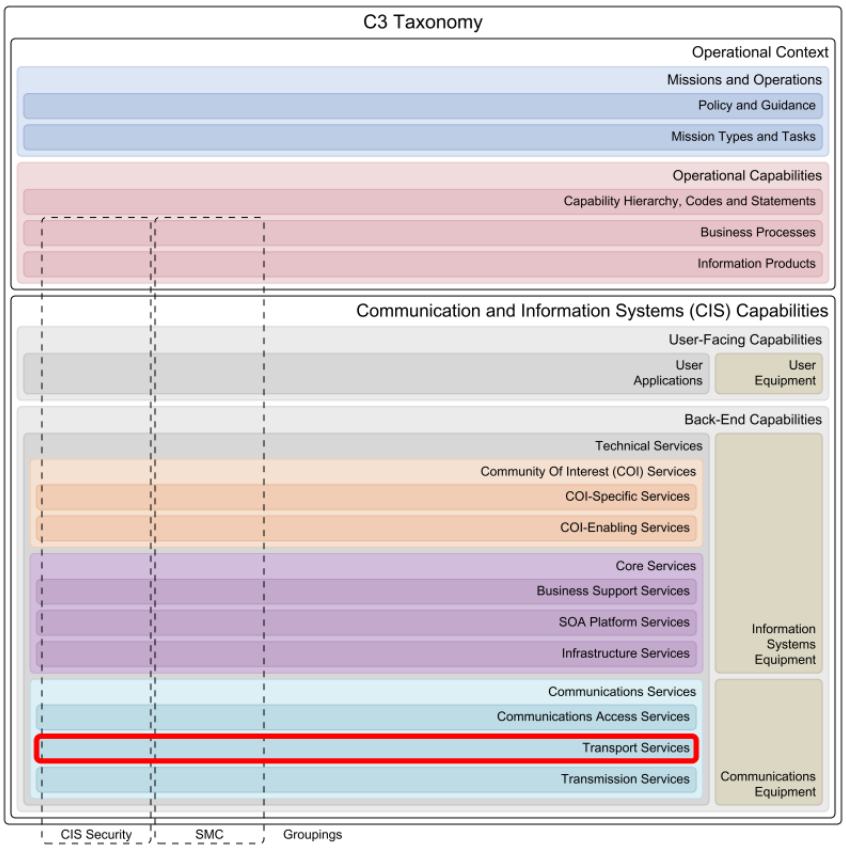
5.1.9.2 Video Access Services

The Video Access Services provide the delivery or exchange of video information either over packet-based, frame-based, circuit-based, or digital (link-based) access services, through adaptation (e.g. encoding and compression) the capability for video appliances like webcams, cameras (e.g surveillance), etc.

5.1.9.3 VTC Access Services

The Video Teleconference (VTC) Access Services provide the delivery or exchange of multimedia communication sessions involving simultaneous two-way video and audio transmission to be established between two or more locations, through various VTC appliances, for example (web)camera, telephone, microphone, (touch)screens and other visual aids.

5.2 Transport Services



The Transport Services correspond to 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.

5.2.1 Transport CIS Security Services

The Transport CIS Security Services provide a foundation to implement and enforce CIS Security policies at the communications transport level.

5.2.1.1 Transport Cryptography Services

The Transport Cryptography Services provide encryption capabilities required to secure (encrypt & decrypt) transfer of data over a variety of end-to-end transports supported over and/or within the "Core Network" (e.g. WAN, PCN).

5.2.2 Transport SMC Services

The Transport Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the communications transport level.

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.

Within the context of SMC for all Communications Services, the functions and subsequent requirements on each the three layers - Communications Access Services, Transport Services and Transmission Services - experience a great overlap and high level of similarity. Therefore all SMC Services for these layers are defined under Communications Access SMC Services, while they are valid for this layer just the same.

5.2.2.1 Transport Logging Services

The Transport Logging Services capture transport related events and/or errors for the purpose of regulatory compliance, performance optimizations, auditing or trouble shooting.

5.2.2.2 Transport Monitoring Services

The Transport Monitoring Services provide information on the actual utilization and performance of monitored Transport Services. The Transport Monitoring Services deliver information about service exceptions and support root-causes analysis to help locate performance bottlenecks, errors, or incomplete transactions.

5.2.2.3 Transport Metering Services

The Transport Metering Services measures the utilization of transport resources over specific period of times. Calculated average values of the measurements can be then used to enforce Service Level Agreements (SLAs), billing purposes and overall usage trend forecasting.

5.2.3 Edge Services

The 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).

5.2.3.1 Packet-based Transport Services

The Packet-based Transport Services provide the transport of Internet Protocol (IP) packets between two or more end-points, involving forwarding between packet-based routers using destination-based or policy-based routing protocols natively or over Virtual Private Network (VPN) tunnels. In these services the routing is performed on a per-packet basis. The services' "unit" is the packet flow, a flow of packets sharing a given attribute coded in the packet header (e.g. source, destination address or type of service).

Packet-based Transport Services can interface to Transmission Services through various possible Cross-layer Adaptation Functions (CLAF) such as Packet Optical Transport (P-OTS), based on the transport of IP packets over fibre using Multiprotocol Label Swiching Transport Profile (MPLS-TP).

The same breakdown provided under the Packet-based Access Services class applies to the Packet-based Transport Services class. Only certain service types like Session-based VPNs are not applicable in this Transport Services context as those can only be initiated from the user end-point devices and applications (e.g. a browser running on a laptop, in turn served by a packet-based access service on its network interface).

5.2.3.2 Frame-based Transport Services

The Frame-based Transport Services provide the transport of frames or cells between two or more end-points, involving forwarding between frame/cell switches using associated switching protocols. In Frame-based Transport Services switching is performed on a per-frame, per-cell basis. The services' "unit" is the virtual circuit, consisting of a flow of frames or cells, which share a given attribute coded in the frame or cell header (e.g. an MPLS tag, or stack of MPLS tags, or a Data Link Connection Identifier (DLCI) value in Frame Relay, or a VLAN tag in Carrier Ethernet).

Frame-based Transport Services can interface to Transmission Services through various possible Cross-layer Adaptation Functions (CLAF) often by directly transporting frames (or cells) over fibre (e.g. Ethernet over SDH).

Frame-based Transport Services can be native or emulated over higher layer protocols (e.g. over IP/MPLS).

Frame-based Transport Services service classes (and various support protocols within) are:

- Native Frame-based Transport -- Frame Relay, Asynchronous Transfer Mode (ATM); Multiprotocol Label Switching (MPLS); and Ethernet; or
- Emulated Frame-based Transport -- L2VPN (over IP, or IP/MPLS); Ethernet over MPLS; Virtual Private LAN Service (VPLS, multipoint to multipoint); and Virtual Private Wire Services (VPWS, point to point).

5.2.3.3 Circuit-based Transport Services

The Circuit-based Transport Services provide the transport of data channels between two points, multiplexed over a transmission line (leased line, or digital trunk line) using Time Division Multiplexing (TDM). Channels can carry raw synchronous data which is framed to fit into the channelized structure of the transmission line. Trunk lines can be switched at intermediate points. In these services switching is performed on a per-channel basis. The services' "unit" is the channel within the digital trunk line, and each channel carries a framed synchronous data stream (voice or data).

Circuit-based Transport Services can be native, or emulated over higher layer protocols (e.g. IP or ATM).

Circuit-based Transport Services service classes (and various support protocols within) are:

- Native Circuit-based Transport Services -- ISDN PRI, and TDM (E1,E3, etc); and
- Circuit Emulation Services -- ISDN PRI over IP, TDM over IP, and E3 over ATM.

5.2.3.4 Link Emulation Transport Services

The Link Emulation Transport Services provide the emulation of synchronous serial data streams (i.e. data and clock) over packet, frame or circuit-based Edge Transport Services.

5.2.4 Transit Services

The Transit 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 Transit Services (e.g. routers, switches, radio relays, SATCOM transponders, etc) may operate at different points across the core of the network. The Transit 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 Packet-, Frame- and Circuit-based Transport Services. Nonetheless, Transit Services are not concerned with emulated Communications Access Services or Packet-, Frame- and Circuit-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.

Transit 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 Transit Service is specified and will form part of the Service Level Specification (SLS).

5.2.4.1 Packet Routing Services

The Packet Routing Services provide static or dynamic routing and forwarding of Internet Protocol (IP) version 4 packets, based on dynamic, destination- or policy-based protocols.

Similar as with IPv4 Routed Access Services, each routing protocol is associated to a service type (i.e. an implementation option for the provider). Examples of IPv4 Routed Access Services implementation options are Static routing, Link-state Unicast routing (e.g. RIP, EIGRP), Distance-vector Unicast routing (OSPF), Path-vector Unicast routing (BGP), Policy-based Unicast routing (PBR), Multicast routing, and Mobile Ad-hoc Networking (MANET, e.g. OLSR-based). On top of those, other applicable service types, related to the provider edge of a transport network, are Traffic Engineering Services (e.g. MPLS-TE), and Virtual Routing and Forwarding Services.

5.2.4.2 Frame Switching Services

The Frame Switching Services provide the static or dynamic switching and forwarding of frames, cells, and the resulting virtual circuits (permanent or switched).

The following service types can be considered as being associated with frame-based encapsulation and switching protocols:

- Frame-based Switching , e.g. frame relay switching service
- Cell-based Switching, e.g. ATM switching service
- Label-based switching, e.g. MPLS switching service
- Tag-based switching, e.g. VLAN/ethernet switching service

5.2.4.3 Link Switching Services

The Link Switching Services provide static switching and forwarding of different fractional channels or full digital trunk lines over an established (e.g. dialed-up) dedicated communications channel (circuit). The communications channel functions as if the nodes were physically connected and guarantees the full bandwidth of the channel for the duration of the communication session.

The following service types can be considered as being associated with link-switching protocols:

- Slot-based switching -- Switching different time slots within a TDMA carrier to different nodes in a TDMA network (wireless, satcom), for transmission or reception. Considered protocols, also serving a time-domain multiple access purpose, are multi-frequency Time Division Multiple Access (TDMA) and selective TDMA.
- Frequency-based (or wavelength-based) switching services -- Switching different frequencies (or wavelengths) within a given frequency range, to different nodes in a FDMA network (wireless, satcom) for transmission or reception. Considered protocols are Single-Carrier Frequency-Division Multiple Access (SC-FDMA), Orthogonal Frequency-Division Multiple Access (OFDMA) or Wavelength Division Multiple Access (WDMA).
- Code-based switching services -- Switching different codes within a given family of pseudo-random codes, modulating RF carriers, to different nodes in a Code-division Multiple Access network (wireless, satcom) for transmission or reception. Considered protocols are W-CDMA, TD-CDMA, TD-SCDMA, DS-CDMA, FH-CDMA, OFHMA and MC-CDMA.
- Channel switching services -- Switching RF carriers to channels/sub-channels on different transponders, coverage areas, for transmission or reception (applies to satellite communications only).

5.2.5 Aggregation Services

The Aggregation Services provide the aggregation of traffic over parallel converging transmission paths, and involves Packet-, Frame- and Circuit-based 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 Transit Services, Aggregation Services can be closely mapped to the OSI stack lower layers.

5.2.5.1 Packet-based Aggregation Services

The Packet-based Aggregation Services provide the termination of tunnels carrying Internet Protocol (IP) packets or, in other words, the termination of Access Services under the packet-based category VPN class through VPN concentrators.

Packet-based Aggregation Services also provide the termination of IP flows (not tunnelled) in star topologies supported over wireless or SATCOM (e.g. IP SATCOM hub). In this case the services terminate packet-based IPv4 Routed Access Services or IPv6 Routed Access Services (subtended over SATCOM or radio).

Hence, the following three service types can be considered for aggregation:

- IPv4 Routed Access Services;
- IPv6 Routed Access Services; and
- VPN Services or virtual IP routed services, which can either be Packet-based VPN termination Services (IP VPN) or Session-based VPN termination Services (SSL/TLS VPN).

5.2.5.2 Frame-based Aggregation Services

The Frame-based Aggregation Services provide the termination of Frame-based Access Services or Frame-based Transport Services supported by different Transmission Services (e.g. optical, wireless terrestrial, SATCOM).

The following service types can be considered:

- Star Topology frame services (Ethernet based, e.g. L2 satcom hub);
- L2 SATCOM hub services;
- DSL hub services (terrestrial, ATM based); and
- DLOS/NLOS hub services (incl. WiMAX).

5.2.5.3 Circuit-based Aggregation Services

The Circuit-based Aggregation Services involve the termination of multiple tributary circuits (e.g. E1), each providing circuit-based transport services to different network nodes, and multiplexing them into an aggregate rate (e.g. 16x E1 lines at 2 Mbps each, multiplexed into one E3 line at 34 Mbps).

5.2.5.4 Link-based Aggregation Services

The Link-based (multiple access) Aggregation Services involve the termination of FDMA links (traffic flows transported over carriers at different frequencies), TDMA links (traffic flows transported over time slots of the same or multiple carriers) or CDMA links (traffic flows transported over the same or multiple carriers, using different spreading codes), or variants of these protocols involving one node (hub) acting as concentrator either by stacking multiple modems, or by implementing an integrated multi-modem assembly.

5.2.6 Broadcast Services

The Broadcast Services provide the distribution of transport flows through a combination both the "within the core" and "at the edge" infrastructure types to form a logical "ring'. Broadcast Services within the core involve the broadcast of transport flows towards multiple edge-points that connect to the broadcast node either directly over transmission lines or through Transit Services. Broadcast Services at the edge involve the broadcast of traffic flows towards multiple end-nodes that connect to the broadcast node over transmission lines.

Broadcast Services involve Packet-, Frame- and Circuit-based 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).

5.2.6.1 Packet-based Broadcast Services

The Packet-based Broadcast Services provide the dissemination of IP multicast packets.

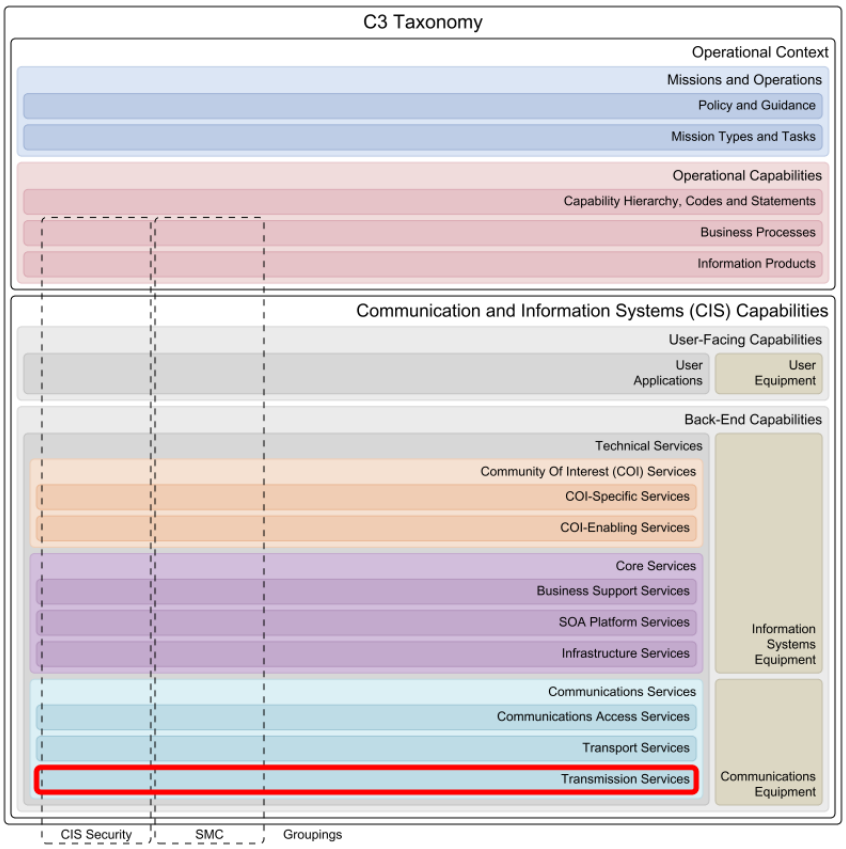
5.2.6.2 Frame-based Broadcast Services

The Frame-based Broadcast Services provide the dissemination of (MAC or VLAN) frames.

5.2.6.3 Link-based Broadcast Services

The Link-based Broadcast Services provide the dissemination of simplex data links.

5.3 Transmission Services



The 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.

5.3.1 Transmission CIS Security Services

The Transmission CIS Security Services provide a foundation to implement and enforce CIS Security policies at the communications transmission level.

5.3.1.1 Transmission Security Services

The Transmission Security Services provide Transmission Security (TRANSEC) which is a component of Communications Security (COMSEC). TRANSEC measures are designed to protect transmissions from interception and exploitation by means other than cryptanalysis. TRANSEC aims to achive low probability of interception (LPI); low probability of detection (LPD); and antijamming (EPM or ECCM).

TRANSEC methods include frequency hopping and spread spectrum where the required pseudorandom sequence generation is controlled by a cryptographic algorithm and key.

5.3.2 Transmission SMC Services

The Transmission Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the communications transmission level.

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.

5.3.2.1 Transmission Logging Services

The Transmission Logging Services capture transmission related events and/or errors for the purpose of regulatory compliance, performance optimizations, auditing or trouble shooting.

5.3.2.2 Transmission Monitoring Services

The Transmission Monitoring Services provide information on the actual utilization of monitored Transport Services. The Transmission Monitoring Services deliver information about service exceptions and help identify problems.

5.3.2.3 Transmission Metering Services

The Transmission Metering Services measures the utilization of transmission services over specific period of times. Calculated average values of the measurements can be then used to enforce Service Level Agreements (SLAs), billing purposes and overall usage trend forecasting.

5.3.3 Wired Transmission Services

The Wired Transmission Services support physical transfer of data, point-to-point or point-to multipoint, using wired transmission medium amongst two or more static nodes. Based on range and capacity, these services are distinguished for Local Area Networks (LAN - over relatively short distances), Metropolitan Area Networks (MAN - medium to high capacity over distances spanning tens of kilometers) or Wide Area Networks (WAN - high capacity wired transmission medium over long distances).

5.3.3.1 Wired Local Area Transmission Services

The Wired Local Area Transmission Services support physical transfer of data, 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.

5.3.3.2 Wired Metropolitan Area Transmission Services

The Wired Metropolitan Area Transmission Services support physical transfer of data, 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).

5.3.3.3 Wired Wide Area Transmission Services

The Wired Wide Area Transmission Services support physical transfer of data, 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).

5.3.4 Wireless LOS Static Transmission Services

The 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.

5.3.4.1 Wireless LOS Static Narrowband Transmission Services

The Wireless Line of Sight (LOS) Static Narrowband 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, and employing narrowband low capacity wireless terminals operating mainly in the VHF, UHF frequency bands and in the HF frequency band using direct or ground wave propagation.

Examples of Wireless LOS Static Narrowband Transmission Services are Single Channel HF/VHF/UHF Radio Equipment, Slow Hop HF EPM Communications Systems, Tactical Data Exchange (Link11/Link 11B), and Future NATO Narrowband Waveform (NBWF).

5.3.4.2 Wireless LOS Static Wideband Transmission Service

The Wireless Line of Sight (LOS) Static Wideband 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, and employing wideband high capacity wireless terminals operating in the UHF frequency band, S band (2 to 4 GHz), C band (4 to 8 GHz) and NATO military band IV (4.4 to 5 GHz).

Examples of Wireless LOS Static Wideband Transmission Services are Point-to Point Microwave radio links, Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metropolitan Area Network (WMAN), Worldwide Interoperability for Microwave Access (WiMAX), Tactical Highband Networking Waveform (HNW), and Future NATO Wideband Waveform (WBWF).

5.3.5 Wireless LOS Mobile Transmission Services

The 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).

5.3.5.1 Wireless LOS Mobile Narrowband Transmission Services

The Wireless Line of Sight (LOS) Mobile Narrowband 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, and employing narrowband low capacity wireless terminals operating mainly in the VHF, UHF frequency bands and in the HF frequency band using direct or ground wave propagation.

Examples of Wireless LOS Mobile Narrowband Transmission Services are Single Channel HF/VHF/UHF Radio Equipment, Slow Hop HF EPM Communications Systems, Tactical Data Exchange (Link11/Link 11B), and Future NATO Narrowband Waveform (NBWF), all with the consideration that adequate tracking antennas are employed and the transceivers are

adapted for platform motion. Additional service types are Terrestrial Trunked Radio (TETRA), Militarized Cellular Networks, Digital Enhanced Cordless Telecommunications (DECT), and Narrowband HF/VHF Subnet Relay.

5.3.5.2 Wireless LOS Mobile Wideband Transmission Services

The Wireless Line of Sight (LOS) Mobile Wideband 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, and employing wideband high capacity wireless terminals operating in the UHF frequency band, S band (2 to 4 GHz), C band (4 to 8 GHz) and NATO military band IV (4.4 to 5 GHz).

Examples of the Wireless LOS Mobile Wideband Transmission Services are Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metropolitan Area Network (WMAN), Worldwide Interoperability for Microwave Access (WiMAX), Tactical Highband Networking Waveform (HNW), and Future NATO Wideband Waveform (WBWF), all with the consideration that adequate tracking antennas are employed and the transceivers are adapted for platform motion. Additional service types are Wideband Network Radio (WNR) systems, High Capacity Data Radio (HCDR) systems, and Wideband UHF Subnet Relay.

5.3.6 Wireless BLOS Static Transmission Services

The 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.

5.3.6.1 Wireless BLOS Static Narrowband Transmission Services

The Wireless Beyond Line of Sight (BLOS) Static Narrowband Transmission Services support the wireless transfer of data amongst two or more static nodes Beyond Line of Sight (LOS) of each other, employing modulated Radio Frequency (RF) carriers in different frequency bands, and employing narrowband low capacity wireless terminals operating in the VLF and HF (sky wave propagation) frequency band, or narrowband SATCOM operating in the VHF, UHF and SHF frequency bands and L band (1 to 2 GHz) and X band (8 to 12 GHz).

Examples of Wireless BLOS Static Narrowband Transmission Services are Single and Multichannel VLF and LF ON-Line and On-Line and Off-Line OOK Systems, Single Channel HF Radio Equipment, Slow Hop HF EPM Communications Systems, Tactical Data Exchange (Link11/Link 11B), UHF Demand Assigned Multiple Access (DAMA), Super High Frequency (SHF) Military Satellite Communications (MILSATCOM), Iridium satellite phone communications, and Inmarsat satellite services.

5.3.6.2 Wireless BLOS Static Wideband Transmission Services

The Wireless Beyond Line of Sight (BLOS) Static Wideband Transmission Services support the wireless transfer of data amongst two or more static nodes Beyond Line of Sight (LOS) of each other, employing modulated Radio Frequency (RF) carriers in different frequency bands, and employing wideband high capacity wireless terminals operating in the SHF frequency band and the C band (4 to 8 GHz) and NATO military band IV (4.4 to 5 GHz).

Examples of Wireless BLOS Static Wideband Transmission Services are SHF Military Satellite Communications (MILSATCOM), SHF Medium Data Rate (MDR) Military Satellite Communications (MILCOM) Jam-Resistant Modem, Satellite Broadcast Service (SBS), Broadband Global Area Network (BGAN), and troposcatter services operating in the 4 to 5 GHz range (i.e. C band) up to a distance of approximately 300 km.

5.3.7 Wireless BLOS Mobile Transmission Services

The 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).

5.3.7.1 Wireless BLOS Mobile Narrowband Transmission Services

The Wireless Beyond Line of Sight (BLOS) Mobile Narrowband 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, and employing narrowband low capacity wireless terminals operating mainly in the VHF, UHF frequency bands and in the HF frequency band using sky wave propagation.

Examples of Wireless BLOS Mobile Narrowband Transmission Services are Single and Multichannel VLF and LF ON-Line and On-Line and Off-Line OOK Systems, Single Channel HF Radio Equipment, Slow Hop HF EPM Communications Systems, Tactical Data Exchange (Link11/Link 11B), UHF Demand Assigned Multiple Access (DAMA), Super High Frequency (SHF) Military Satellite Communications (MILSATCOM), Iridium satellite phone communications, and Inmarsat satellite services, all with the consideration that adequate tracking antennas are employed and the transceivers are adapted for platform motion.

An additional example is describing HALE service while employing a UAV mounted VHF-UHF CRP supporting AM/FM Line of Sight, SINCGARS ESIP/FH2, HAVEQUICK I/II, Advanced Narrowband Digital Voice Terminal (ANDVT), MIL-STD-188-181C 56kbps, and SATCOM Integrated Waveform MIL-STD-188-182B/183B.

5.3.7.2 Wireless BLOS Mobile Wideband Transmission Services

The Wireless Beyond Line of Sight (BLOS) Mobile Wideband 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, and employing wideband high capacity wireless terminals operating in the SHF frequency band and the C band (4 to 8 GHz) and NATO military band IV (4.4 to 5 GHz).

Examples of Wireless BLOS Mobile Wideband Transmission Services are SHF Military Satellite Communications (MILSATCOM), SHF Medium Data Rate (MDR) Military Satellite Communications (MILCOM) Jam-Resistant Modem, Satellite Broadcast Service (SBS), and Broadband Global Area Network (BGAN), all with the consideration that adequate tracking antennas are employed and the transceivers are adapted for platform motion.

C3 Technical Services Taxonomy

Community Of Interest (COI) Services

COI-Specific Services

COI-Specific CIS Security Services
- Recognized Cyber Picture Services
- Cyber Defence Services
- CIS Security Audit Analysis Services
- Advanced Threat Management Service
- Electronic Key Management Services

COI-Specific SMC Services
- Spectrum Management Services
- Spectrum Usage Information Services
- Call Management Services
- VTC Management Services

Joint Services
- Surface Area Management Services
- NATO Crisis Response Measures Services

Air Services
- Recognized Air Picture Services
- Aeronautical Information Services
- ACO Services
- Air Asset List Services
- ATO Services
- Airspace Management Services
- Airspace Structure Management Services
- Airlift Services
- Air Threat Analysis Services
- Air Weapon Matching Services
- Air Mobility Analysis Services

Land Services
- Recognized Ground Picture Services
- Manoeuver Planning Services
- Task Time Location Management Services
- Terrain Analyzer Services
- Task Classifier Services
- Force Comparison Services

Maritime Services
- Recognized Maritime Picture Services
- Maritime Anomaly Detection Services
- Water Space Management Services
- Mine Warfare Services
- Amphibious Warfare Services
- Sonar Prediction Services

JISR Services
- Intelligence Requirements Management Services
- JISR Collection and Exploitation Plans Services
- JISR Sensor Services
- JISR Exploitation Services
- JISR Analysis and Production Services
- JISR Reporting Services
- JISR Imagery and Video Services

Logistics Services
- Recognized Logistic Picture Services
- Recognized Medical Picture Services
- Casualty Rate Estimation Services

Electronic Warfare Services
- Emitter Services
- Emitter Analysis Services
- Restricted Frequency List Services

Environmental Services
- Recognized Environmental Picture Services
- Geography Services
- Meteorology Services
- Oceanography Services
- Hydrography Services
- Space Weather Services

CIMIC Services
- Behaviour Analysis Services
- Pattern Analysis Services

ETEE Services
- Objectives Management Services
- MEL MIL Management Services

Modeling and Simulation Services
- Modeling and Simulation Infrastructure Services
- Modeling and Simulation Integration Services

COI-Enabling Services

COI-Enabling CIS Security Services
- Cyber Threat Detection Services

COI-Enabling SMC Services
- Data Exchange Monitoring Services

Operations Planning Services
- Deployment Plan Services
- Courses of Action Services
- Synchronisation Matrix Services
- Order of Battle Services
- Operation Plan Development Services
- Targeting Services

Tasking and Order Services
- Resource Request Services
- Resource Allocation Services
- Operations Estimation Services
- Tasking Services
- Operations Assessment Services
- Operations Order Services

Situational Awareness Services
- Recognized Picture Services
- Symbology Services

Battlespace Information Services
- Battlespace Event Services
- Battlespace Object Services
- Track Services

Modeling and Simulation Enabling Services
- Battlespace Simulation Services
- Radio Simulation Services
- Ground Truth Battlespace Objects Services
- Ground Truth Battlespace Events Services

Core Services

Business Support Services

Business Support CIS Security Services
- Business Support Guard Services

Business Support SMC Services
- Application Store Services
- Configuration Management Database Services

Unified Communication and Collaboration Services
- Military Messaging Services
- Informal Messaging Services
- Fax Services
- Calendaring and Scheduling Services
- Video-based Communication Services
- Audio-based Communication Services
- Text-based Collaboration Services
- Whiteboarding Services
- Presence Services
- Document Sharing Services
- Application Sharing Services

Information Management Services
- Content Management Services
- Workflow Services
- Distributed Search Services
- Report Generation Services
- Analytics Services
- Language Support Services

ERP Services
- Financial Resource Management Services
- Human Resource Management Services
- Supply Chain Management Services
- Project Planning Services

Geospatial Services
- Geospatial Catalog Services
- Geospatial Web Map Services
- Geospatial Web Feature Services
- Geospatial Web Coverage Services
- Geospatial Web Map Tile Services
- Geospatial Network Analysis Services
- Geospatial Coordinate Services
- Geospatial Terrain Analysis Services

SOA Platform Services

SOA Platform CIS Security Services
- SOA Platform Guard Services
- Security Token Services
- Policy Enforcement Point Services
- Policy Decision Point Services
- Policy Administration Point Services
- Information Labeling Services

SOA Platform SMC Services
- SOA SMC Policy Enforcement Services
- Service Discovery Services
- SOA Platform Logging Services
- SOA Platform Monitoring Services
- SOA Platform Metering Services

Message-Oriented Middleware Services
- Direct Messaging Services
- Message Brokering Services
- Message Routing Services
- Message Proxying Services
- Message Queueing Services
- Message Caching Services

Web Platform Services
- Web Hosting Services
- Web Presentation Services
- Web Caching Services
- Web Proxying Services

Information Platform Services
- Information Discovery Services
- Information Access Services
- Information Aggregation Services
- Metadata Repository Services
- Information Annotation Services
- Business Rules Services

Composition Services
- Orchestration Services
- Choreography Services
- Transaction Services

Mediation Services
- Protocol Transformation Services
- Data Format Transformation Services

Infrastructure Services

Infrastructure CIS Security Services
- Digital Identity Services
- Credentialing Services
- Authentication Services
- Privilege Management Services
- Authorization and Access Services
- Digital Certificate Services
- Intrusion Detection Services
- Malware Detection Services
- Infrastructure Guard Services
- Infrastructure Cryptography Services

Infrastructure SMC Services
- Infrastructure Provisioning Services
- Infrastructure Logging Services
- Infrastructure Monitoring Services
- Infrastructure Metering Services

Infrastructure Processing Services
- Operating System Services
- Virtualized Processing Services

Infrastructure Storage Services
- Block-Level Storage Services
- Non-relational Structured Storage Services
- Directory Storage Services
- File System Storage Services
- Blob Storage Services
- Relational Database Storage Services

Infrastructure Networking Services
- Host Configuration Services
- Network Load Balancing Services
- Printing and Scanning Services
- Data Transfer Services
- Domain Name Services
- Distributed Time Services
- Remote Access Services

Communications Services

Communications Access Services

Communications Access CIS Security Services
- Communications Security Services
- Network Access Control Services
- Network Firewall Services

Communications Access SMC Services
- Resource Trouble Management Services
- Resource Configuration and Activation Services
- Resource Performance Management Services
- Resource Testing Services
- Resource Data Collection and Distribution Services
- Resource Discovery Services

Analogue Access Services
- Analogue Audio Access Services
- Analogue Video Access Services
- Analogue Sensor Access Services

Digital Access Services
- Native Digital Link Access Services
- Emulated Digital Link Access Services

Message-based Access Services
- Tactical Messaging Access Services
- Short Messaging Access Services

Packet-based Access Services
- IPv4 Routed Access Services
- IPv6 Routed Access Services
- VPN Access Services

Frame-based Access Services
- Native Frame-based Access Services
- Emulated Frame-based Access Services

Circuit-based Access Services
- Native Circuit-based Access Services
- Emulated Circuit-based Access Services

Multimedia Access Services
- Voice Access Services
- Video Access Services
- VTC Access Services

Transport Services

Transport CIS Security Services
- Transport Cryptography Services

Transport SMC Services
- Transport Logging Services
- Transport Monitoring Services
- Transport Metering Services

Edge Services
- Packet-based Transport Services
- Frame-based Transport Services
- Circuit-based Transport Services
- Link Emulation Transport Services

Transit Services
- Packet Routing Services
- Frame Switching Services
- Link Switching Services

Aggregation Services
- Packet-based Aggregation Services
- Frame-based Aggregation Services
- Circuit-based Aggregation Services
- Link-based Aggregation Services

Broadcast Services
- Packet-based Broadcast Services
- Frame-based Broadcast Services
- Link-based Broadcast Services

Transmission Services

Transmission CIS Security Services
- Transmission Security Services

Transmission SMC Services
- Transmission Logging Services
- Transmission Monitoring Services
- Transmission Metering Services

Wired Transmission Services
- Wired Local Area Transmission Services
- Wired Metropolitan Area Transmission Services
- Wired Wide Area Transmission Services

Wireless LOS Static Transmission Services
- Wireless LOS Static Narrowband Transmission Services
- Wireless LOS Static Wideband Transmission Service

Wireless LOS Mobile Transmission Services
- Wireless LOS Mobile Narrowband Transmission Services
- Wireless LOS Mobile Wideband Transmission Services

Wireless BLOS Static Transmission Services
- Wireless BLOS Static Narrowband Transmission Services
- Wireless BLOS Static Wideband Transmission Services

Wireless BLOS Mobile Transmission Services
- Wireless BLOS Mobile Narrowband Transmission Services
- Wireless BLOS Mobile Wideband Transmission Services